aws

Entwicklerhandbuch

# AWS IoT Core

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS IoT Core: Entwicklerhandbuch

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Marken und Handelsmarken von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, die geeignet ist, Kunden irrezuführen oder Amazon in irgendeiner Weise herabzusetzen oder zu diskreditieren. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

# Table of Contents

Was ist AWS IoT? ..... 1
So greifen Ihre Geräte und Apps darauf zu AWS IoT ..... 2
Was AWS IoT kann ich tun ..... 3
IoT ..... 3
IoT in der Hausautomation ..... 3
Wie AWS IoT funktioniert ..... 4
Das IoT-Universum ..... 4
AWS IoT Dienstleistungen im Überblick ..... 7
AWS IoT Core Dienstleistungen ..... 12
Erfahren Sie mehr über AWS IoT ..... 16
Schulungsressourcen für AWS IoT ..... 16
AWS IoT Ressourcen und Leitfäden ..... 17
AWS IoT in den sozialen Medien ..... 18
AWS Dienste, die von der AWS IoT Core Rules Engine verwendet werden ..... 18
Kommunikationsprotokolle, unterstützt von AWS IoT Core ..... 19
Was ist neu in derAWS IoT -Konsolenumgebung ..... 20
Legende ..... 24
Arbeitet mit AWS SDKs ..... 24
Erste-Schritte-Tutorials ..... 26
Connect dein erstes Gerät mit AWS IoT Core ..... 26
Einrichten AWS-Konto ..... 28
Melde dich an für ein AWS-Konto ..... 28
Erstellen eines Benutzers mit Administratorzugriff ..... 29
Öffnen Sie die AWS IoT Konsole ..... 31
Interaktives Tutorial ..... 31
IoT-Geräte verbinden ..... 32
Der Status des Offline-Geräts wird gespeichert ..... 33
Gerätedaten an Dienste weiterleiten ..... 34
Schnellverbindungs-Tutorial ..... 35
Schritt 1. Beginnen Sie mit dem Tutorial ..... 36
Schritt 2. Dies erstellt ein Objekt ..... 37
Schritt 3. Laden Sie Dateien auf Ihr Gerät herunter ..... 41
Schritt 4. Ausführen des Beispiels ..... 44
Schritt 5. Weiter erkunden ..... 48

Testen Sie die Konnektivität ... 49
Connect-Tutorial für Fortgeschrittene ... 55
Welche Geräteoption ist für Sie am besten geeignet? ... 56
AWS IoT Ressourcen erstellen ... 57
Konfigurieren Ihres Geräts ... 62
MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen ... 103
Anzeigen von MQTT-Nachrichten im MQTT-Client ... 104
Veröffentlichen von MQTT-Nachrichten vom MQTT-Client ... 107
Testen von geteilten Abonnements im MQTT-Client ... 109
AWS IoT Anleitungen ... 111
Demos mit dem AWS IoT Device Client erstellen ... 111
Voraussetzungen für die Erstellung von Demos mit dem AWS IoT Geräte-Client ... 112
Vorbereitung der Verwendung des IoT Device Client ... 115
Installation und Konfiguration des IoT-Geräteclients ... 130
Kommunizieren Sie mit dem Geräteclient über MQTT ... 144
Führen Sie IoT-Jobs mit dem Device Client aus ... 165
Bereinigen ... 180
Mit dem AWS IoT Gerät Lösungen entwickeln SDKs ... 190
Fangen Sie an, Lösungen mit dem AWS IoT Gerät zu entwickeln SDKs ... 190
Ein Gerät AWS IoT Core mithilfe des AWS IoT Geräts an anschließen SDK ... 191
AWS IoT Regeln erstellen, um Gerätedaten an andere Dienste weiterzuleiten ... 216
Beibehalten des Gerätestatus mit Geräteschatten, während das Gerät offline ist ... 264
Erstellen eines benutzerdefinierten Autorisierers für AWS IoT Core ... 296
Überwachung der Bodenfeuchte mit einem AWS IoT Raspberry Pi ... 315
Verbinden mit AWS IoT Core ... 330
Endpunkte von AWS IoT Core – Steuerebene ... 330
AWS IoT Geräteendpunkte ... 331
AWS IoT Core für WAN-Gateways und -Geräte LoRa ... 333
Connect zu AWS IoT Core Service-Endpunkten her ... 334
AWS CLI für AWS IoT Core ... 334
AWS SDKs ... 335
AWS Mobil SDKs ... 341
REST APIs der AWS IoT Core Dienste ... 342
Geräte Connect mit AWS IoT ... 342
AWS IoT Gerätedaten und Dienstendpunkte ... 343
AWS IoT Gerät SDKs ... 346

Gerätekommunikationsprotokolle ..... 348
MQTT-Themen ..... 393
Domänenkonfigurationen ..... 422
Connect zu AWS IoT FIPS-Endpunkten her ..... 452
Endpunkte von AWS IoT Core – Steuerebene ..... 452
Endpunkte von AWS IoT Core – Datenebene ..... 453
AWS IoT Core- Endpunkte des Anmeldeinformationsanbieters ..... 453
Endpunkte von AWS IoT Device Management – Auftragsdaten ..... 454
Endpunkte von AWS IoT Device Management – Fleet Hub ..... 454
Endpunkte AWS IoT Device Management – Secure Tunneling ..... 455
Geräte verwalten ..... 456
Registrierung ..... 457
Ein Objekt erstellen ..... 457
Objekte auflisten ..... 458
Objekte beschreiben ..... 460
Ein Objekt aktualisieren ..... 461
Ein Objekt löschen ..... 461
Ein Prinzipal an ein Objekt anfügen ..... 462
Listet Dinge auf, die mit einem Principal verknüpft sind ..... 463
Listet die mit einer Sache verknüpften Prinzipale auf ..... 463
Listet Dinge auf, die mit einem Prinzipal V2 verknüpft sind ..... 464
Listet die mit einer Sache verknüpften Prinzipale auf V2 ..... 464
Ein Prinzipal von einem Objekt trennen ..... 465
Objekttypen ..... 466
Objekttyp erstellen ..... 466
Objekttypen auflisten ..... 467
Einen Objekttyp beschreiben ..... 468
Einen Objekttyp mit einem Objekt verknüpfen ..... 468
Aktualisiere einen Dingtyp ..... 469
Einen Objekttyp als veraltet einstufen ..... 469
Einen Objekttyp löschen ..... 471
Statische Objektgruppen ..... 471
Erstellen einer statischen Objektgruppe ..... 473
Beschreiben einer Objektgruppe ..... 474
Hinzufügen eines Objekts zu einer statischen Objektgruppe ..... 475
Entfernen eines Objekts aus einer statischen Objektgruppe ..... 476

Auflisten von Objekten in einer Objektgruppe ... 476
Auflisten von Objektgruppen ... 477
Auflisten von Gruppen für ein Objekt ... 479
Aktualisieren einer statischen Objektgruppe ... 480
Löschen einer Objektgruppe ... 480
Anfügen einer Richtlinie an eine statische Objektgruppe ... 481
Trennen einer Richtlinie von einer statischen Objektgruppe ... 482
Auflisten der an eine statische Objektgruppe angefügten Richtlinien ... 482
Auflisten der Gruppen für eine Richtlinie ... 482
Abrufen gültiger Richtlinien für ein Objekt ... 483
Test-Autorisierung für MQTT-Aktionen ... 484
Dynamische Objektgruppen ... 486
Anwendungsfälle dynamischer Dinggruppen ... 486
Erstellen einer dynamischen Objektgruppe ... 488
Beschreiben einer dynamischen Objektgruppe ... 489
Aktualisieren einer dynamischen Objektgruppe ... 490
Löschen einer dynamischen Objektgruppe ... 491
Einschränkungen dynamischer und statischer Dinggruppen ... 491
Einschränkungen dynamischer Dinggruppen ... 492
Eine Sache mit einer Verbindung verknüpfen ... 495
Anwendungsfälle ... 495
Wie ordne ich eine Sache einer Verbindung zu ... 496
Fügen Sie propagierende Attribute hinzu ... 499
AWS Management Console ... 500
AWS CLI ... 501
Markieren von Ressourcen ... 503
Grundlagen zu Tags (Markierungen) ... 503
Tag-Beschränkungen und -Einschränkungen ... 505
Tag mit Richtlinien IAM ... 505
Fakturierungsgruppen ... 508
Anzeigen von Kostenzuordnungs- und Nutzungsdaten ... 509
Sicherheit ... 511
Sicherheit in AWS IoT ... 512
Authentifizierung ... 513
Übersicht zum X.509-Zertifikat ... 513
Serverauthentifizierung ... 513

Client-Authentifizierung ... 518
Benutzerspezifische Authentifizierung und Autorisierung ... 560
Autorisierung ... 591
AWS Schulung und Zertifizierung ... 595
AWS IoT Core Richtlinien ... 595
Autorisieren von direkten Aufrufen von AWS Diensten mithilfe des AWS IoT Core Credential Providers ... 675
Kontenübergreifender Zugriff mit IAM ... 682
Datenschutz ... 684
Datenverschlüsselung in AWS IoT ... 686
Transportsicherheit in AWS IoT Core ... 686
Datenverschlüsselung ... 692
Identity and Access Management ... 693
Zielgruppe ... 694
Authentifizierung mit IAM-Identitäten ... 695
Verwalten des Zugriffs mit Richtlinien ... 698
Wie AWS IoT funktioniert mit IAM ... 701
Beispiele für identitätsbasierte Richtlinien ... 734
AWS verwaltete Richtlinien ... 739
Fehlerbehebung ... 754
Protokollieren und Überwachen ... 756
Überwachungstools ... 757
Compliance-Validierung ... 758
Ausfallsicherheit ... 760
Verwendung AWS IoT Core mit VPC-Endpunkten ... 761
VPC-Endpunkte für AWS IoT Core die Datenebene erstellen ... 761
Erstellen von VPC-Endpunkten für den AWS IoT Core -Anmeldeinformationsanbieter ... 762
Erstellen eines Amazon-VPC-Schnittstellenendpunkts ... 763
Konfigurieren einer privat gehosteten Zone ... 765
Steuerung des Zugriffs auf AWS IoT Core über VPC-Endpunkte ... 767
Einschränkungen ... 768
Skalierung von VPC-Endpunkten mit AWS IoT Core ... 769
Verwenden von benutzerdefinierten Domains mit VPC-Endpunkten ... 769
Verfügbarkeit von VPC-Endpunkten für AWS IoT Core ... 770
Sicherheit der Infrastruktur ... 770
Überwachung der Sicherheit ... 770

Bewährte Methoden für die Gewährleistung der Sicherheit ..... 771
Schutz von MQTT-Verbindungen in AWS IoT ..... 771
Synchronisieren der internen Uhr eines Geräts ..... 774
Überprüfen des Serverzertifikats ..... 775
Verwenden einer einzigen Identität pro Gerät ..... 775
Verwenden Sie eine Sekunde AWS-Region als Backup ..... 776
Just-in-Time-Bereitstellung nutzen ..... 776
Berechtigungen zum Ausführen von AWS IoT Device Advisor-Tests ..... 776
Confused-Deputy-Prävention im dienstübergreifenden Szenario für Device Advisor ..... 778
AWS Schulung und Zertifizierung ..... 779
Überwachen AWS IoT ..... 780
Konfigurieren Sie die AWS IoT Protokollierung ..... 781
Konfigurieren der Protokollierungsrolle und -richtlinie ..... 782
Konfigurieren der Standard-Protokollierung in AWS IoT (Konsole) ..... 784
Standardanmeldung konfigurieren AWS IoT (CLI) ..... 786
Konfigurieren der ressourcenspezifischen Protokollierung in AWS IoT (CLI) ..... 787
Protokollstufen ..... 791
Überwachen Sie AWS IoT Alarme und Messwerte mit Amazon CloudWatch ..... 791
AWS IoT Metriken verwenden ..... 792
CloudWatch Alarme erstellen ..... 792
Metriken und Dimensionen ..... 797
Überwachung AWS IoT mithilfe von Protokollen CloudWatch ..... 822
AWS IoT Protokolle in der CloudWatch Konsole anzeigen ..... 822
CloudWatch Protokolliert AWS IoT Protokolleinträge ..... 823
Geräteseitige Protokolle auf Amazon hochladen CloudWatch ..... 861
Funktionsweise ..... 861
Geräteseitige Protokolle mithilfe von AWS IoT -Regeln hochladen ..... 863
AWS IoT API-Aufrufe protokollieren ..... 873
AWS IoT Informationen in CloudTrail ..... 873
Grundlegendes zu AWS IoT Einträgen in Protokolldateien ..... 875
Regeln ..... 877
Gewähren von Zugriff ..... 878
Widerrufen Sie den Zugriff auf die Regelengine ..... 881
Berechtigungen zum Übergeben einer Rolle ..... 881
Erstellen einer Regel ..... 882
Erstellen Sie eine Regel (Konsole) ..... 884

Regel erstellen (CLI) ..... 885
Eine Regel verwalten ..... 890
Eine Regel taggen ..... 890
Eine Regel anzeigen ..... 891
Löschen einer Regel ..... 891
AWS IoT Regelaktionen ..... 892
Apache Kafka ..... 895
CloudWatch Alarme ..... 908
CloudWatch Logs ..... 910
CloudWatch Metriken ..... 912
DynamoDB ..... 915
Dynamo DBv2 ..... 918
Elasticsearch ..... 920
HTTP ..... 923
IoT Analytics ..... 965
AWS IoT Events ..... 967
AWS IoT SiteWise ..... 969
Firehose ..... 975
Kinesis Data Streams ..... 978
Lambda ..... 980
Ort ..... 984
OpenSearch ..... 987
Wiederveröffentlichen ..... 990
S3 ..... 994
Salesforce-IoT ..... 996
SNS ..... 997
SQS ..... 1000
Step Functions ..... 1002
Timestream ..... 1004
Fehlerbehebung bei einer Regel ..... 1012
Greifen Sie auf kontoübergreifende Ressourcen zu ..... 1012
Voraussetzungen ..... 1013
Kontoübergreifende Einrichtung für Amazon SQS ..... 1013
Kontoübergreifende Einrichtung für Amazon SNS ..... 1015
Kontoübergreifende Einrichtung für Amazon S3 ..... 1017
Kontoübergreifende Einrichtung für AWS Lambda ..... 1019

Fehlerbehandlung (Fehleraktion) ..... 1022
Nachrichtenformat für Fehleraktion ..... 1022
Beispiel für Fehleraktion ..... 1024
Basic Ingest ..... 1025
Verwenden von Basic Ingest ..... 1026
AWS IoT SQL-Referenz ..... 1027
SELECT-Klausel ..... 1028
FROM-Klausel ..... 1030
WHERE-Klausel ..... 1032
Datentypen ..... 1032
Operatoren ..... 1038
Funktionen ..... 1049
Literale ..... 1123
Case-Anweisungen ..... 1123
JSON-Erweiterungen ..... 1125
Ersetzungsvorlagen ..... 1127
Verschachtelte Objektabfragen ..... 1129
Binäre Nutzlasten ..... 1131
SQL-Versionen ..... 1138
Shadows ..... 1140
Verwendung von Schatten ..... 1140
Auswählen der Verwendung benannter oder unbenannter Schatten ..... 1141
Zugreifen auf Schatten ..... 1142
Verwenden von Schatten in Geräten, Apps und anderen Cloudservices ..... 1143
Nachrichtenreihenfolge ..... 1143
Kürzen von Shadow-Nachrichten ..... 1145
Verwenden von Schatten in Geräten ..... 1146
Initialisierung des Geräts bei der ersten Verbindung zu AWS IoT ..... 1147
Nachrichten werden verarbeitet, während das Gerät angeschlossen ist AWS IoT ..... 1150
Nachrichten werden verarbeitet, wenn das Gerät wieder eine Verbindung herstellt mit AWS IoT ..... 1151
Verwenden von Schatten in Apps und Services ..... 1151
Initialisierung der App oder des Dienstes bei der Verbindung zu AWS IoT ..... 1153
Der Verarbeitungsstatus ändert sich, während die App oder der Dienst verbunden ist AWS IoT ..... 1153
Erkennen, dass ein Gerät verbunden ist ..... 1153

Simulieren der Device Shadow-Servicekommunikation ..... 1155
Einrichten der Simulation ..... 1156
Initialisieren des Geräts ..... 1156
Senden einer Aktualisierung von der App ..... 1160
Reaktion auf eine Aktualisierung im Gerät ..... 1163
Beobachten Sie das Update in der App ..... 1168
Über die Simulation hinaus ..... 1169
Interaktion mit Schatten ..... 1170
Protokollunterstützung ..... 1170
Anforderungs- und Meldestatus ..... 1171
Aktualisieren eines Shadows ..... 1171
Abrufen eines Shadow-Dokuments ..... 1176
Löschen von Schattendaten ..... 1177
Geräteschatten-REST-API ..... 1180
GetThingShadow ..... 1181
UpdateThingShadow ..... 1182
DeleteThingShadow ..... 1183
ListNamedShadowsForThing ..... 1184
MQTT-Themen für Geräteschatten ..... 1186
/get ..... 1187
/get/accepted ..... 1188
/update/rejected ..... 1189
/update ..... 1190
/update/delta ..... 1191
/update/accepted ..... 1192
/update/documents ..... 1193
/update/rejected ..... 1194
/delete ..... 1195
/delete/accepted ..... 1196
/delete/rejected ..... 1197
Dokumente des Device Shadow-Services ..... 1198
Beispiele für Schatten-Dokumente ..... 1198
Dokumenteigenschaften ..... 1205
Delta-Status ..... 1206
Versioning von Schattendokumenten ..... 1208
Client-Tokens in Schattendokumenten ..... 1209

Eigenschaften des leeren Schattendokuments ... 1209
Array-Werte in Schattendokumenten ... 1210
Device Shadow-Fehlermeldungen ... 1211
Softwarepaket-Katalog ... 1213
Vorbereitung der Verwendung des Softwarepaket-Katalogs ... 1214
Lebenszyklus der Paketversion ... 1214
Namenskonventionen für Paketversionen ... 1216
Standardversion ... 1216
Versionsattribute ... 1216
Stückliste der Software ... 1217
Aktivierung der AWS IoT Flottenindizierung ... 1221
Reservierter benannter Schatten ... 1221
Löschen eines Softwarepakets ... 1223
Vorbereitung der Sicherheit ... 1223
Ressourcenbasierte Authentifizierung ... 1224
AWS IoT Berufsrechte für die Bereitstellung von Paketversionen ... 1225
AWS IoT Jobrechte zur Aktualisierung des reservierten benannten Schattens ... 1227
AWS IoT Jobs, Berechtigungen zum Herunterladen von Amazon S3 ... 1229
Berechtigungen zur Aktualisierung der Softwareliste für eine Paketversion ... 1229
Vorbereitung der Flottenindizierung ... 1232
Den `$package` Schatten als Datenquelle festlegen ... 1232
In der Konsole dargestellte Metriken ... 1233
Abfragemuster ... 1234
Sammeln der Paketversion und Verteilung über `getBucketsAggregation` ... 1237
AWS IoT Jobs vorbereiten ... 1237
Ersetzungsparameter für Jobs AWS IoT ... 1237
Vorbereitung des Auftragsdokuments und der Paketversion für die Bereitstellung ... 1242
Benennen der Pakete und Versionen bei der Bereitstellung ... 1246
Gezielte Jobsuche mithilfe AWS IoT dynamischer Dinggruppen ... 1246
Reservierte benannte Schatten- und Paketversionen ... 1247
Deinstallation eines Softwarepakets ... 1248
Erste Schritte ... 1248
Ein Paket und eine Version erstellen ... 1249
Bereitstellen einer Paketversion ... 1252
Zuordnen einer Paketversion ... 1254
Aufträge ... 1256

Auf AWS IoT Jobs zugreifen ..... 1256
AWS IoT Jobs, Regionen und Endpunkte ..... 1256
Was ist eine Fernsteuerung? ..... 1257
Vorteile der Verwendung von AWS IoT Device Management Jobs für Remote-Operationen ..... 1257
Was ist AWS IoT Jobs? ..... 1259
Wichtige Konzepte von Jobs ..... 1261
Aufträge und Status der Auftragsausführung ..... 1265
Verwalten von Aufträgen ..... 1270
Codesignatur für Aufgaben ..... 1271
Auftragsdokument ..... 1271
Vorsigniert URLs ..... 1271
Vorsignierte URL für den Datei-Upload ..... 1274
Vorsignierte URL mit Amazon S3 S3-Versionierung ..... 1275
Erstellen und Verwalten von Aufträgen mithilfe der Konsole ..... 1277
Erstellen und Verwalten von Aufträgen mithilfe des CLI. ..... 1280
Auftragsvorlagen ..... 1292
Benutzerdefinierte und AWS verwaltete Vorlagen ..... 1293
Verwenden Sie AWS verwaltete Vorlagen ..... 1293
Erstellen von benutzerdefinierten Auftragsvorlagen ..... 1314
Auftrags--Konfigurationen ..... 1323
Wie funktionieren Auftragskonfigurationen ..... 1324
Zusätzliche Konfigurationen angeben ..... 1340
Geräte und Aufträge ..... 1350
Programmieren von Geräten zur Arbeit mit Aufträgen ..... 1353
Geräteworkflow ..... 1354
Arbeitsablauf für Aufträge ..... 1356
Auftragsbenachrichtigungen ..... 1361
AWS IoT Jobs API-Operationen ..... 1369
Auftragsverwaltung und -steuerung API und Datentypen ..... 1372
Aufträge, Geräte, MQTT- und HTTPS-API-Operationen und Datentypen ..... 1392
Schutz der Benutzer und Geräte für Aufträge ..... 1407
Erforderlicher Richtlinientyp für Jobs AWS IoT ..... 1408
Autorisieren von Benutzern für Aufträge und Cloud-Services ..... 1409
Autorisieren von Geräten, Aufträge zu verwenden ..... 1422
AWS IoT Grenzwerte für Jobs ..... 1427

Grenzwerte für die Ausführung von Job ... 1427
Limits für aktive und gleichzeitige Aufträge ... 1429
Befehle ... 1434
Befehle, Konzepte und Status ... 1435
Befehle und wichtige Konzepte ... 1435
Status des Befehls ... 1437
Status der Befehlsausführung ... 1438
Arbeitsablauf für Befehle ... 1442
Befehle erstellen und verwalten ... 1443
Wählen Sie Ziele aus und abonnieren Sie Themen ... 1444
Befehlsausführungen starten und überwachen ... 1446
(Optional) Aktivieren Sie Benachrichtigungen für Befehlsereignisse ... 1447
Befehle erstellen und verwalten ... 1449
Erstellen Sie eine Befehlsressource ... 1449
Ruft Informationen zu einem Befehl ab ... 1453
Listen Sie Befehle in Ihrem auf AWS-Konto ... 1455
Aktualisieren Sie eine Befehlsressource ... 1457
Verwerfen Sie eine Befehlsressource oder stellen Sie sie wieder her ... 1459
Löschen Sie eine Befehlsressource ... 1460
Befehlsausführungen starten und überwachen ... 1462
Starten Sie die Ausführung eines Befehls ... 1463
Aktualisieren Sie das Ergebnis einer Befehlsausführung ... 1469
Rufen Sie die Ausführung eines Befehls ab ... 1476
Befehlsaktualisierungen mit dem MQTT-Testclient anzeigen ... 1479
Listet die Befehlsausführungen in Ihrem auf AWS-Konto ... 1481
Löschen Sie die Ausführung eines Befehls ... 1484
Eine Befehlsressource als veraltet kennzeichnen ... 1485
Wichtige Überlegungen ... 1486
Eine Befehlsressource (Konsole) als veraltet kennzeichnen ... 1486
Eine Befehlsressource (CLI) verwerfen ... 1486
Überprüfen Sie den Zeitpunkt und den Status der Deprecation ... 1487
Stellen Sie eine Befehlsressource wieder her ... 1488
Sicheres Tunneling ... 1489
Was ist Secure Tunneling? ... 1489
Secure Tunneling-Konzepte ... 1490
Wie funktioniert Secure Tunneling ... 1491

Sicherer Tunnellebenszyklus ... 1492
Secure Tunneling-Tutorials ... 1493
Tutorials in diesem Abschnitt ... 1494
Öffnen Sie einen Tunnel und starten Sie eine SSH-Sitzung zum Remote-Gerät ... 1495
Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen ... 1513
Lokaler Proxy ... 1518
Wie man den lokalen Proxy benutzt ... 1519
Konfigurieren Sie den lokalen Proxy für Geräte, die einen Web-Proxy verwenden ... 1526
Multiplexing und gleichzeitige TCP-Verbindungen ... 1534
Multiplexing mehrerer Datenströme ... 1535
Gleichzeitige TCP-Verbindungen verwenden ... 1539
Ein Remote-Gerät konfigurieren und IoT-Agent verwenden ... 1542
IoT-Agent-Snippet ... 1542
Steuern des Zugriffs auf Tunnel ... 1544
Voraussetzungen für den Tunnelzugriff ... 1544
Richtlinien für den Tunnelzugriff ... 1545
Lösung von Verbindungsproblemen beim Secure Tunneling ... 1552
Fehler beim ungültigen Client-Zugriffstoken ... 1553
Fehler bei Nichtübereinstimmung der Client-Tokens ... 1553
Verbindungsprobleme bei Remote-Geräten ... 1555
Gerätebereitstellung ... 1558
Bereitstellung von Geräten in AWS IoT ... 1559
Bereitstellung von Flotten APIs ... 1561
Bereitstellen von Geräten ohne Gerätezertifikate mithilfe der Flottenbereitstellung ... 1561
Bereitstellung durch Anspruch ... 1562
Bereitstellung durch vertrauenswürdigen Benutzer ... 1565
Verwenden von Pre-Provisioning-Hooks mit der AWS -CLI ... 1567
Bereitstellen von Geräten mit Gerätezertifikaten ... 1571
Bereitstellung eines einzelnen Objekts ... 1571
Just-in-time Bereitstellung ... 1572
Massenregistrierung ... 1579
Bereitstellen von Vorlagen ... 1580
Bereich "Parameters" ... 1580
Bereich „Ressourcen“ ... 1581
Vorlagenbeispiel für eine Massenregistrierung ... 1587

Beispiel für eine Vorlage für die just-in-time Bereitstellung (JITP) ... 1588
Flottenbereitstellung ... 1590
Pre-Provisioning-Hooks ... 1594
Pre-Provisioning-Hook-Eingabe ... 1595
Pre-Provisioning-Hook-Rückgabewert ... 1595
Lambda-Beispiel für einen Pre-Provisioning-Hook ... 1596
Selbstverwaltete Zertifikatsignierung mithilfe des Zertifikatsanbieters AWS IoT Core ... 1599
So funktioniert die selbstverwaltete Zertifikatsignierung bei der Flottenbereitstellung ... 1600
Eingabe der Lambda-Funktion des Zertifikatsanbieters ... 1602
Rückgabewert der Lambda-Funktion des Zertifikatsanbieters ... 1602
Beispiel-Lambda-Funktion ... 1602
Selbstverwaltete Zertifikatsignierung für die Flottenbereitstellung ... 1604
AWS CLI Befehle für den Zertifikatsanbieter ... 1606
Erstellen von IAM-Richtlinien und -Rollen für Benutzer, die ein Gerät installieren ... 1609
Erstellen einer IAM-Richtlinie für Benutzer, die ein Gerät installieren werden ... 1609
Erstellen einer IAM-Rolle für Benutzer, die ein Gerät installieren werden ... 1610
Aktualisieren einer vorhandenen Richtlinie, um eine neue Vorlage zu autorisieren ... 1611
MQTT-API für die Gerätebereitstellung ... 1613
CreateCertificateFromCsr ... 1613
CreateKeysAndCertificate ... 1616
RegisterThing ... 1618
-Flottenindizierung ... 1621
Verwalten von Indexaktualisierungen ... 1621
Verbindungsstatus für ein bestimmtes Gerät abfragen ... 1621
Datenquellenübergreifende Suche ... 1621
Abfragen von Aggregatdaten ... 1622
Überwachung aggregierter Daten und Erstellung von Alarmen mithilfe von Flottenkennzahlen 1622
Verwalten der Flottenindizierung ... 1622
Objektindizierung ... 1622
Modus für die Objektgruppenindizierung. ... 1624
Verwaltete Felder ... 1624
Benutzerdefinierte Felder ... 1626
Verwalten der Objektindizierung ... 1627
Verwalten der Objektgruppenindizierung ... 1644
Status der Gerätekonnektivität ... 1646
Funktionsweise ... 1646

Features ... 1646
Vorteile ... 1647
Voraussetzungen ... 1647
Beispiele ... 1648
Abfragen von Aggregatdaten ... 1649
GetStatistics ... 1650
GetCardinality ... 1653
GetPercentiles ... 1654
GetBucketsAggregation ... 1656
Autorisierung ... 1657
Abfragesyntax ... 1658
Unterstützte Features ... 1658
Nicht unterstützte Funktionen ... 1658
Hinweise ... 1659
Beispiel für Objektabfragen ... 1659
Beispiel für Objektgruppenabfragen ... 1664
Indexierung von Standortdaten ... 1665
Unterstützte Datumsformate ... 1666
Wie indexiert man Standortdaten ... 1667
Konfiguration der Objektindizierung. ... 1668
Beispiele für Geoqueries ... 1670
Erste Schritte-Tutorial ... 1671
Flottenmetriken ... 1676
Erste Schritte-Tutorial ... 1677
Verwalten von Flottenmetriken ... 1684
MQTTbasierte Dateibereitstellung ... 1692
Was ist ein Stream? ... 1692
Einen Stream verwalten ... 1693
Erteilen von Berechtigungen für Ihre Geräte ... 1694
Connect deine Geräte mit AWS IoT ... 1695
TagResource Verwendung ... 1696
Verwenden Sie die AWS IoT MQTT basierte Dateizustellung auf Geräten ... 1696
Wird verwendet DescribeStream , um Stream-Daten abzurufen ... 1697
Abrufen von Datenblöcken aus einer Stream-Datei ... 1699
Behandlung von Fehlern bei der AWS IoT MQTT basierten Dateizustellung ... 1706
Ein Beispiel für einen Anwendungsfall in Free RTOS OTA ... 1708

Device Advisor ..... 1709
Einrichtung ..... 1711
Erstellen eines IoT-Dings ..... 1711
Erstellen Sie eine IAM Rolle, die Sie als Ihre Geräterolle verwenden möchten ..... 1711
Erstellen Sie eine individuell verwaltete Richtlinie für einen IAM Benutzer zur Verwendung von Device Advisor ..... 1715
Erstellen Sie einen IAM Benutzer für die Verwendung von Device Advisor ..... 1715
Konfigurieren Ihres Geräts ..... 1718
Erste Schritte mit Device Advisor in der Konsole ..... 1720
Device-Advisor-Workflow ..... 1729
Voraussetzungen ..... 1729
Erstellen einer Testsuite-Definition ..... 1729
Abrufen einer Testsuite-Definition ..... 1732
Abrufen eines Testendpunkts ..... 1733
Ausführen einer Testsuite ..... 1733
Abrufen einer Testsuite-Ausführung ..... 1734
Beenden einer Testsuite-Ausführung ..... 1734
Abrufen eines Qualifizierungsberichts für eine erfolgreiche Ausführung der Qualifizierungstestsuite ..... 1735
Ausführlicher Konsolen-Workflow von Device Advisor ..... 1736
Voraussetzungen ..... 1736
Erstellen einer Testsuite-Definition ..... 1736
Ausführen einer Testsuite ..... 1744
Beenden einer Testsuite-Ausführung (optional) ..... 1746
Anzeigen von Details und Protokolle der Testsuite-Ausführung ..... 1748
Herunterladen eines AWS IoT -Qualifikationsberichts ..... 1750
Konsolen-Workflow für Tests mit langer Dauer ..... 1750
Device VPC Advisor-Endpunkte ()AWS PrivateLink ..... 1759
Überlegungen zu Endpunkten AWS IoT Core Device Advisor VPC ..... 1760
Erstellen Sie einen VPC Schnittstellenendpunkt für AWS IoT Core Device Advisor ..... 1761
Kontrolle des Zugriffs auf AWS IoT Core Device Advisor mehrere VPC Endpunkte ..... 1761
Device-Advisor-Testfälle ..... 1763
Device Advisor-Testfälle, um sich für das AWS Gerätequalifizierungsprogramm zu qualifizieren. ..... 1763
TLS ..... 1764
MQTT ..... 1771

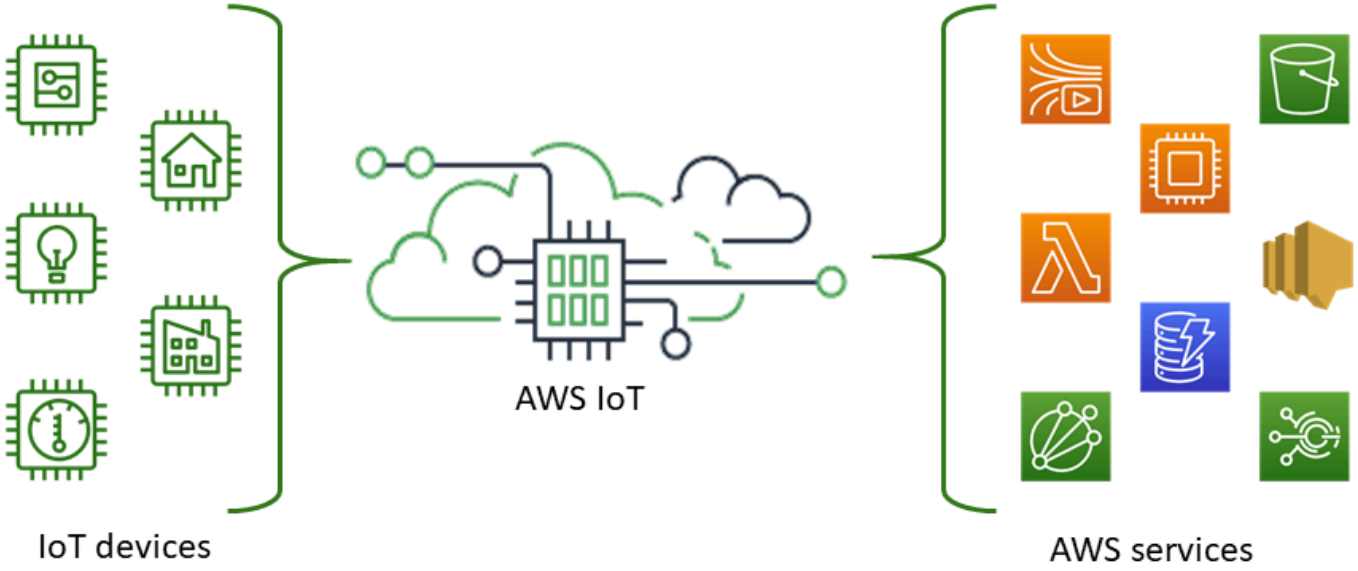
Shadow ... 1786
Auftragsausführung ... 1788
Berechtigungen und Richtlinien ... 1790
Tests mit langer Dauer ... 1791
Standort des Geräts ... 1809
Messungstypen und Solver ... 1809
So funktioniert der AWS IoT Core Gerätestandort ... 1811
Wie benutzt man den Gerätestandort AWS IoT Core ... 1812
Auflösen des Standorts von IoT-Geräten ... 1813
Auflösen des Gerätestandorts (Konsole) ... 1813
Gerätestandort wird aufgelöst () API ... 1817
Fehlerbehebung beim Auflösen des Standorts ... 1819
Auflösen des Gerätestandorts mithilfe von Themen MQTT ... 1820
Format der MQTT Themen zum Gerätestandort ... 1820
Richtlinien für MQTT Themen zum Gerätestandort ... 1821
Themen zum Gerätestandort und Nutzlast ... 1823
Location Solver und Geräte-Payload ... 1828
WLAN-basierter Solver ... 1828
Solver auf Mobilfunkbasis ... 1829
IP-Reverse-Lookup-Solver ... 1834
GNSSSolver ... 1835
Ereignismeldungen ... 1837
Generieren von Ereignisnachrichten ... 1837
Richtlinie für den Empfang von Ereignisnachrichten ... 1837
Ereignisse aktivieren für AWS IoT ... 1838
Registry-Ereignisse ... 1843
Objektereignisse ... 1843
Objekttypereignisse ... 1845
Objektgruppenereignisse ... 1849
Auftragsereignisse ... 1854
Ereignisse im Lebenszyklus ... 1859
„Verbinden/Verbindung trennen“-Ereignisse ... 1860
Ereignis mit fehlgeschlagenem Verbindungsversuch ... 1864
„Abonnieren/Abonnement beenden“-Ereignisse ... 1866
Fehlerbehebung ... 1868
AWS IoT Core Anleitung zur Fehlerbehebung ... 1868

Diagnostizieren von Verbindungsproblemen ... 1869
Fehler bei der Regeldiagnose ... 1873
Diagnostizieren von Problemen mit Schatten ... 1875
Problemdiagnose bei Salesforce-Aktionen ... 1877
Diagnostizieren von Stream-Limits ... 1879
Behebung von Verbindungsabbrüchen bei Geräteflotten ... 1879
AWS IoT Device Management Leitfaden zur Fehlerbehebung ... 1880
AWS IoT Problembehebung bei Jobs ... 1881
Fehlerbehebung bei der Flottenindizierung ... 1886
AWS IoT Fehlerbehebung im Geräteverwaltungs-Softwarepaketkatalog ... 1889
AWS IoT Leitfaden zur Fehlerbehebung in Device Advisor ... 1896
AWS IoT Fehler ... 1899
AWS IoT Geräte SDKs - SDKs, Mobil- und AWS IoT Geräteclient ... 1901
AWS IoT Gerät SDKs ... 1901
AWS IoT Geräte-SDK für Embedded C ... 1904
AWS Mobil SDKs ... 1904
AWS IoT Geräteclient ... 1905
Frühere AWS IoT Geräteversionen SDKs ... 1906
Codebeispiele ... 1907
Grundlagen ... 1913
Hallo AWS IoT ... 1914
Erlernen der Grundlagen ... 1919
Aktionen ... 1975
AWS IoT-Kontingente ... 2038
AWS IoT Core – Preise ... 2039
... mmxl

# Was ist AWS IoT?

AWS IoT stellt die Cloud-Dienste bereit, die Ihre IoT-Geräte mit anderen Geräten und AWS Cloud-Diensten verbinden. AWS IoT bietet Gerätesoftware, mit der Sie Ihre IoT-Geräte in AWS IoT basierte Lösungen integrieren können. Wenn Ihre Geräte eine Verbindung herstellen können AWS IoT, AWS IoT können Sie sie mit den bereitgestellten Cloud-Diensten verbinden. AWS

Eine praktische Einführung zu finden Sie AWS IoT unterErste-Schritte-Tutorials.




Mit AWS IoT können Sie die für Ihre Lösung am besten geeigneten up-to-date Technologien auswählen. Unterstützt die folgenden Protokolle, um Sie bei der Verwaltung und Unterstützung Ihrer IoT-Geräte vor Ort zu AWS IoT Core unterstützen:

- MQTT (Message Queuing und Telemetrietransport)
- MQTT über WSS (Websockets Secure)
- HTTPS (Hypertext Transfer Protocol – Secure)
- LoRaWAN (Weitbereichsnetzwerk mit großer Reichweite)

Der AWS IoT Core Message Broker unterstützt Geräte und Clients, die die Protokolle MQTT und MQTT über WSS verwenden, um Nachrichten zu veröffentlichen und zu abonnieren. Er unterstützt auch Geräte und Clients, die das HTTPS-Protokoll zum Veröffentlichen von Nachrichten verwenden.

AWS IoT Core for LoRa WAN hilft Ihnen dabei, WLAN-Geräte (Low-Power LoRa Long-range Wide Area Network) zu verbinden und zu verwalten. AWS IoT Core für LoRa WAN entfällt die Notwendigkeit, einen LoRa WAN-Netzwerkserver (LNS) zu entwickeln und zu betreiben.

Wenn Sie AWS IoT Funktionen wie Gerätekommunikation, Regeln oder Aufgaben nicht benötigen, finden Sie unter AWS Messaging Informationen zu anderen AWS IoT Messaging-Diensten, die Ihren Anforderungen möglicherweise besser entsprechen.

## So greifen Ihre Geräte und Apps darauf zu AWS IoT

AWS IoT bietet die folgenden Schnittstellen fürAWS IoT Anleitungen:

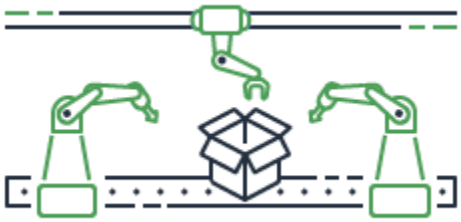
- AWS IoT Gerät SDKs — Erstellen Sie auf Ihren Geräten Anwendungen, die Nachrichten an senden und von AWS IoT denen Nachrichten empfangen werden. Weitere Informationen finden Sie unter AWS IoT Geräte SDKs - SDKs, Mobil- und AWS IoT Geräteclient.
- AWS IoT Core für LoRa WAN — Connect und verwalten Sie Ihre WAN-Geräte und -Gateways mit großer Reichweite, indem Sie AWS IoT Core for LoRa LoRa WAN verwenden.
- AWS Command Line Interface (AWS CLI) — Befehle für AWS IoT Windows, macOS und Linux ausführen. Diese Befehle ermöglichen Ihnen die Erstellung und Verwaltung von Dingobjekten, Zertifikaten, Regeln, Jobs und Richtlinien. Informationen zu den ersten Schritten finden Sie im AWS Command Line Interface -Benutzerhandbuch. Weitere Informationen zu den Befehlen für AWS IoT finden Sie unter iot in der AWS CLI Befehlsreferenz.
- AWS IoT API — Erstellen Sie Ihre IoT-Anwendungen mithilfe von HTTP- oder HTTPS-Anfragen. Diese API-Aktionen ermöglichen Ihnen die programmgesteuerte Erstellung und Verwaltung von Objekten, Zertifikaten, Regeln und Richtlinien. Weitere Informationen zu den API-Aktionen für AWS IoT finden Sie unter Aktionen in der AWS IoT API-Referenz.
- AWS SDKs—Erstellen Sie Ihre IoT-Anwendungen APIs sprachspezifisch. Diese umfassen SDKs die HTTP/HTTPS-API und ermöglichen es Ihnen, in jeder der unterstützten Sprachen zu programmieren. Weitere Informationen finden Sie unter AWS SDKs und Tools.

Sie können auch AWS IoT über die AWS IoT Konsole darauf zugreifen, die eine grafische Benutzeroberfläche (GUI) bietet, über die Sie die Ding-Objekte, Zertifikate, Regeln, Jobs, Richtlinien und andere Elemente Ihrer IoT-Lösungen konfigurieren und verwalten können.

# Was AWS IoT kann ich tun

In diesem Thema werden einige der von AWS IoT unterstützten Lösungen beschrieben, die Sie möglicherweise benötigen.

## IoT



Dies sind einige Beispiele für AWS IoT Lösungen für industrielle Anwendungsfälle, bei denen IoT-Technologien eingesetzt werden, um die Leistung und Produktivität industrieller Prozesse zu verbessern.

Lösungen für industrielle Anwendungsfälle

- Wird verwendet AWS IoT , um prädiktive Qualitätsmodelle in industriellen Betrieben zu erstellen

  Erfahren Sie, wie AWS IoT Sie Daten aus Industriebetrieben sammeln und analysieren können, um prädiktive Qualitätsmodelle zu erstellen. Weitere Informationen
- Wird AWS IoT zur Unterstützung der vorausschauenden Wartung in Industriebetrieben verwendet

  Erfahren Sie, wie Sie bei der Planung präventiver Wartungsarbeiten helfen AWS IoT können, um ungeplante Ausfallzeiten zu reduzieren. Weitere Informationen

## IoT in der Hausautomation

Dies sind einige Beispiele für AWS IoT Lösungen für Anwendungsfälle in der Hausautomation, bei denen IoT-Technologien eingesetzt werden, um skalierbare IoT-Anwendungen zu entwickeln, die Haushaltsaktivitäten mithilfe von vernetzten Heimgeräten automatisieren.

Lösungen für die Hausautomation

- Verwenden Sie es AWS IoT in Ihrem vernetzten Zuhause

  Erfahren Sie, wie AWS IoT Sie integrierte Hausautomationslösungen anbieten können.
- Wird verwendet AWS IoT , um Sicherheit und Überwachung zu Hause zu gewährleisten

  Erfahren Sie, wie AWS IoT Sie maschinelles Lernen und Edge-Computing auf Ihre Hausautomationslösung anwenden können.

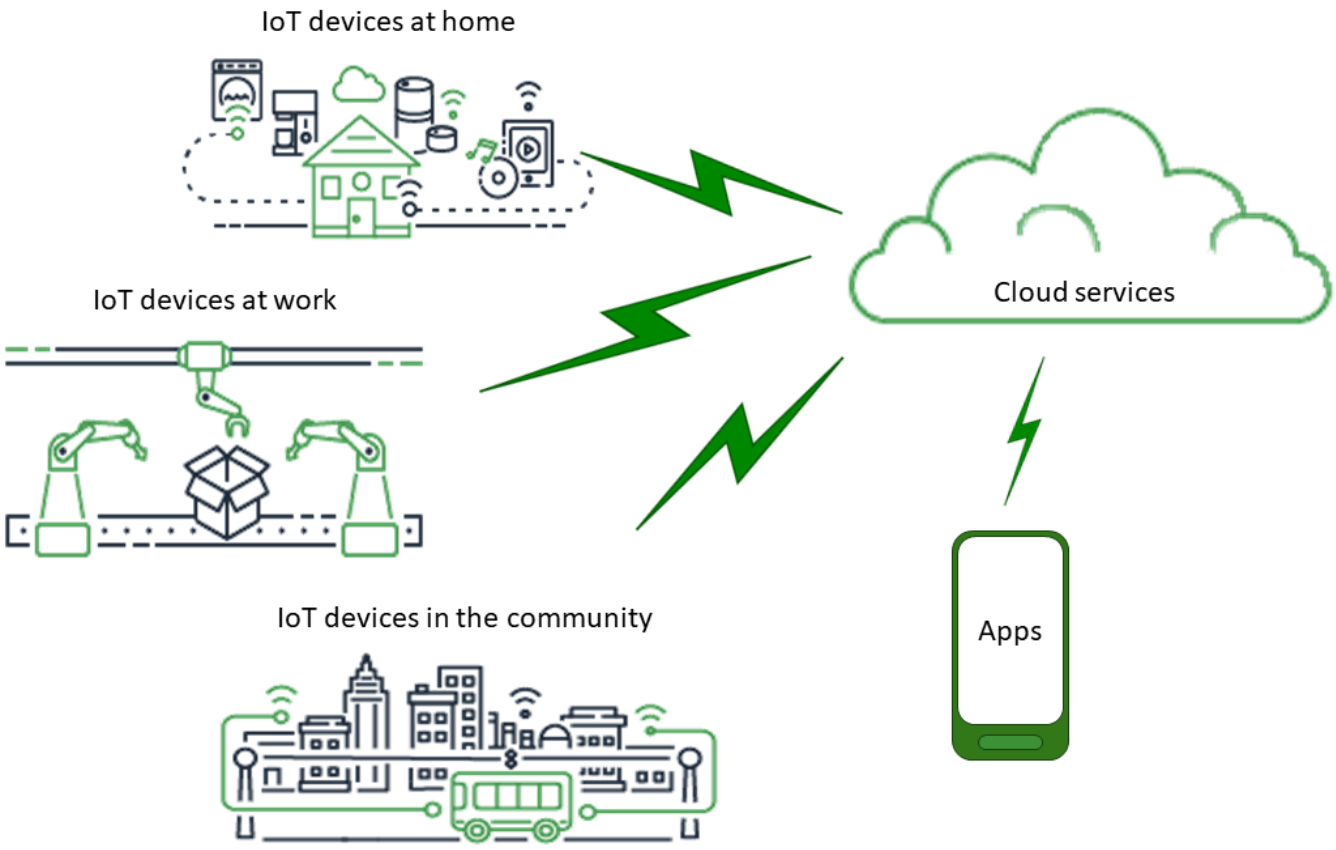
Eine Liste von Lösungen für industrielle, private und kommerzielle Anwendungsfälle finden Sie im AWS IoT Solution Repository.

# Wie AWS IoT funktioniert

AWS IoT bietet Cloud-Dienste und Geräteunterstützung, mit denen Sie IoT-Lösungen implementieren können. AWS bietet viele Cloud-Dienste zur Unterstützung IoT-basierter Anwendungen. Damit Sie verstehen, wo Sie anfangen sollen, bietet dieser Abschnitt ein Diagramm und eine Definition der wichtigsten Konzepte, um Sie in das IoT-Universum einzuführen.

## Das IoT-Universum

Im Allgemeinen besteht das Internet der Dinge (IoT) aus den in diesem Diagramm gezeigten Schlüsselkomponenten.




## Apps

Apps bieten Endbenutzern Zugriff auf IoT-Geräte und die Funktionen, die von den Cloud-Diensten bereitgestellt werden, mit denen diese Geräte verbunden sind.

## Cloud-Dienste

Cloud-Dienste sind verteilte, groß angelegte Datenspeicher- und Verarbeitungsdienste, die mit dem Internet verbunden sind. Beispiele sind unter anderem:

- IoT-Verbindungs- und Verwaltungsdienste

  AWS IoT ist ein Beispiel für einen IoT-Verbindungs- und Verwaltungsdienst.
- Rechendienste wie Amazon Elastic Compute Cloud und AWS Lambda
- Datenbankdienste wie Amazon DynamoDB.

## Kommunikation

Geräte kommunizieren mithilfe verschiedener Technologien und Protokolle mit Cloud-Diensten. Beispiele sind unter anderem:

- Wi-Fi/Breitband-Internet
- Breitband-Mobilfunkdaten
- Schmalband-Mobilfunkdaten
- Wide Area Network (LoRaWAN) mit großer Reichweite
- Proprietäre HF-Kommunikation

## Geräte

Ein Gerät ist eine Art von Hardware, die Schnittstellen und Kommunikation verwaltet. Geräte befinden sich normalerweise in unmittelbarer Nähe der realen Schnittstellen, die sie überwachen und steuern. Geräte können Rechen- und Speicherressourcen wie Mikrocontroller, CPUs und Speicher enthalten. Beispiele sind unter anderem:

- Raspberry Pi
- Arduino
- Assistenten für Sprachschnittstellen
- LoRaWAN und Geräte
- Amazon-Sidewalk-Geräte
- Maßgeschneiderte IoT-Geräte

## Schnittstellen

Eine Schnittstelle ist eine Komponente, die ein Gerät mit der physischen Welt verbindet.

- Benutzeroberflächen

  Komponenten, mit denen Geräte und Benutzer miteinander kommunizieren können.

  - Eingangsschnittstellen

    Ermöglichen Sie einem Benutzer die Kommunikation mit einem Gerät

Beispiele: Tastatur, Knopf

- Eingangsschnittstellen

  Ermöglichen Sie einem Benutzer die Kommunikation mit einem Gerät

  Beispiele: alphanumerisches Display, grafisches Display, Kontrollleuchte, Alarmglocke

- Sensoren

  Eingabekomponenten, die etwas in der Außenwelt so messen oder wahrnehmen, dass ein Gerät es versteht. Beispiele sind unter anderem:

  - Temperatursensor (wandelt die Temperatur in ein analoges oder digitales Signal um)
  - Feuchtigkeitssensor (wandelt die relative Luftfeuchtigkeit in ein analoges oder digitales Signal um)
  - Analog-Digital-Wandler (wandelt eine analoge Spannung in einen numerischen Wert um)
  - Ultraschall-Entfernungsmessgerät (wandelt eine Entfernung in einen numerischen Wert um)
  - Optischer Sensor (wandelt eine Lichtstärke in einen numerischen Wert um)
  - Kamera (wandelt Bilddaten in digitale Daten um)

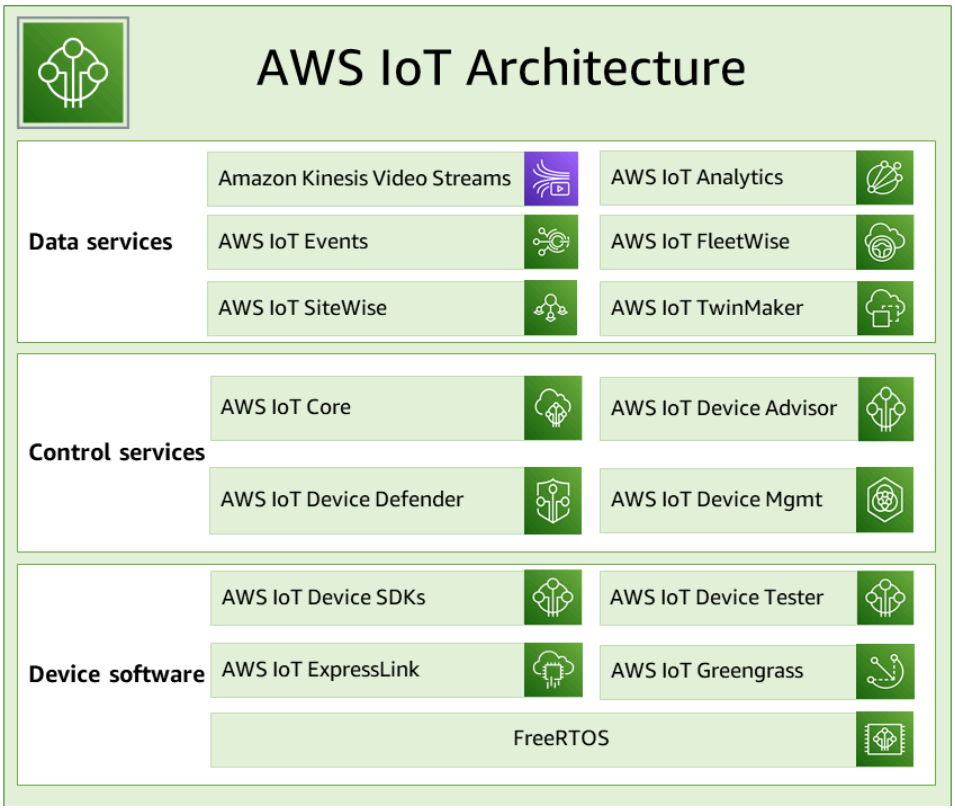
- Aktuator

  Ausgabekomponenten, mit denen das Gerät etwas in der Außenwelt steuern kann. Beispiele sind unter anderem:

  - Schrittmotoren (wandeln elektrische Signale in Bewegung um)
  - Relais (steuern hohe elektrische Spannungen und Ströme)

## AWS IoT Dienstleistungen im Überblick

AWS IoT Stellt im IoT-Universum die Dienste bereit, die die Geräte unterstützen, die mit der Welt interagieren, und die Daten, die zwischen ihnen ausgetauscht werden, und AWS IoT. AWS IoT besteht aus den in dieser Abbildung gezeigten Diensten zur Unterstützung Ihrer IoT-Lösung.




## AWS IoT Gerätesoftware

AWS IoT stellt diese Software zur Unterstützung Ihrer IoT-Geräte bereit.

AWS IoT Gerät SDKs

Das AWS IoT Gerät und das Handy SDKs helfen Ihnen dabei, Ihre Geräte effizient miteinander zu verbinden AWS IoT. The AWS IoT Device and Mobile SDKs umfasst Open-Source-Bibliotheken, Entwicklerhandbücher mit Beispielen und Portierungsleitfäden, sodass Sie innovative IoT-Produkte oder -Lösungen auf den Hardwareplattformen Ihrer Wahl entwickeln können.

AWS IoT Device Tester

AWS IoT Device Testerfür FreeRTOS und AWS IoT Greengrass ist ein Testautomatisierungstool für Mikrocontroller. AWS IoT Device Tester testet Ihr Gerät, um festzustellen, ob es FreeRTOS oder oder Dienste ausführen kann AWS IoT Greengrass und ob es mit Diensten zusammenarbeitet. AWS IoT

AWS IoT ExpressLink

AWS IoT ExpressLink unterstützt eine Reihe von Hardwaremodulen, die von Partnern entwickelt und angeboten werden.AWS Zu den Konnektivitätsmodulen gehört AWS validierte Software,

mit der Sie Geräte schneller und einfacher mit der Cloud verbinden und problemlos in eine Reihe von AWS Diensten integrieren können. Weitere Informationen finden Sie auf der AWS IoT ExpressLinkÜbersichtsseite oder im AWS IoT ExpressLink Programmierhandbuch.

AWS IoT Greengrass

AWS IoT Greengrasserstreckt sich AWS IoT auf Edge-Geräte, sodass diese lokal auf die von ihnen generierten Daten reagieren, Vorhersagen auf der Grundlage von Modellen für maschinelles Lernen treffen und Gerätedaten filtern und aggregieren können. AWS IoT Greengrass ermöglicht es Ihren Geräten, Daten näher am Ort ihrer Entstehung zu sammeln und zu analysieren, selbstständig auf lokale Ereignisse zu reagieren und sicher mit anderen Geräten im lokalen Netzwerk zu kommunizieren. Sie können Edge-Anwendungen mithilfe von vorgefertigten Softwaremodulen, sogenannten Komponenten, erstellen, die Ihre Edge-Geräte mit AWS Diensten oder Diensten von Drittanbietern verbinden können. AWS IoT Greengrass

FreeRTOS

FreeRTOS ist ein Open-Source-Echtzeitbetriebssystem für Mikrocontroller, mit dem Sie kleine Edge-Geräte mit geringem Stromverbrauch in Ihre IoT-Lösung integrieren können. FreeRTOS umfasst einen Kernel und eine wachsende Anzahl von Softwarebibliotheken, die viele Anwendungen unterstützen. FreeRTOS-Systeme können kleine Geräte mit geringem Stromverbrauch sicher mit AWS IoT verbinden und leistungsstärkere Edge-Geräte unterstützen, die AWS IoT Greengrass ausführen.

## AWS IoT Dienste steuern

Connect zu den folgenden AWS IoT Diensten her, um die Geräte in Ihrer IoT-Lösung zu verwalten.

AWS IoT Core

AWS IoT Coreist ein verwalteter Cloud-Dienst, der es verbundenen Geräten ermöglicht, sicher mit Cloud-Anwendungen und anderen Geräten zu interagieren. AWS IoT Core kann viele Geräte und Nachrichten unterstützen und diese Nachrichten verarbeiten und an AWS IoT Endpunkte und andere Geräte weiterleiten. Mit AWS IoT Core können Ihre Anwendungen mit all Ihren Geräten interagieren, auch wenn sie nicht verbunden sind.

AWS IoT Core Geräte-Ratgeber

AWS IoT Core Device Advisor ist eine cloudbasierte, vollständig verwaltete Testfunktion zur Validierung von IoT-Geräten während der Entwicklung von Gerätesoftware. Device Advisor

bietet vorgefertigte Tests, mit denen Sie IoT-Geräte auf zuverlässige und sichere Konnektivität überprüfen können AWS IoT Core, bevor Sie Geräte in der Produktion einsetzen.

AWS IoT Device Defender

AWS IoT Device Defender hilft Ihnen, Ihre IoT-Geräteflotte zu schützen. AWS IoT Device Defender überprüft Ihre IoT-Konfigurationen kontinuierlich, um sicherzustellen, dass sie nicht von den bewährten Sicherheitsmethoden abweichen. AWS IoT Device Defender sendet eine Warnung, wenn es Lücken in Ihrer IoT-Konfiguration erkennt, die ein Sicherheitsrisiko darstellen könnten, z. B. wenn Identitätszertifikate von mehreren Geräten gemeinsam genutzt werden oder wenn ein Gerät mit einem widerrufenen Identitätszertifikat versucht, eine Verbindung herzustellen. AWS IoT Core

AWS IoT Geräteverwaltung

AWS IoT Mithilfe der Geräteverwaltungsdienste können Sie die Vielzahl der verbundenen Geräte, aus denen sich Ihre Geräteflotten zusammensetzen, verfolgen, überwachen und verwalten. AWS IoT Mithilfe von Geräteverwaltungsdiensten können Sie sicherstellen, dass Ihre IoT-Geräte nach ihrer Bereitstellung ordnungsgemäß und sicher funktionieren. Sie bieten auch sicheres Tunneling für den Zugriff auf Ihre Geräte, die Überwachung ihres Zustands, die Erkennung und Behebung von Problemen aus der Ferne sowie Dienste zur Verwaltung von Gerätesoftware- und Firmware-Updates.

## AWS IoT Datendienste

Analysieren Sie die Daten der Geräte in Ihrer IoT-Lösung und ergreifen Sie geeignete Maßnahmen, indem Sie die folgenden AWS IoT Dienste nutzen.

Amazon Kinesis Video Streams

Mit Amazon Kinesis Video Streams können Sie Live-Videos von Geräten in die AWS Cloud streamen, wo sie dauerhaft gespeichert, verschlüsselt und indexiert werden, sodass Sie auf Ihre Daten zugreifen können. easy-to-use APIs Sie können mit Amazon Kinesis Video Streams enorme Mengen an Live-Videodaten aus Millionen von Quellen erfassen, darunter Smartphones, Sicherheitskameras, Webcams sowie Kameras in Fahrzeugen, Drohnen und anderen Geräten. Amazon Kinesis Video Streams ermöglicht Ihnen die Wiedergabe von Videos zur Live- und On-Demand-Ansicht und die schnelle Erstellung von Anwendungen, die durch die Integration mit Amazon Rekognition Video und Bibliotheken für ML-Frameworks die Vorteile von Computer Vision und Videoanalysen nutzen. Sie können außer Videodaten auch andere zeitlich serialisierte Daten senden, wie beispielsweise Audiodaten, Wärmebilder, Tiefendaten, RADAR-Daten usw.

### Amazon Kinesis Video Streams mit WebRTC

Amazon Kinesis Video Streams mit WebRTC bietet eine standardkonforme WebRTC-Implementierung als vollständig verwaltete Funktion. Sie können Amazon Kinesis Video Streams mit WebRTC verwenden, um Medien sicher live zu streamen oder bidirektionale Audio- oder Videointeraktionen zwischen beliebigen Kamera-IoT-Geräten und WebRTC-kompatiblen Mobil- oder Webplayern durchzuführen. Da es sich um eine vollständig verwaltete Funktion handelt, müssen Sie keine WebRTC-bezogene Cloud-Infrastruktur wie Signal- oder Media-Relay-Server aufbauen, betreiben oder skalieren, um Medien sicher über Anwendungen und Geräte zu streamen. Mit Amazon Kinesis Video Streams mit WebRTC können Sie ganz einfach Anwendungen für peer-to-peer Live-Medienstreaming oder Audio- oder Videointeraktivität in Echtzeit zwischen Kamera-IoT-Geräten, Webbrowsern und Mobilgeräten für eine Vielzahl von Anwendungsfällen erstellen.

### AWS IoT Analytik

AWS IoT Mit Analytics können Sie anspruchsvolle Analysen für riesige Mengen unstrukturierter IoT-Daten effizient ausführen und operationalisieren. AWS IoT Analytics automatisiert jeden schwierigen Schritt, der zur Analyse von Daten von IoT-Geräten erforderlich ist. AWS IoT Analytics filtert, transformiert und reichert IoT-Daten an, bevor sie zur Analyse in einem Zeitreihendatenspeicher gespeichert werden. Sie können Ihre Daten analysieren, indem Sie einmalige oder geplante Abfragen mit dem integrierten SQL-Abfrage-Engine oder maschinellem Lernen ausführen.

### AWS IoT Events

AWS IoT Events erkennt Ereignisse von IoT-Sensoren und -Anwendungen und reagiert darauf. Ereignisse sind Datenmuster, die kompliziertere Umstände als erwartet identifizieren, z. B. Bewegungsmelder, die Bewegungssignale verwenden, um Lichter und Sicherheitskameras zu aktivieren. AWS IoT Events überwacht kontinuierlich Daten von mehreren IoT-Sensoren und -Anwendungen und lässt sich in andere Dienste wie IoT AWS IoT Core SiteWise, DynamoDB und andere integrieren, um eine Früherkennung und einzigartige Einblicke zu ermöglichen.

### AWS IoT FleetWise

AWS IoT FleetWiseist ein verwalteter Dienst, mit dem Sie Fahrzeugdaten nahezu in Echtzeit sammeln und in die Cloud übertragen können. Damit AWS IoT FleetWise können Sie auf einfache Weise Daten von Fahrzeugen sammeln und organisieren, die unterschiedliche Protokolle und Datenformate verwenden. AWS IoT FleetWise hilft dabei, Nachrichten auf niedriger Ebene in für Menschen lesbare Werte umzuwandeln und das Datenformat in der Cloud für Datenanalysen

zu standardisieren. Sie können auch Datenerfassungsschemata definieren, um zu kontrollieren, welche Daten in Fahrzeugen gesammelt und wann sie in die Cloud übertragen werden sollen.

AWS IoT SiteWise

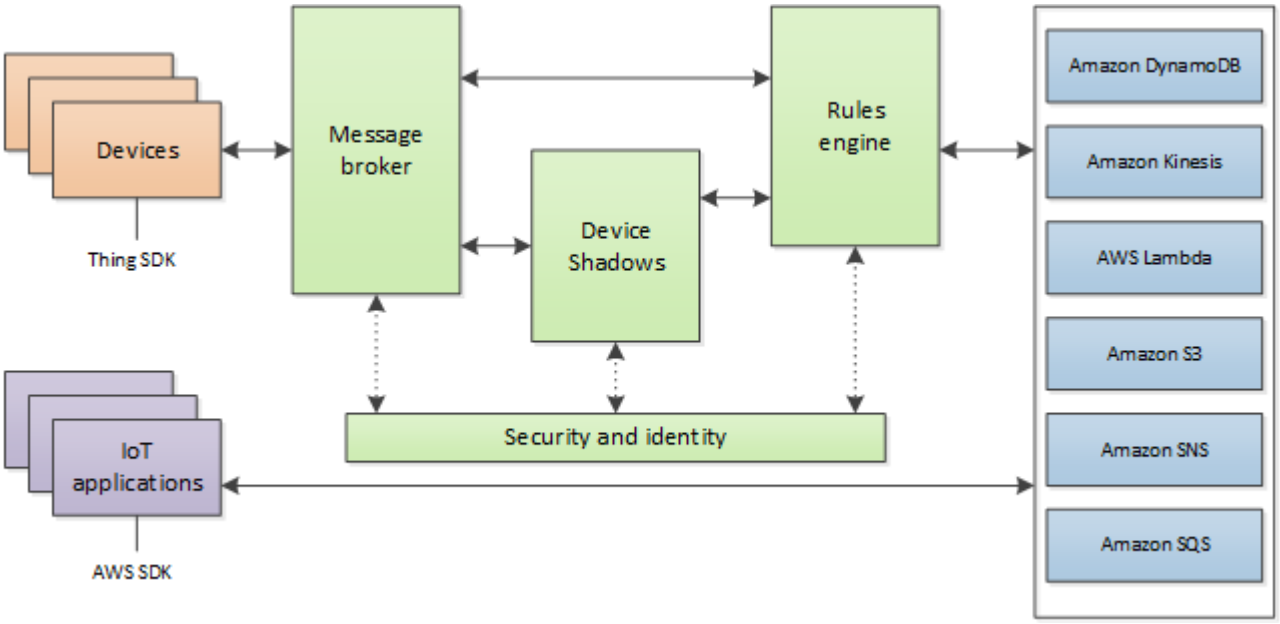
AWS IoT SiteWisesammelt, speichert, organisiert und überwacht Daten, die von Industrieanlagen per MQTT-Nachrichten oder in großem Maßstab übertragen werden, indem Software bereitgestellt wird, die auf APIs einem Gateway in Ihren Einrichtungen ausgeführt wird. Das Gateway stellt eine sichere Verbindung zu Ihren lokalen Datenservern her und automatisiert den Prozess der Erfassung und Organisation der Daten sowie deren Übertragung an die Cloud. AWS

AWS IoT TwinMaker

AWS IoT TwinMakererstellt betriebsbereite digitale Zwillinge aus physischen und digitalen Systemen. AWS IoT TwinMaker erstellt digitale Visualisierungen mithilfe von Messungen und Analysen aus einer Vielzahl von realen Sensoren, Kameras und Unternehmensanwendungen, damit Sie den Überblick über Ihre physische Fabrik, Ihr Gebäude oder Ihre Industrieanlage behalten. Sie können reale Daten verwenden, um den Betrieb zu überwachen, Fehler zu diagnostizieren und zu korrigieren und den Betrieb zu optimieren.

## AWS IoT Core Dienstleistungen

AWS IoT Core stellt die Dienste bereit, die Ihre IoT-Geräte mit der AWS Cloud verbinden, sodass andere Cloud-Dienste und -Anwendungen mit Ihren mit dem Internet verbundenen Geräten interagieren können.



Im nächsten Abschnitt werden die einzelnen in der Abbildung gezeigten AWS IoT Core Dienste beschrieben.

## AWS IoT Core Messaging-Dienste

Die AWS IoT Core Konnektivitätsdienste bieten eine sichere Kommunikation mit den IoT-Geräten und verwalten die Nachrichten, die zwischen ihnen und übertragen AWS IoT werden.

Device Gateway

Ermöglicht Geräten die sichere und effiziente Kommunikation mit AWS IoT. Die Gerätekommunikation wird durch sichere Protokolle gesichert, die X.509-Zertifikate verwenden.

Message Broker

Bietet einen sicheren Mechanismus für Geräte und AWS IoT Anwendungen, um Nachrichten voneinander zu veröffentlichen und zu empfangen. Sie können entweder das MQTT-Protokoll direkt oder MQTT-Over WebSocket zum Veröffentlichen und Abonnieren verwenden. Weitere Informationen zu von AWS IoT unterstützten Protokollen und Ports finden Sie unter the section called “Gerätekommunikationsprotokolle”. Geräte und Clients können auch die HTTP-REST-Schnittstelle verwenden, um Daten im Message Broker zu veröffentlichen.

Der Message Broker verteilt Gerätedaten an Geräte, die ihn abonniert haben, und an andere AWS IoT Core Dienste wie den Device Shadow-Dienst und die Rules Engine.

AWS IoT Core für WAN LoRa

AWS IoT Core for LoRa WAN ermöglicht die Einrichtung eines privaten LoRa WAN-Netzwerks, indem Sie Ihre LoRa WAN-Geräte und -Gateways miteinander verbinden, AWS ohne dass ein LoRa WAN-Netzwerkserver (LNS) entwickelt und betrieben werden muss. Von LoRa WAN-Geräten empfangene Nachrichten werden an die Rules Engine gesendet, wo sie formatiert und an andere Dienste gesendet werden können. AWS IoT

Regeln-Engine

Der Rules Engine verbindet Daten vom Message Broker mit anderen AWS IoT -Diensten zur Speicherung und weiteren Verarbeitung. Sie können beispielsweise eine DynamoDB-Tabelle einfügen, aktualisieren oder abfragen oder eine Lambda-Funktion aufrufen, die auf einem Ausdruck basiert, den Sie im Rules Engine definiert haben. Sie können eine SQL-basierte Sprache verwenden, um Daten aus Nachrichten-Payloads auszuwählen, zu verarbeiten und an sonstige Services wie Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB und AWS Lambda zu senden. Sie können den Message Broker auch verwenden, um Nachrichten

erneut an weitere Abonnenten zu senden. Weitere Informationen finden Sie unter Regeln für AWS IoT.

## AWS IoT Core Dienste steuern

Die AWS IoT Core Kontrolldienste bieten Funktionen zur Gerätesicherheit, Verwaltung und Registrierung.

Benutzerdefinierter Authentifizierungsservice

Sie können Genehmiger definieren, mit denen Sie Ihre eigene Authentifizierungs- und Autorisierungsstrategie unter Verwendung eines benutzerdefinierten Authentifizierungsservice und einer Lambda-Funktion verwalten können. Benutzerdefinierte Autorisierer ermöglichen die Authentifizierung Ihrer Geräte und AWS IoT die Autorisierung von Vorgängen mithilfe von Bearer-Token-Authentifizierungs- und Autorisierungsstrategien.

Benutzerdefinierte Autorisierer können verschiedene Authentifizierungsstrategien implementieren, z. B. die Überprüfung von JSON-Web-Tokens oder die Angabe von Providern. OAuth Sie müssen Richtliniendokumente zurücksenden, die vom Gerätegateway zur Autorisierung von MQTT-Vorgängen verwendet werden. Weitere Informationen finden Sie unter Benutzerspezifische Authentifizierung und Autorisierung.

Service zur Gerätebereitstellung

Ermöglicht die Bereitstellung von Geräten mithilfe einer Vorlage, die die für Ihr Gerät erforderlichen Ressourcen beschreibt: ein Dingobjekt, ein Zertifikat und eine oder mehrere Richtlinien. Ein Dingobjekt ist ein Eintrag in der Registrierung, der Attribute zur Beschreibung eines Geräts enthält. Geräte verwenden Zertifikate zur Authentifizierung. AWS IoT Richtlinien bestimmen, welche Vorgänge ein Gerät in AWS IoT ausführen kann.

Die Vorlagen enthalten Variablen, die durch Werte in einem Wörterbuch (Map) ersetzt werden. Sie können mit derselben Vorlage mehrere Geräte bereitstellen, indem Sie einfach verschiedene Werte für die Vorlagenvariablen im Wörterbuch übergeben. Weitere Informationen finden Sie unter Gerätebereitstellung.

Gruppen-Registry

Mithilfe von Gruppen können Sie verschiedene Geräte gleichzeitig verwalten, indem Sie sie in Gruppen zusammenfassen. Gruppen können wiederum Gruppen enthalten – so können Sie eine Gruppenhierarchie aufbauen. Jede Aktion, die Sie an einer übergeordneten Gruppe

ausführen, gilt auch für die untergeordneten Gruppen. Dieselbe Aktion gilt auch für alle Geräte in der übergeordneten Gruppe und für alle Geräte in den untergeordneten Gruppen. Berechtigungen für eine Gruppe gelten für alle Geräte in der Gruppe und in sämtlichen untergeordneten Gruppen. Weitere Informationen finden Sie unter Geräte verwalten mit AWS IoT.

Jobs-Service

Ermöglicht die Definition einer Reihe von Remote-Operationen, die an ein oder mehrere mit AWS IoT verbundene Geräte gesendet und dort ausgeführt werden. Sie können beispielsweise einen Auftrag definieren, der eine Reihe von Geräten anweist, Anwendungs- oder Firmware-Updates herunterzuladen und zu installieren, einen Neustart vorzunehmen, die Zertifikate zu rotieren oder Remote-Fehlerbehebungsvorgänge auszuführen.

Zum Erstellen eines Auftrags geben Sie eine Beschreibung der Remote-Operationen sowie eine Liste von Zielen an, die diese ausführen sollen. Bei den Zielen kann es sich um einzelne Geräte und/oder Gruppen handeln. Weitere Informationen finden Sie unter AWS IoT Jobs.

Registrierung

Organisiert die Ressourcen, die jedem Gerät in der AWS Cloud zugeordnet sind. Sie registrieren Ihre Geräte und weisen jedem bis zu drei benutzerdefinierte Attribute zu. Sie können jedem Gerät auch Zertifikate und MQTT-Clients IDs zuordnen, um sie besser verwalten und Fehler beheben zu können. Weitere Informationen finden Sie unter Geräte verwalten mit AWS IoT.

Sicherheits- und Identitätsservice

Bietet gemeinsame Verantwortung für die Sicherheit in der AWS Cloud. Ihre Geräte müssen ihre Anmeldeinformationen sicher aufbewahren, damit Daten sicher an den Message Broker gesendet werden können. Message Broker und Rules Engine verwenden AWS-Sicherheitsfunktionen, um Daten sicher an Geräte oder sonstige AWS -Dienste zu senden. Weitere Informationen finden Sie unter Authentifizierung.

## AWS IoT Core Datendienste

Die AWS IoT Core Datendienste helfen Ihren IoT-Lösungen dabei, auch mit Geräten, die nicht immer verbunden sind, ein zuverlässiges Anwendungserlebnis zu bieten.

Geräteschatten

Ein JSON-Dokument, das dazu verwendet wird, um aktuelle Statusinformationen für ein Gerät zu speichern und abzurufen.

Geräteschatten-Service

Der Geräteschatten-Dienst behält den Status eines Geräts bei, sodass Anwendungen mit einem Gerät kommunizieren können – unabhängig davon, ob das Gerät online ist oder nicht. Wenn ein Gerät offline ist, verwaltet der Geräteschatten-Dienst seine Daten für verbundene Anwendungen. Wenn das Gerät wieder eine Verbindung herstellt, synchronisiert es seinen Status mit dem seines Schattens im Geräteschatten-Dienst. Außerdem können Ihre Geräte ihren aktuellen Status zur Verwendung durch Anwendungen oder andere Geräte veröffentlichen. Weitere Informationen finden Sie unter AWS IoT Device Shadow-Dienst.

### AWS IoT Core Support-Service

Amazon Sidewalk-Integration für AWS IoT Core

Amazon Sidewalk ist ein gemeinsam genutztes Netzwerk, das die Konnektivitätsoptionen verbessert, damit Geräte besser zusammenarbeiten können. Amazon Sidewalk unterstützt eine Vielzahl von Kundengeräten, z. B. Geräte zur Ortung von Haustieren oder Wertsachen, Geräte, die Smart-Home-Sicherheit und Lichtsteuerung bieten, und Geräte, die Ferndiagnosen für Geräte und Werkzeuge ermöglichen. Amazon Sidewalk Integration for AWS IoT Core ermöglicht es Geräteherstellern, ihre Sidewalk-Geräteflotte zur AWS IoT Cloud hinzuzufügen.

Weitere Informationen finden Sie unter AWS IoT Core für Amazon Sidewalk.

## Erfahren Sie mehr über AWS IoT

Dieses Thema hilft Ihnen, sich mit der Welt von vertraut zu machen AWS IoT. Sie erhalten allgemeine Informationen darüber, wie IoT-Lösungen in verschiedenen Anwendungsfällen eingesetzt werden, Schulungsressourcen, Links zu sozialen Medien für AWS IoT und alle anderen AWS Dienste sowie eine Liste der AWS IoT verwendeten Dienste und Kommunikationsprotokolle.

### Schulungsressourcen für AWS IoT

Wir bieten diese Schulungen an, damit Sie mehr darüber erfahren AWS IoT und erfahren, wie Sie sie auf Ihr Lösungsdesign anwenden können.

- Einführung in AWS IoT

  Ein Videoüberblick über AWS IoT und seine wichtigsten Dienste.

- Tauchen Sie tief in AWS IoT Authentifizierung und Autorisierung ein

  Ein Kurs für Fortgeschrittene, der sich mit den Konzepten der AWS IoT Authentifizierung und Autorisierung befasst. Sie lernen, wie Sie Clients authentifizieren und autorisieren, auf die AWS IoT Kontroll- und Datenebene zuzugreifen. APIs
- Reihe „Grundlagen zum Internet of Things (Internet der Dinge)“

  Ein Lernpfad mit IoT-eLearning-Modulen zu verschiedenen IoT-Technologien und -Funktionen.

## AWS IoT Ressourcen und Leitfäden

Dies sind ausführliche technische Ressourcen zu bestimmten Aspekten von AWS IoT.

- IoT Lens — AWS IoT Well-Architected Framework

  Ein Dokument, das die Best Practices für die Architektur Ihrer IoT-Anwendungen beschreibt. AWS
- Gestaltung von MQTT-Themen für AWS IoT Core

  Ein Whitepaper, das die bewährten Methoden für die Gestaltung von MQTT-Themen AWS IoT Core und die Nutzung AWS IoT Core von Funktionen mit MQTT beschreibt.
- Zusammenfassung und Einführung

  Ein PDF-Dokument, das die verschiedenen Möglichkeiten zur Bereitstellung großer AWS IoT Geräteflotten beschreibt.
- AWS IoT Core Device Advisor

  AWS IoT Core Device Advisor bietet vorgefertigte Tests, mit denen Sie IoT-Geräte auf zuverlässige und sichere Konnektivität überprüfen können AWS IoT Core, bevor Sie Geräte in der Produktion einsetzen.
- AWS IoT Ressourcen

  IoT-spezifische Ressourcen wie Technische Leitfäden, Referenzarchitekturen, eBooks und kuratierte Blogbeiträge, die in einem durchsuchbaren Index präsentiert werden.
- IoT-Atlas

  Übersichten zur Lösung gängiger IoT-Designprobleme. Der IoT-Atlas bietet detaillierte Einblicke in die Designherausforderungen, auf die Sie bei der Entwicklung Ihrer IoT-Lösung wahrscheinlich stoßen werden.

- AWS Whitepapers und Leitfäden

  Unsere aktuelle Sammlung von Whitepapern und Leitfäden zu und anderen Technologien. AWS IoT AWS

## AWS IoT in den sozialen Medien

Diese Social-Media-Kanäle informieren über AWS IoT und AWS verwandte Themen.

- Das Internet der Dinge auf AWS IoT — Offizieller Blog
- AWS IoT Videos im Amazon Web Services Services-Kanal auf YouTube

Diese Social-Media-Konten decken alle AWS Dienste ab, einschließlich AWS IoT

- Der Amazon Web Services Services-Kanal auf YouTube
- Amazon Web Services auf Twitter
- Amazon Web Services auf Facebook
- Amazon Web Services auf Instagram
- Amazon Web Services auf LinkedIn

## AWS Dienste, die von der AWS IoT Core Rules Engine verwendet werden

Die AWS IoT Core Regel-Engine kann eine Verbindung zu diesen AWS Diensten herstellen.

- Amazon-DynamoDB

  Amazon DynamoDB ist ein skalierbarer NoSQL-Datenbank-Service, der schnelle und vorhersehbare Datenbankleistung bietet.
- Amazon Kinesis

  Amazon Kinesis macht es einfach, Streaming-Daten in Echtzeit zu sammeln, zu verarbeiten und zu analysieren, sodass Sie zeitnahe Einblicke erhalten und schnell auf neue Informationen reagieren können. Amazon Kinesis kann Echtzeitdaten wie Video-, Audio-, Anwendungsprotokolle, Website-Clickstreams und IoT-Telemetriedaten für maschinelles Lernen, Analysen und andere Anwendungen aufnehmen.
- AWS Lambda

AWS Lambda ermöglicht es Ihnen, Code auszuführen, ohne Server bereitzustellen oder zu verwalten. Sie können Ihren Code so einrichten, dass er automatisch bei AWS IoT Daten und Ereignissen ausgelöst wird, oder ihn direkt über eine Web- oder Mobil-App aufrufen.

- Amazon Simple Storage Service

  Amazon Simple Storage Service (Amazon S3) kann jede Datenmenge jederzeit und von überall im Internet speichern und abrufen. AWS IoT Regeln können Daten zur Speicherung an Amazon S3 senden.

- Amazon Simple Notification Service

  Amazon Simple Notification Service (Amazon SNS) ist ein Webservice, mit dem Anwendungen, Endanwender und Geräte sofort Benachrichtigungen senden und empfangen können.

- Amazon Simple Queue Service

  Amazon Simple Queue Service (Amazon SQS) ist Nachrichten-Warteschlangen-Service, der Microservices, verteilte Systeme und Serverless Anwendungen entkoppelt und skaliert.

- OpenSearch Amazon-Dienst

  Amazon OpenSearch Service (OpenSearch Service) ist ein verwalteter Service, der die Bereitstellung, den Betrieb und die Skalierung OpenSearch vereinfacht. Dabei handelt es sich um eine beliebte Open-Source-Such- und Analyse-Engine.

- Amazon SageMaker KI

  Amazon SageMaker AI kann Modelle für maschinelles Lernen (ML) erstellen, indem es Muster in Ihren IoT-Daten findet. Der Service verwendet diese Modelle, um neue Daten zu verarbeiten und Prognosen für Ihre Anwendung zu generieren.

- Amazon CloudWatch

  Amazon CloudWatch bietet eine zuverlässige, skalierbare und flexible Überwachungslösung, mit der Sie Ihre eigenen Überwachungssysteme und -infrastruktur einrichten, verwalten und skalieren können.

## Kommunikationsprotokolle, unterstützt von AWS IoT Core

Diese Themen enthalten weitere Informationen zu den Kommunikationsprotokollen, die von AWS IoT verwendet werden. Weitere Informationen zu den Protokollen, die von Geräten und Diensten

verwendet werden AWS IoT und mit denen Geräte und Dienste verbunden werden AWS IoT, finden Sie unterVerbinden mit AWS IoT Core.

- MQTT (Message Queuing Telemetry Transport)

  Die Homepage der Website MQTT.org, auf der Sie die MQTT-Protokollspezifikationen finden. Weitere Informationen darüber, wie MQTT AWS IoT unterstützt wird, finden Sie unterMQTT.
- HTTPS (Hypertext Transfer Protocol – Secure)

  Geräte und Apps können über HTTPS auf AWS IoT Dienste zugreifen.
- LoRaWAN (Weitverkehrsnetzwerk mit großer Reichweite)

  LoRaWAN-Geräte und Gateways können mithilfe AWS IoT Core von AWS IoT Core for LoRa WAN eine Verbindung herstellen.
- TLS (Transport Layer Security) v1.3

  Die Spezifikation von TLS v1.3 (RFC 5246). AWS IoT verwendet TLS v1.3, um sichere Verbindungen zwischen Geräten und herzustellen. AWS IoT

# Was ist neu in derAWS IoT -Konsolenumgebung

Wir sind dabei, die Benutzeroberfläche derAWS IoT Konsole zu aktualisieren, um ein neues Erlebnis zu bieten. Wir aktualisieren die Benutzeroberfläche schrittweise, sodass einige Seiten in der Konsole ein neues Erlebnis bieten, andere möglicherweise sowohl das ursprüngliche als auch das neue Erlebnis und einige nur das ursprüngliche Erlebnis bieten.

Diese Tabelle zeigt den Status einzelner Bereiche derAWS IoT Konsolenbenutzeroberfläche zum 27. Januar 2022.

AWS IoTStatus der Konsolenbenutzeroberfläche

| Konsolenseite | Die -Erlebnis | Neue -Erlebnis | Kommentare |
|---|---|---|---|
| Monitor | Nicht verfügbar | Verfügbar | |
| Aktivität | Nicht verfügbar | Verfügbar | |
| Onboard — Los geht's | Nicht verfügbar | Verfügbar | In den CN-Regionen nicht verfügbar |

| Konsolenseite | Die -Erlebnis | Neue -Erlebnis | Kommentare |
|---|---|---|---|
| Onboard — Vorlagen für die Flottenbereitstellung | Verfügbar | Verfügbar | |
| Managen — Dinge | Verfügbar | Verfügbar | |
| Verwalten - Typen | Verfügbar | Verfügbar | |
| Verwalten - Dinggruppen | Verfügbar | Verfügbar | |
| Verwalten — Abrechnungsgruppen | Verfügbar | Verfügbar | |
| Manage - Jobs | Verfügbar | Verfügbar | |
| Verwalten - Jobvorlagen | Nicht verfügbar | Verfügbar | |
| Verwalten - Tunnel | Nicht verfügbar | Verfügbar | |
| Fleet Hub — Los geht's | Nicht verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |
| Fleet Hub - Anwendungen | Nicht verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |
| Greengrass - Erste Schritte | Nicht verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |
| Greengrass - Core-Geräte | Nicht verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |

| Konsolenseite | Die -Erlebnis | Neue -Erlebnis | Kommentare |
|---|---|---|---|
| Greengrass - Komponenten | Nicht verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |
| Greengrass - Bereitstellungen | Nicht verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |
| Greengrass - Klassisch (V1) | Verfügbar | Verfügbar | |
| Drahtlose Konnektivität — Einführung | Nicht verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |
| Drahtlose Konnektivität — Gateways | Nicht verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |
| Drahtlose Konnektivität — Geräte | Nicht verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |
| Drahtlose Konnektivität — Profile | Nicht verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |
| Drahtlose Konnektivität — Ziele | Nicht verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |
| Sicher - Zertifikate | Verfügbar | Verfügbar | |
| Sicher — Richtlinien | Verfügbar | Verfügbar | |
| Sicher - CAs | Verfügbar | Verfügbar | |

| Konsolenseite | Die -Erlebnis | Neue -Erlebnis | Kommentare |
|---|---|---|---|
| Sicher — Rollenaliase | Verfügbar | Verfügbar | |
| Sicher — Autorisatoren | Verfügbar | Verfügbar | |
| Verteidigen - Intro | Nicht verfügbar | Verfügbar | |
| Verteidigen — Audit | Nicht verfügbar | Verfügbar | |
| Verteidigen — Erkennen | Nicht verfügbar | Verfügbar | |
| Verteidigen — Maßnahmen zur Schadensbegrenzung | Nicht verfügbar | Verfügbar | |
| Defend - Einstellungen | Nicht verfügbar | Verfügbar | |
| Gesetz - Regeln | Verfügbar | Verfügbar | |
| Act - Destinationen | Verfügbar | Verfügbar | |
| Test - Geräteberater | Verfügbar | Verfügbar | Nicht in allen verfügbarAWS-Regionen |
| Test - MQTT-Testclient | Verfügbar | Verfügbar | |
| Software | Verfügbar | Verfügbar | |
| Einstellungen | Nicht verfügbar | Verfügbar | |
| Lernen | Verfügbar | Noch nicht verfügbar | |

## Legende

Statuswerte

- Verfügbar

  Diese Benutzeroberflächenerfahrung kann genutzt werden.
- Nicht verfügbar

  Diese Benutzerschnittstelle kann nicht verwendet werden.
- Noch nicht verfügbar

  An der neuen Benutzeroberfläche wird gearbeitet, aber sie ist noch nicht fertig.
- In Bearbeitung

  Die -Benutzerumgebung wird gerade aktualisiert. Einige Seiten bieten jedoch möglicherweise immer noch die ursprüngliche Benutzererfahrung.

# Verwendung AWS IoT mit einem SDK AWS

AWS Software Development Kits (SDKs) sind für viele gängige Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

| SDK-Dokumentation | Codebeispiele |
| --- | --- |
| AWS SDK für C++ | AWS SDK für C++ Codebeispiele |
| AWS CLI | AWS CLI Code-Beispiele |
| AWS SDK für Go | AWS SDK für Go Code-Beispiele |
| AWS SDK für Java | AWS SDK für Java Code-Beispiele |
| AWS SDK für JavaScript | AWS SDK für JavaScript Code-Beispiele |
| AWS SDK für Kotlin | AWS SDK für Kotlin Code-Beispiele |
| AWS SDK für .NET | AWS SDK für .NET Code-Beispiele |

| SDK-Dokumentation | Codebeispiele |
| --- | --- |
| AWS SDK für PHP | AWS SDK für PHP Code-Beispiele |
| AWS -Tools für PowerShell | Tools für PowerShell Codebeispiele |
| AWS SDK für Python (Boto3) | AWS SDK für Python (Boto3) Code-Beispiele |
| AWS SDK für Ruby | AWS SDK für Ruby Code-Beispiele |
| AWS SDK for Rust | AWS SDK for Rust Code-Beispiele |
| AWS SDK für SAP ABAP | AWS SDK für SAP ABAP Code-Beispiele |
| AWS SDK for Swift | AWS SDK for Swift Code-Beispiele |

**Beispiel für die Verfügbarkeit**

Sie können nicht finden, was Sie brauchen? Fordern Sie ein Codebeispiel an, indem Sie unten den Link Provide feedback (Feedback geben) auswählen.

# Erste Schritte mit AWS IoT Core Tutorials

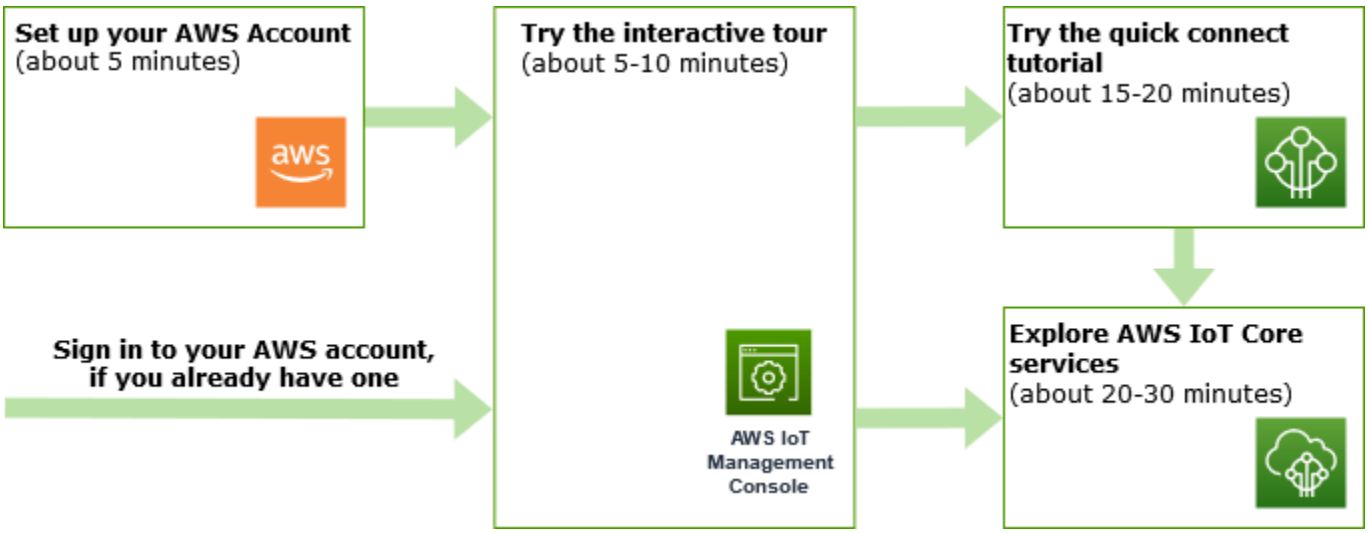
Ganz gleich, ob Sie mit IoT noch nicht vertraut sind oder über langjährige Erfahrung verfügen, in diesen Ressourcen finden Sie die AWS IoT Konzepte und Begriffe, die Ihnen beim Einstieg helfen werden AWS IoT.

- Schauen Sie hinein AWS IoT und sehen Sie sich die einzelnen Komponenten anWie AWS IoT funktioniert.
- Erfahren Sie mehr über AWS IoT in unserer Sammlung von Schulungsmaterialien und Videos. Dieses Thema enthält auch eine Liste von Diensten, mit denen AWS IoT eine Verbindung herstellen kann, Links zu sozialen Medien und Links zu Kommunikationsprotokollspezifikationen.
- the section called “Connect dein erstes Gerät mit AWS IoT Core”.
- Entwickeln Sie Ihre IoT-Lösungen mit Verbinden mit AWS IoT Core und erkunden Sie die AWS IoT Anleitungen.
- Testen und validieren Sie Ihre IoT-Geräte für eine sichere und zuverlässige Kommunikation mit dem Device Advisor.
- Verwalten Sie Ihre Lösung mithilfe von AWS IoT Core Verwaltungsdiensten wie -Flottenindizierung, AWS IoT Jobs und AWS IoT Device Defender.
- Analysieren Sie die Daten von Ihren Geräten mithilfe der AWS IoT Datendienste.

## Connect dein erstes Gerät mit AWS IoT Core

AWS IoT Core Dienste verbinden IoT-Geräte mit AWS IoT Diensten und anderen AWS Diensten. AWS IoT Core umfasst das Device Gateway und den Message Broker, die Nachrichten zwischen Ihren IoT-Geräten und der Cloud verbinden und verarbeiten.

So können Sie mit AWS IoT Core und beginnen AWS IoT.




In diesem Abschnitt werden die AWS IoT Core wichtigsten Dienste vorgestellt und es werden mehrere Beispiele dafür bereitgestellt, wie Sie ein Gerät mit diesen verbinden AWS IoT Core und Nachrichten zwischen ihnen weiterleiten können. Die Weitergabe von Nachrichten zwischen Geräten und der Cloud ist für jede IoT-Lösung von grundlegender Bedeutung. So können Ihre Geräte mit anderen AWS Diensten interagieren.

- Einrichten AWS-Konto

  Bevor Sie AWS IoT Dienste nutzen können, müssen Sie eine einrichten AWS-Konto. Wenn Sie bereits einen AWS-Konto und einen IAM-Benutzer für sich haben, können Sie diese verwenden und diesen Schritt überspringen.

- Probieren Sie das Quick Connect-Tutorial aus

  Dieses Tutorial eignet sich am besten, wenn Sie schnell damit beginnen AWS IoT und sehen möchten, wie es in einem begrenzten Szenario funktioniert. In diesem Tutorial benötigen Sie ein Gerät und installieren AWS IoT Software darauf. Wenn Sie kein IoT-Gerät haben, können Sie Ihren Windows-, Linux- oder macOS-PC als Gerät für dieses Tutorial verwenden. Wenn Sie es versuchen möchten AWS IoT, aber kein Gerät haben, versuchen Sie es mit der nächsten Option.

- Probieren Sie das interaktive Tutorial aus

  Diese Demo eignet sich am besten, wenn Sie sehen möchten, was eine AWS IoT Basislösung leisten kann, ohne ein Gerät anzuschließen oder Software herunterzuladen. Das interaktive Tutorial stellt eine simulierte Lösung vor, die auf AWS IoT Core Diensten basiert und veranschaulicht, wie sie interagieren.

- Lernen Sie AWS IoT Core Dienste anhand eines praktischen Tutorials kennen

Dieses Tutorial eignet sich am besten für Entwickler, die AWS IoT mit anderen AWS IoT Core Funktionen wie der Regel-Engine und Schatten beginnen möchten. Dieses Tutorial folgt einem ähnlichen Prozess wie das Schnellverbindungs-Tutorial, enthält jedoch mehr Details zu den einzelnen Schritten, um einen reibungsloseren Übergang zu den fortgeschritteneren Tutorials zu ermöglichen.

- MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen

  Erfahren Sie, wie Sie den MQTT-Testclient verwenden, um zu beobachten, wie Ihr erstes Gerät MQTT-Nachrichten mit AWS IoT veröffentlicht. Der MQTT-Testclient ist ein nützliches Tool zur Überwachung und Fehlerbehebung von Geräteverbindungen.

> **Note**
>
> Wenn Sie mehr als eines dieser Tutorials für die ersten Schritte ausprobieren oder dasselbe Tutorial wiederholen möchten, sollten Sie das Objekt löschen, das Sie in einem früheren Tutorial erstellt haben, bevor Sie ein anderes beginnen. Wenn Sie das Objekt nicht aus einem früheren Tutorial löschen, müssen Sie für nachfolgende Tutorials einen anderen Objektnamen verwenden. Dies liegt daran, dass der Objektname in Ihrem Konto und AWS-Region eindeutig sein muss.

Weitere Informationen zu finden Sie AWS IoT Core unter Was ist? AWS IoT Core

# Einrichten AWS-Konto

Führen Sie AWS IoT Core vor der ersten Verwendung die folgenden Aufgaben aus:

Themen

- Melde dich an für ein AWS-Konto
- Erstellen eines Benutzers mit Administratorzugriff
- Öffnen Sie die AWS IoT Konsole

## Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Ein Teil des Anmeldevorgangs umfasst den Empfang eines Telefonanrufs oder einer Textnachricht und die Eingabe eines Bestätigungscodes auf der Telefontastatur.

   Wenn Sie sich für eine anmelden AWS-Konto, wird eine Root-Benutzer des AWS-Kontoserstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

## Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

- Öffnen Sie die AWS IoT Konsole

Wenn Sie bereits einen Benutzer AWS-Konto und einen Benutzer für sich haben, können Sie ihn verwenden und mit dem Vorgang fortfahrenthe section called “Öffnen Sie die AWS IoT Konsole”.

## Öffnen Sie die AWS IoT Konsole

Die meisten konsolenorientierten Themen in diesem Abschnitt beginnen mit der AWS IoT Konsole. Wenn Sie noch nicht bei Ihrem angemeldet sind AWS-Konto, melden Sie sich an, öffnen Sie dann die AWS IoT Konsole und fahren Sie mit dem nächsten Abschnitt fort, um mit den ersten Schritten fortzufahren. AWS IoT

# Interaktives Tutorial

Das interaktive Tutorial zeigt die Komponenten einer einfachen IoT-Lösung, die auf AWS IoT basiert. Das Tutorial zeigt, wie IoT-Geräte mit AWS IoT Core Diensten interagieren. Dieses Thema bietet eine Vorschau auf das AWS IoT Core interaktive Tutorial.

> **Note**
>
> Die Bilder in der Konsole enthalten Animationen, die in den Bildern dieses Tutorials nicht vorkommen.

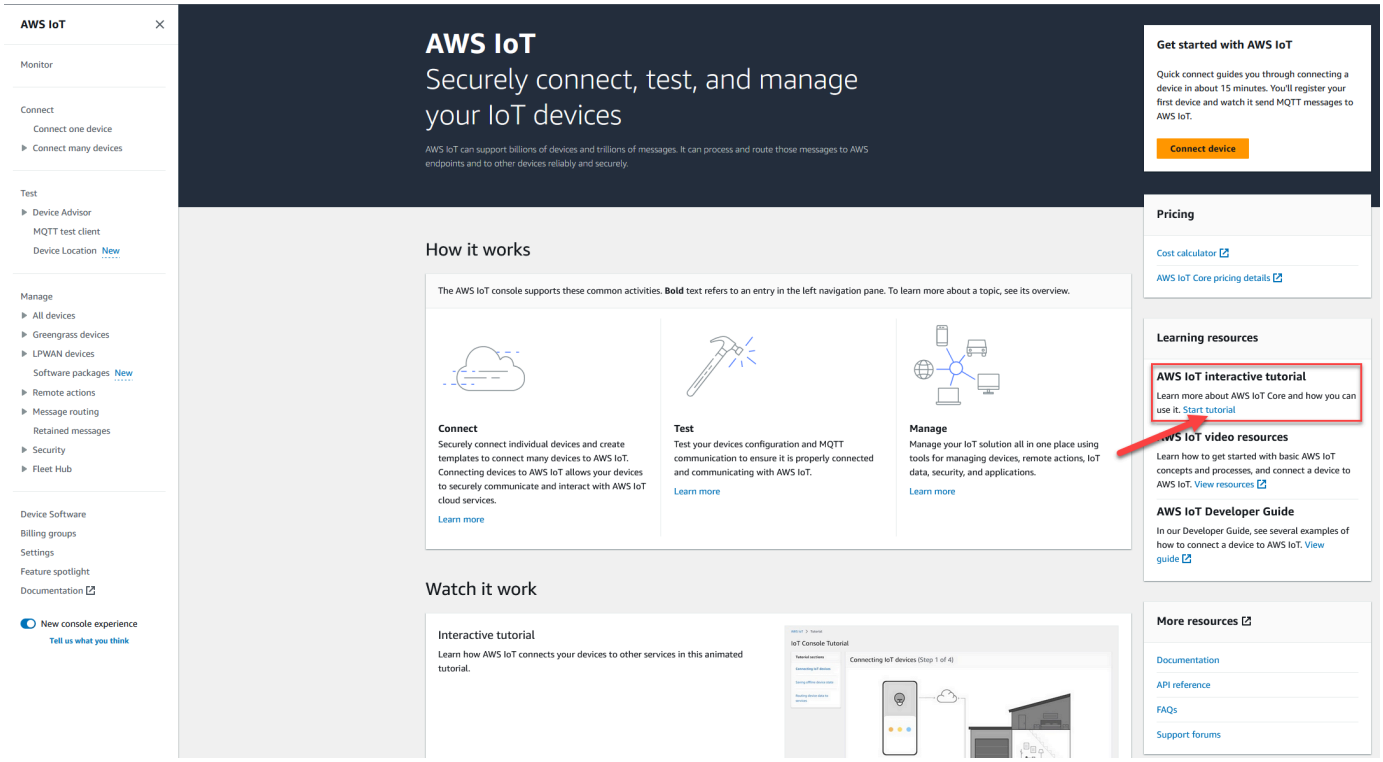
Um die Demo auszuführen, müssen Sie zuerst the section called “Einrichten AWS-Konto”. Für das Tutorial sind jedoch keine AWS IoT Ressourcen, zusätzliche Software oder Programmierung erforderlich.

Rechnen Sie damit, etwa 5-10 Minuten mit dieser Demo zu verbringen. Wenn Sie sich 10 Minuten Zeit nehmen, haben Sie mehr Zeit, um die einzelnen Schritte zu verstehen.

Um das AWS IoT Core interaktive Tutorial auszuführen

1. Öffnen Sie die AWS IoT Startseite in der AWS IoT Konsole.

   Wählen Sie auf der AWS IoT -Startseite im Fensterbereich Lernressourcen die Option Tutorial starten aus.



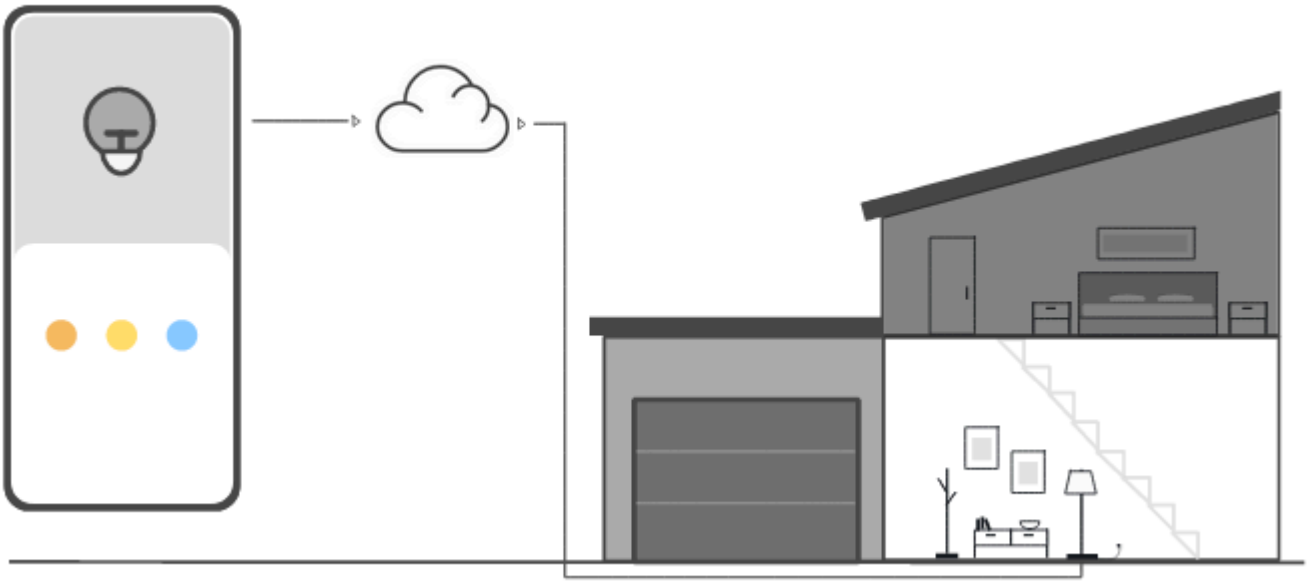

2. Sehen Sie sich auf der Seite mit dem AWS IoT Konsolen-Tutorial die Abschnitte mit den Tutorials an und wählen Sie den Abschnitt Start, wenn Sie bereit sind, fortzufahren.

In den folgenden Abschnitten wird beschrieben, wie das AWS IoT Konsolen-Tutorial diese AWS IoT Core Funktionen präsentiert:

- IoT-Geräte verbinden
- Der Status des Offline-Geräts wird gespeichert
- Gerätedaten an Dienste weiterleiten

# IoT-Geräte verbinden

Erfahren Sie, wie IoT-Geräte mit kommunizieren AWS IoT Core.

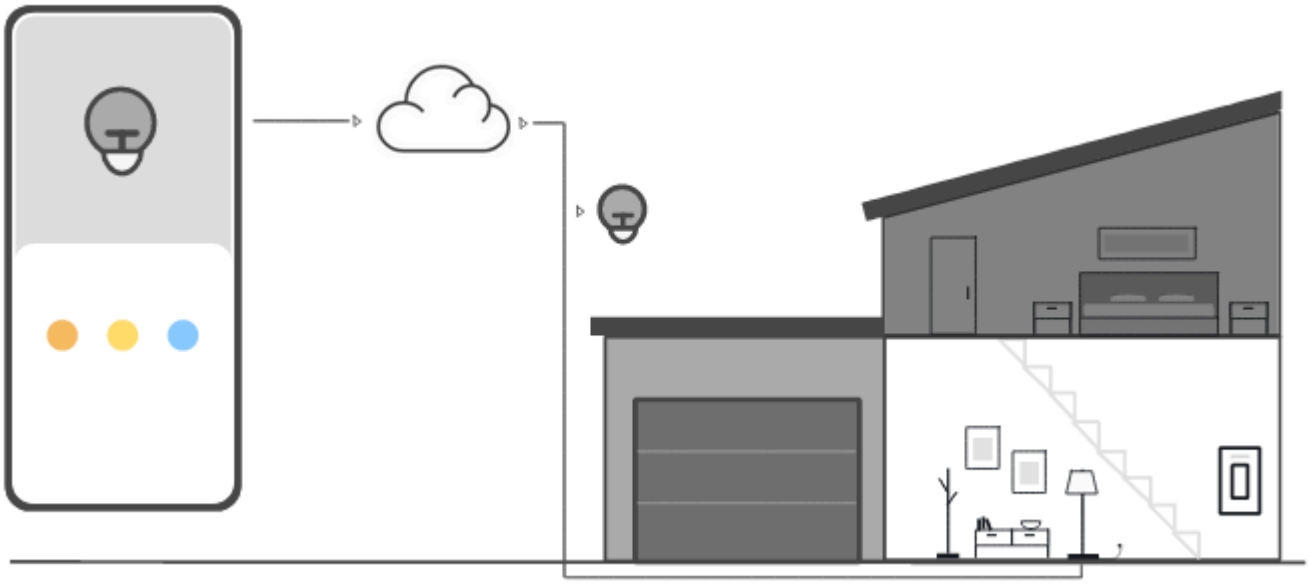


Die Animation in diesem Schritt zeigt, wie sich zwei Geräte, das Steuergerät auf der linken Seite und eine intelligente Lampe im Haus auf der rechten Seite, mit AWS IoT Core in der Cloud verbinden und kommunizieren. Die Animation zeigt, wie die Geräte mit den empfangenen Nachrichten kommunizieren AWS IoT Core und darauf reagieren.

Weitere Informationen zum Anschließen von Geräten an finden Sie AWS IoT Core unterVerbinden mit AWS IoT Core.

## Der Status des Offline-Geräts wird gespeichert

Erfahren Sie, wie der Gerätestatus AWS IoT Core gespeichert wird, solange ein Gerät oder eine App offline ist.



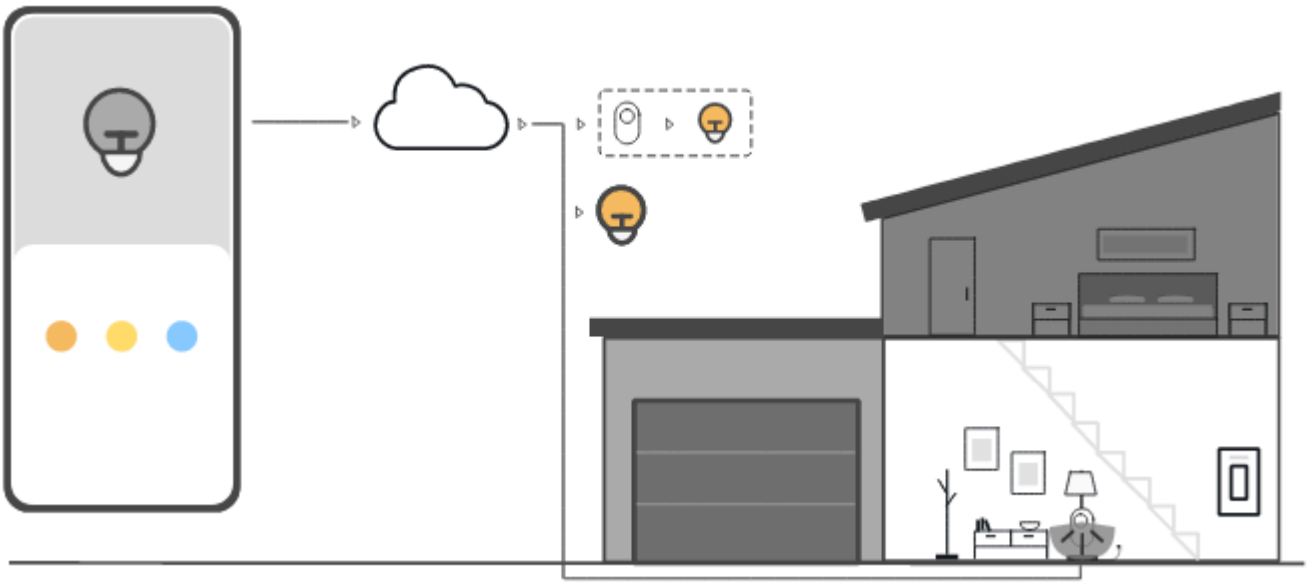
Die Animation in diesem Schritt zeigt, wie der Device Shadow-Dienst Gerätestatusinformationen für das Steuergerät und die intelligente Lampe AWS IoT Core speichert. Während die intelligente Lampe offline ist, speichert der Geräteschatten Befehle vom Steuergerät.

Wenn die Smart-Lampe wieder eine Verbindung mit herstellt AWS IoT Core, ruft sie diese Befehle ab. Wenn das Steuergerät offline ist, speichert der Geräteschatten Statusinformationen von der intelligenten Lampe. Wenn das Steuergerät wieder eine Verbindung herstellt, ruft es den aktuellen Status der intelligenten Lampe ab, um deren Anzeige zu aktualisieren.

Weitere Informationen finden Sie unter Geräteschatten, siehe AWS IoT Device Shadow-Dienst.

## Gerätedaten an Dienste weiterleiten

Erfahren Sie, wie der Gerätestatus an andere AWS Dienste AWS IoT Core gesendet wird.



Die Animation in diesem Schritt zeigt, wie Daten mithilfe von AWS IoT Regeln von den Geräten an andere AWS Dienste AWS IoT Core gesendet werden. AWS IoT Regeln abonnieren bestimmte Nachrichten von den Geräten, interpretieren die Daten in diesen Nachrichten und leiten die interpretierten Daten an andere Dienste weiter. In diesem Beispiel interpretiert eine AWS IoT Regel Daten von einem Bewegungssensor und sendet Befehle an einen Device Shadow, der sie dann an die Smart-Bulb sendet. Wie im vorherigen Beispiel speichert der Geräteschatten die Gerätestatusinformationen für das Steuergerät.

Weitere Informationen zu AWS IoT Regeln finden Sie unterRegeln für AWS IoT.

## Probieren Sie das AWS IoT Core Quick Connect-Tutorial aus

In diesem Tutorial erstellen Sie Ihr erstes Objekt, verbinden ein Gerät damit und sehen, wie es MQTT-Nachrichten sendet.

Sie können damit rechnen, 15 bis 20 Minuten für dieses Tutorial aufzuwenden.

Dieses Tutorial eignet sich am besten für Personen, die schnell damit beginnen möchten AWS IoT , zu erfahren, wie es in einem begrenzten Szenario funktioniert. Wenn Sie nach einem Beispiel suchen, das Ihnen den Einstieg erleichtert, damit Sie weitere Funktionen und Dienste erkunden können, versuchen Sie Erfahren Sie AWS IoT Core in praktischen Tutorials mehr.

In diesem Tutorial laden Sie Software herunter und führen sie auf einem Gerät aus, das im AWS IoT Core Rahmen einer sehr kleinen IoT-Lösung eine Verbindung zu einer Ding-Ressource herstellt. Das

Gerät kann ein IoT-Gerät sein, z. B. ein Raspberry Pi, oder es kann sich auch um einen Computer handeln, auf dem Linux, OS und OSX oder Windows ausgeführt werden. Wenn Sie ein WAN-Gerät (Long Range WAN) mit einem LoRa WAN verbinden möchten AWS IoT, finden Sie weitere Informationen im Tutorial >Geräte und Gateways mit AWS IoT Core für LoRa WAN verbinden.

Wenn Ihr Gerät einen Browser unterstützt, der die AWS IoT -Konsole ausführen kann, empfehlen wir Ihnen, dieses Tutorial auf diesem Gerät abzuschließen.

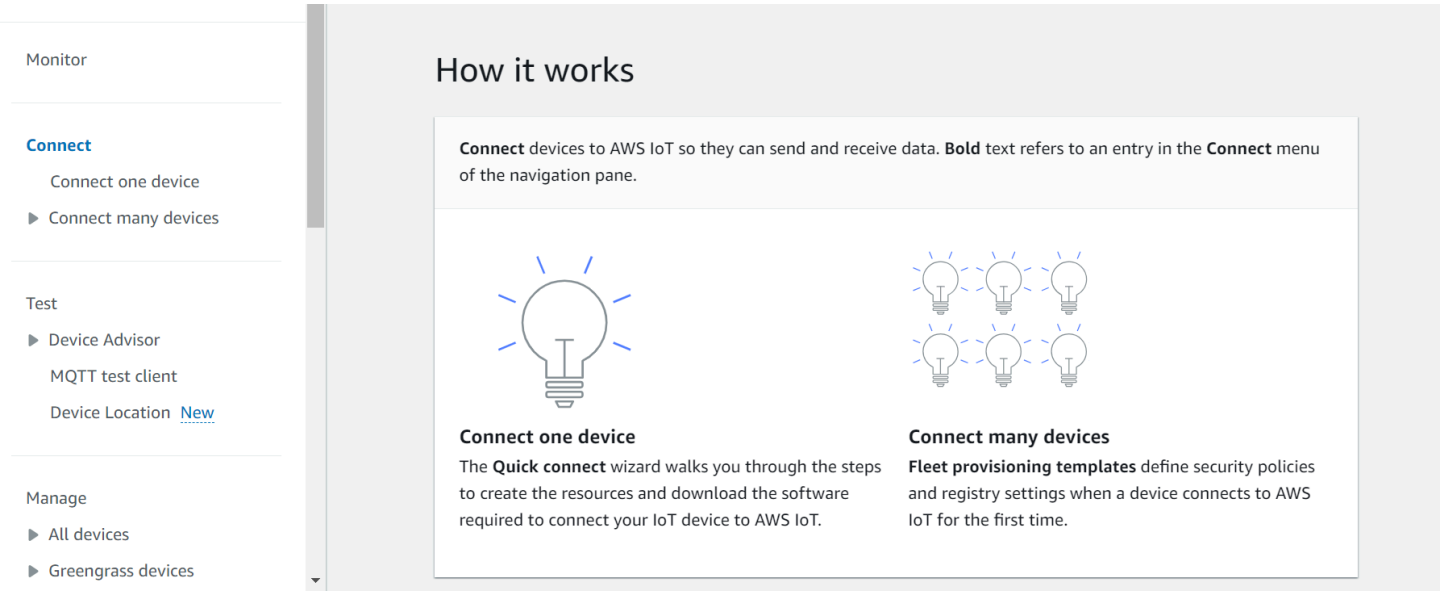
> **Note**
>
> Wenn Ihr Gerät keinen kompatiblen Browser hat, folgen Sie diesem Tutorial auf einem Computer. Wenn Sie im Rahmen des Verfahrens aufgefordert werden, die Datei herunterzuladen, laden Sie sie auf Ihren Computer herunter und übertragen Sie dann die heruntergeladene Datei mithilfe von Secure Copy (SCP) oder einem ähnlichen Verfahren auf Ihr Gerät.

Für das Tutorial muss Ihr IoT-Gerät mit Port 8443 an dem Gerätedatenendpunkt Ihres AWS-Konto kommunizieren. Um zu testen, ob es auf diesen Port zugreifen kann, probieren Sie die Verfahren unter Testen Sie die Konnektivität mit Ihrem Gerätedatenendpunkt aus.

## Schritt 1. Beginnen Sie mit dem Tutorial

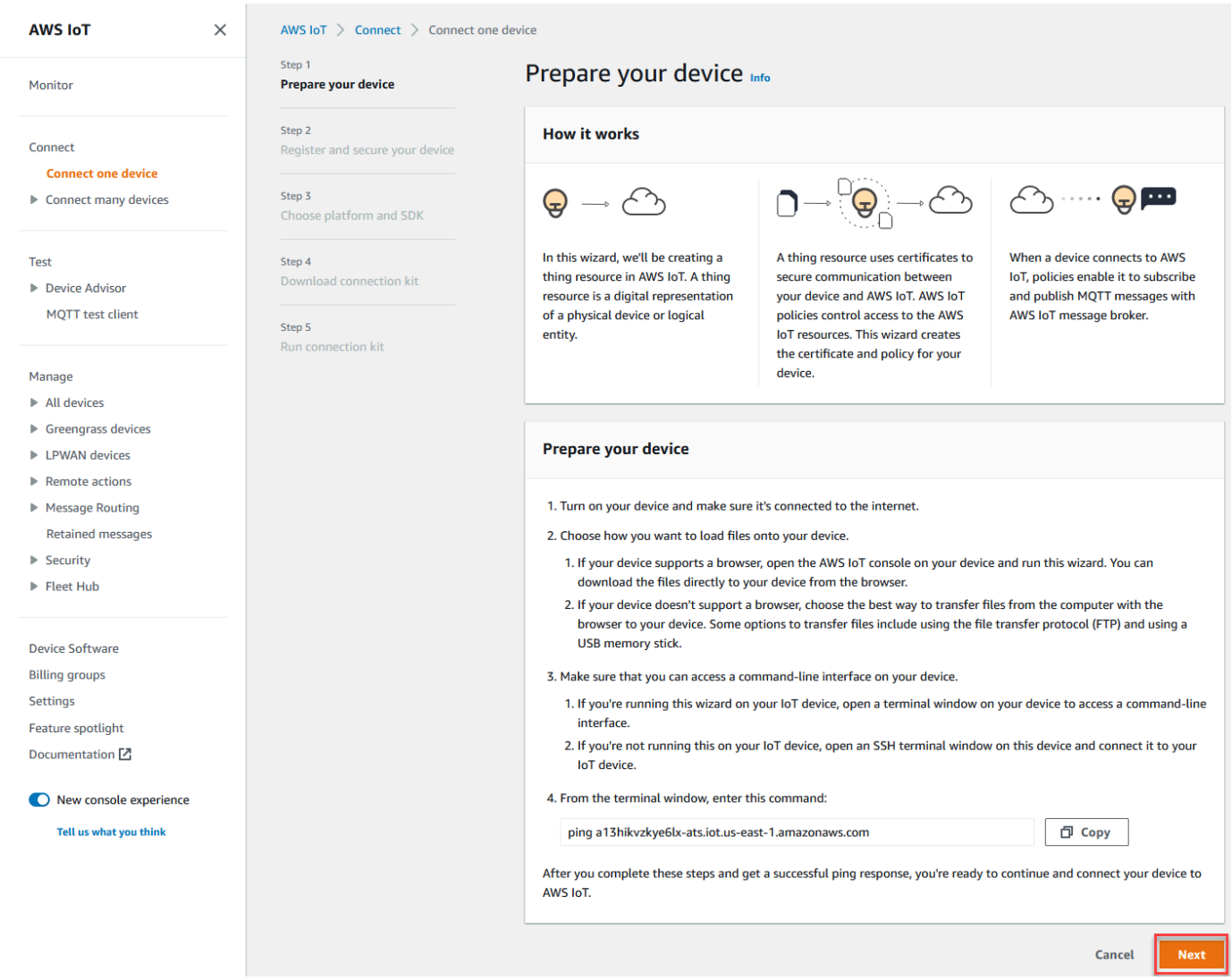
Wenn möglich, führen Sie dieses Verfahren auf Ihrem Gerät aus. Andernfalls sollten Sie bereit sein, später in diesem Verfahren eine Datei auf Ihr Gerät zu übertragen.

Melden Sie sich an der AWS IoT -Konsole an, um das Tutorial zu starten. Wählen Sie auf der Startseite der AWS IoT Konsole auf der linken Seite Connect und dann Connect one device (Ein Gerät verbinden).




## Schritt 2. Dies erstellt ein Objekt

1. Folgen Sie im Abschnitt Gerät vorbereiten den Anweisungen auf dem Bildschirm, um Ihr Gerät für die Verbindung mit AWS IoT vorzubereiten.

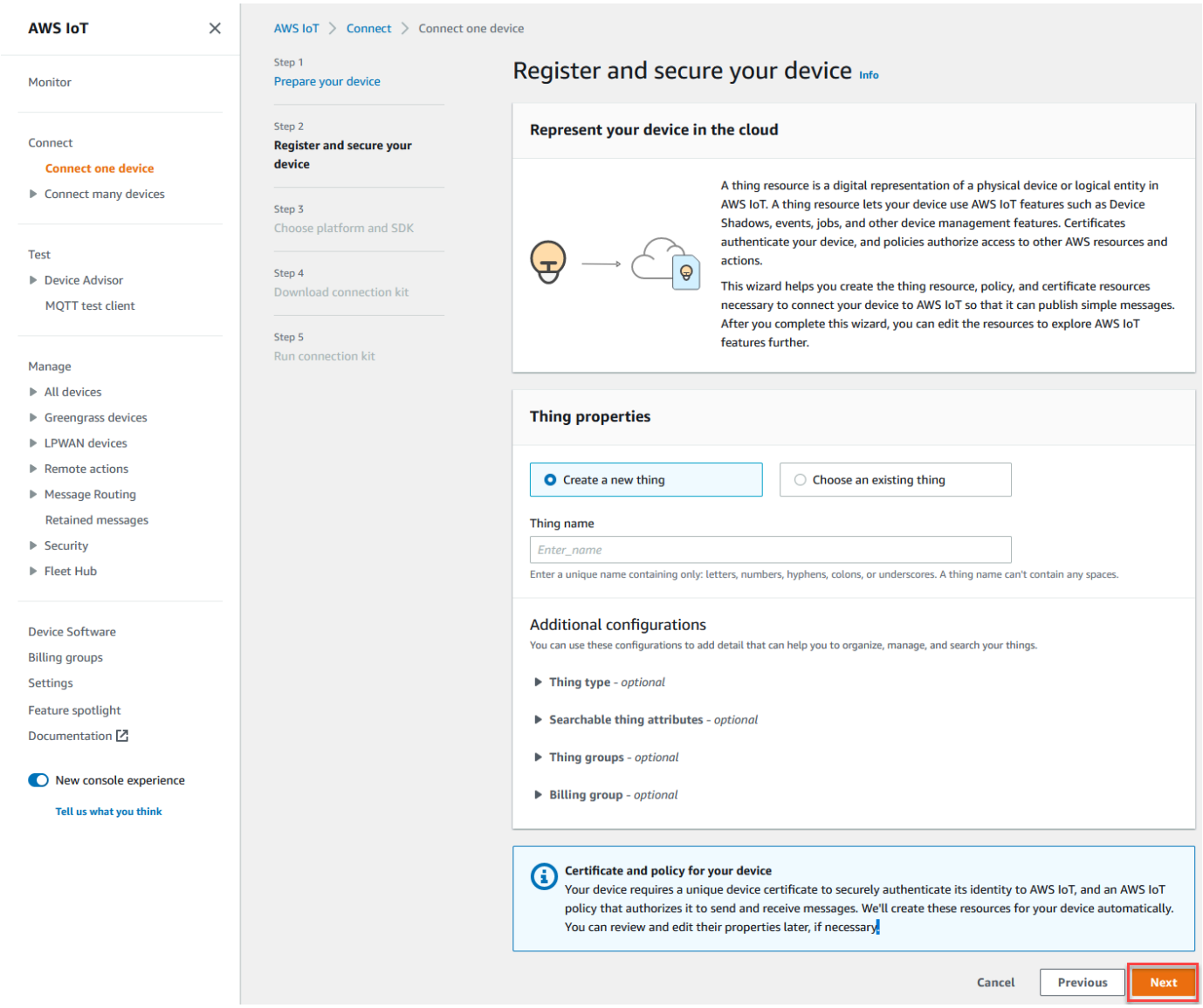



2. Wählen Sie im Bereich Gerät registrieren und sichern die Option Neues Objekt erstellen oder Bestehendes Objekt auswählen aus. Geben Sie im Feld Objektname den Namen für Ihr Objekt ein. Der in diesem Beispiel verwendete Objektname lautet **`TutorialTestThing`**

> **Important**
>
> Überprüfen Sie den Namen Ihres Objekts noch einmal, bevor Sie fortfahren.
> Ein Objektname kann nicht mehr geändert werden, nachdem das Objekt erstellt wurde. Wenn Sie den Namen eines Objekts ändern möchten, müssen Sie ein neues Objekt mit dem richtigen Namen erstellen und dann das Objekt mit dem falschen Namen löschen.

Passen Sie im Abschnitt Zusätzliche Konfigurationen Ihre Objekt-Ressource mithilfe der aufgelisteten optionalen Konfigurationen weiter an.

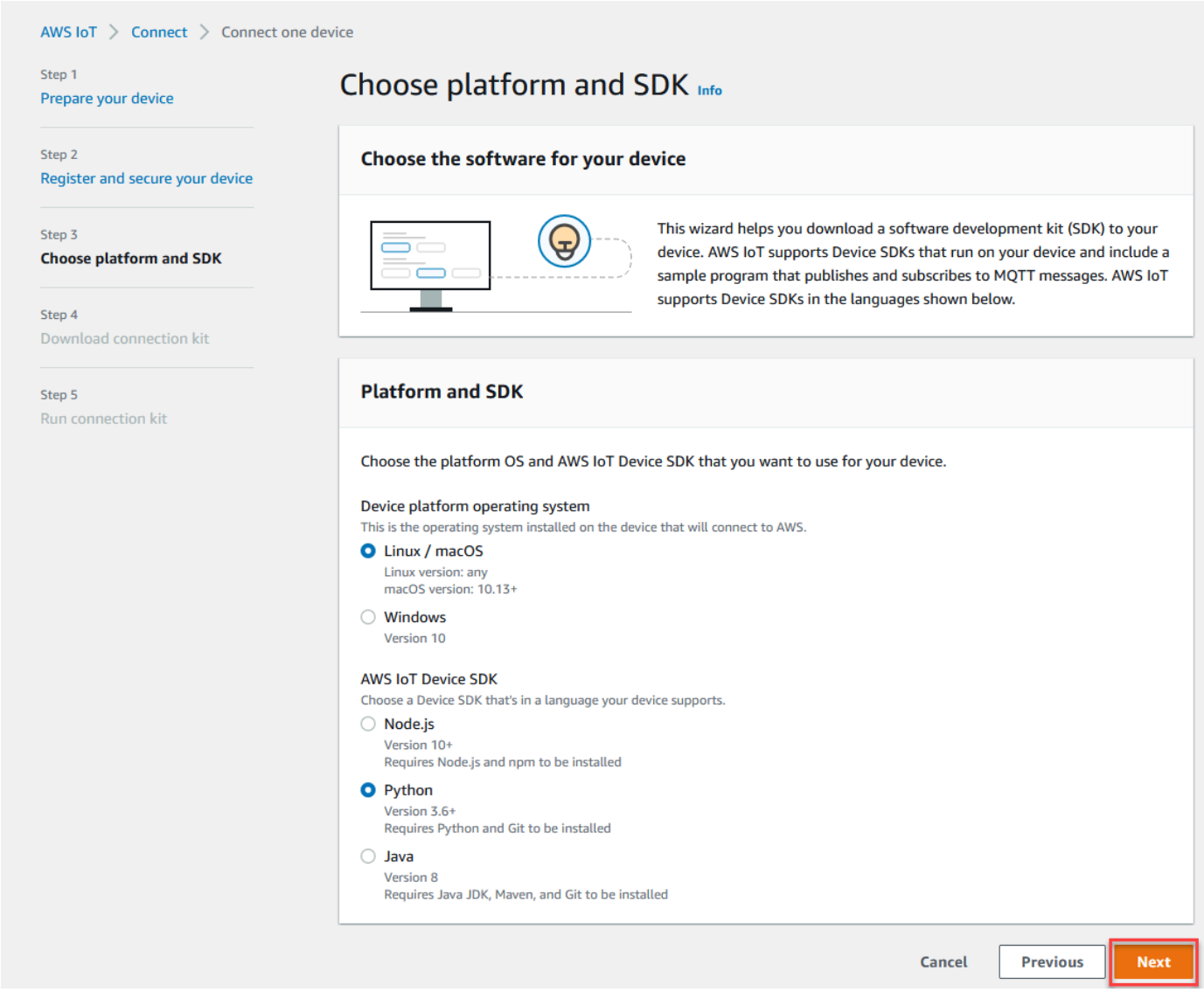
Nachdem Sie Ihrem Objekt einen Namen gegeben und weitere Konfigurationen ausgewählt haben, wählen Sie Weiter.




3. Wählen Sie im Abschnitt Plattform und SDK auswählen die Plattform und die Sprache des AWS IoT Geräte-SDK aus, das Sie verwenden möchten. In diesem Beispiel werden die Linux/OSX Plattform und das Python-SDK verwendet. Stellen Sie sicher, dass Sie Python3 und Pip3 auf Ihrem Zielgerät installiert haben, bevor Sie mit dem nächsten Schritt fortfahren.

> **Note**
>
> Schauen Sie sich am Ende der Konsolenseite unbedingt die Liste der erforderlichen Software an, die für das von Ihnen gewählte SDK erforderlich ist.
> Sie müssen die erforderliche Software auf Ihrem Zielcomputer installiert haben, bevor Sie mit dem nächsten Schritt fortfahren können.

Nachdem Sie die Plattform und die SDK-Sprache für das Gerät ausgewählt haben, wählen Sie Weiter.

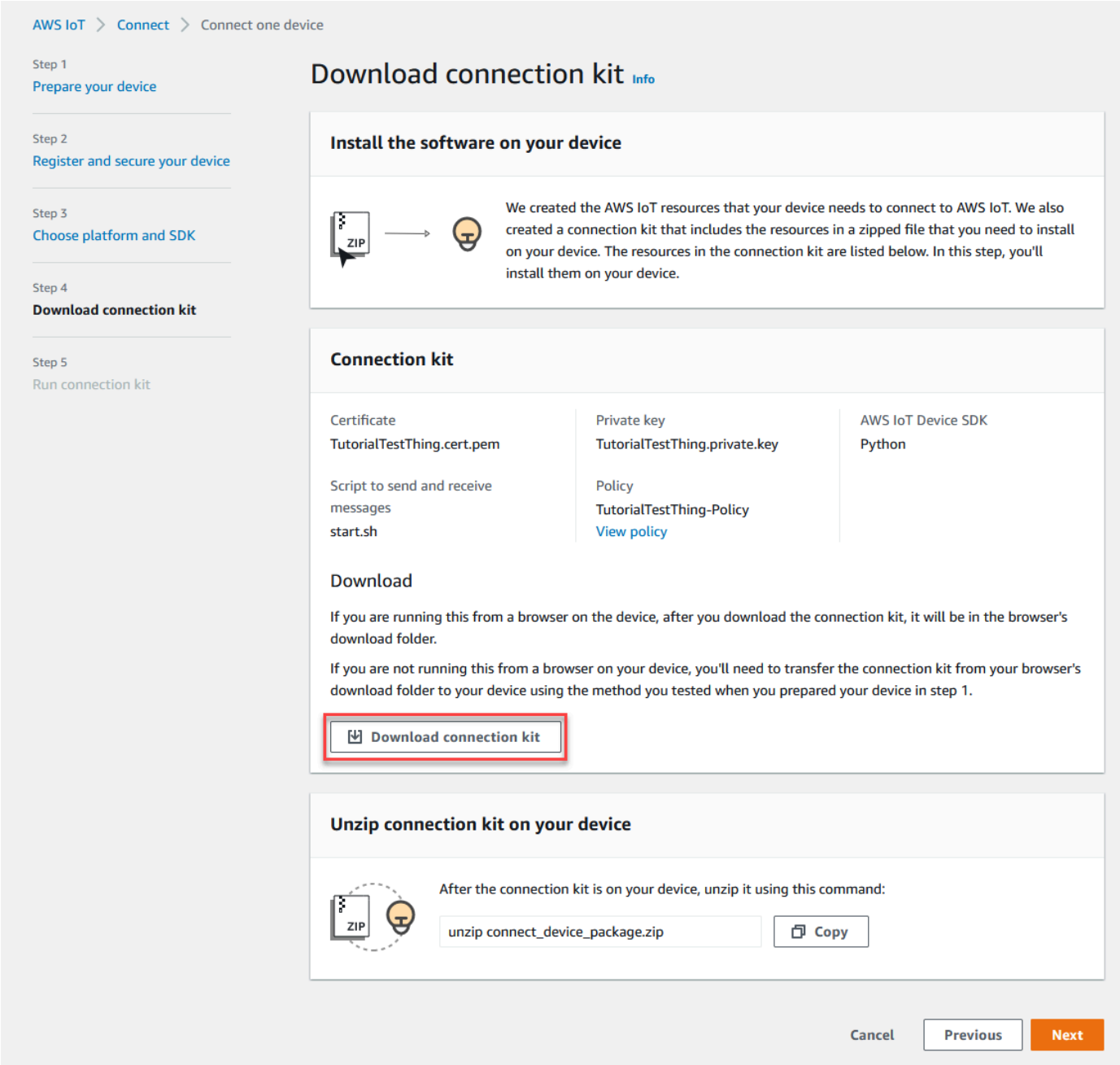


# Schritt 3. Laden Sie Dateien auf Ihr Gerät herunter

Diese Seite wird angezeigt, nachdem das Verbindungskit erstellt AWS IoT wurde, das die folgenden Dateien und Ressourcen enthält, die Ihr Gerät benötigt:

- Die Zertifikatsdateien des Objekts, die zur Authentifizierung des Geräts verwendet werden
- Eine Richtlinienressource, mit der Ihr Objekt zur Interaktion mit AWS IoT autorisiert wird
- Das Skript zum Herunterladen des AWS Geräte-SDK und zum Ausführen des Beispielprogramms auf Ihrem Gerät

1. Wenn Sie bereit sind, fortzufahren, klicken Sie auf die Schaltfläche Verbindungskit herunterladen für, um das Verbindungskit für die zuvor gewählte Plattform herunterzuladen.



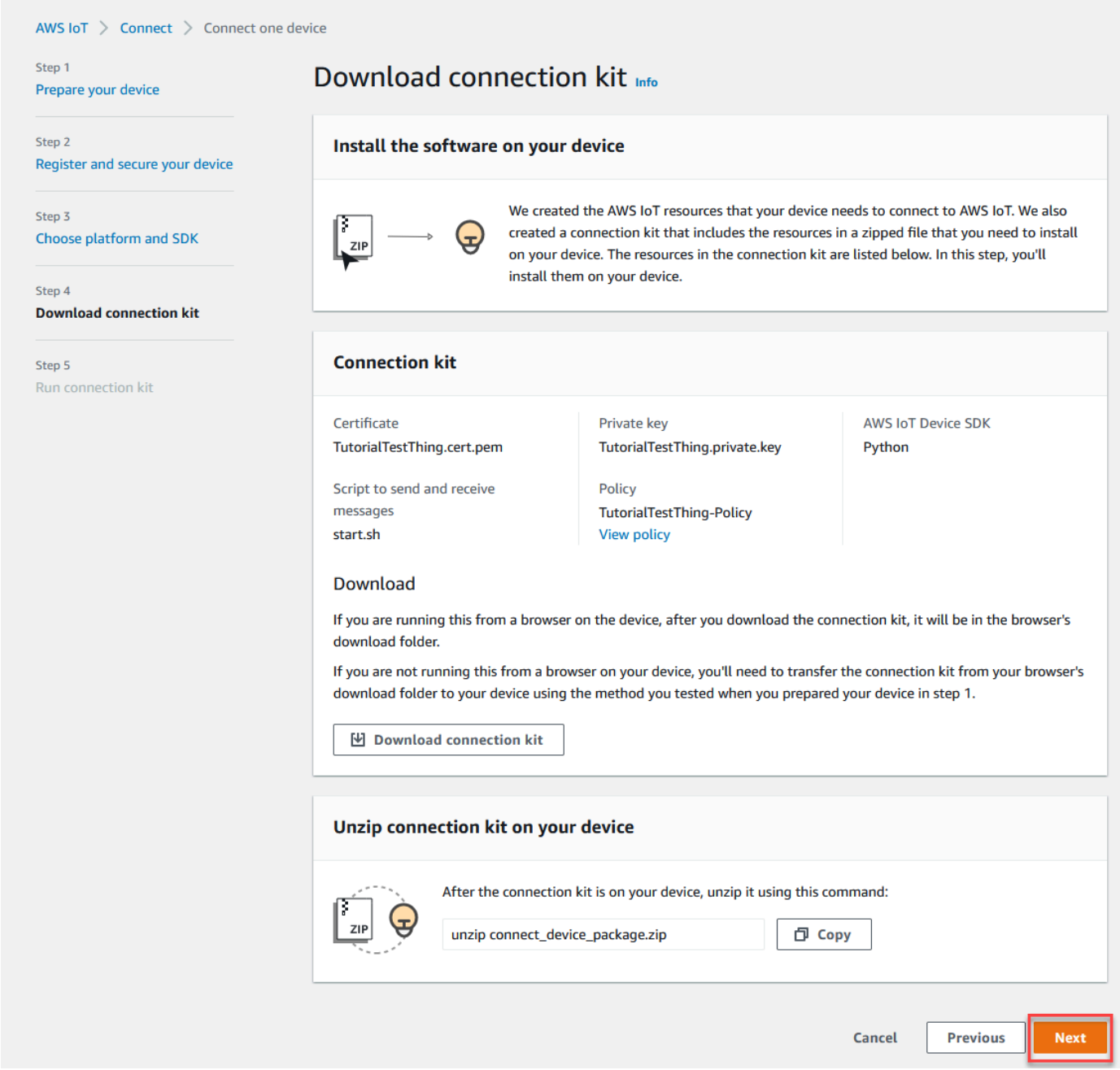

2. Wenn Sie dieses Verfahren auf Ihrem Gerät ausführen, speichern Sie die Verbindungskit-Datei in einem Verzeichnis, von dem aus Sie Befehlszeilen in der Kommandozeile ausführen können.

   Wenn Sie dieses Verfahren nicht auf Ihrem Gerät ausführen, speichern Sie die Verbindungskit-Datei in einem lokalen Verzeichnis und übertragen Sie die Datei dann auf Ihr Gerät.

3. Geben Sie im Abschnitt Verbindungskit auf Ihrem Gerät entpacken unzip connect_device_package.zip in das Verzeichnis ein, in dem sich die Verbindungskit-Dateien befinden.

Wenn Sie ein PowerShell Windows-Befehlsfenster verwenden und der unzip Befehl nicht funktioniert, ersetzen Sie ihn durch und versuchen Sie es erneut unzip mit expand-archive der Befehlszeile.

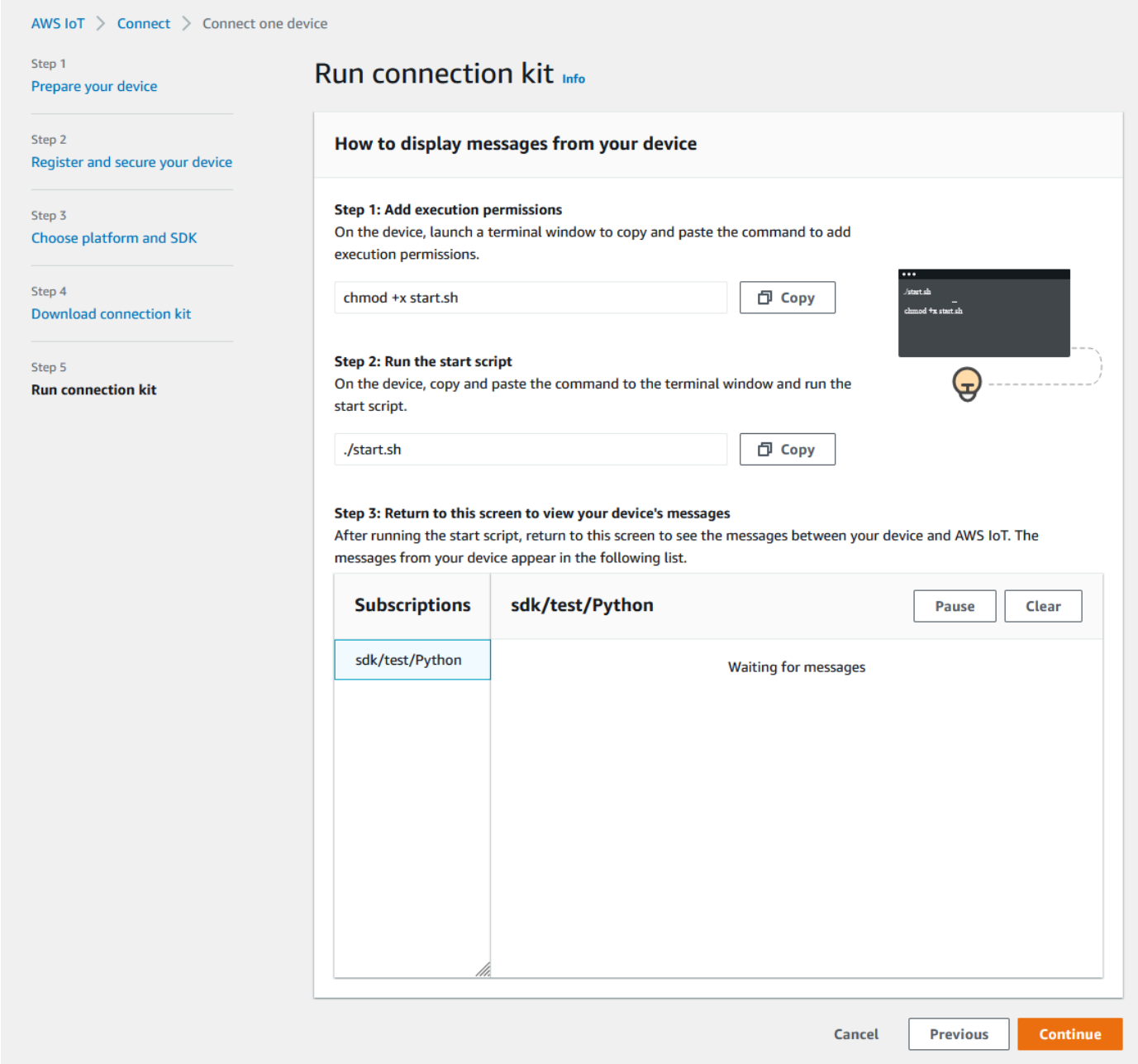
4. Nachdem Sie die Verbindungskit-Datei auf dem Gerät gespeichert haben, setzen Sie das Tutorial fort, indem Sie Weiter wählen.



# Schritt 4. Ausführen des Beispiels

Sie führen dieses Verfahren in einem Terminal oder Befehlsfenster auf Ihrem Gerät durch und folgen dabei den Anweisungen in der Konsole. Die Befehle, die Sie in der Konsole sehen, beziehen sich auf das Betriebssystem, für das Sie sich in the section called “Schritt 2. Dies erstellt ein Objekt” entschieden haben. Die hier gezeigten sind für die Linux/OSX Betriebssysteme.

1. Führen Sie in einem Terminal- oder Befehlsfenster auf Ihrem Gerät im Verzeichnis mit der Verbindungskit-Datei die in der AWS IoT Konsole angezeigten Schritte aus.



2. Nachdem Sie den Befehl aus Schritt 2 in der Konsole eingegeben haben, sollte im Terminal oder Befehlsfenster des Geräts eine Ausgabe angezeigt werden, die der folgenden ähnelt. Diese Ausgabe stammt aus den Nachrichten, an die das Programm sendet und denen, die es dann von AWS IoT Core zurückempfängt.

```
Running pub/sub sample application...
Connecting to a13hikvzkye6lx-ats.iot.us-east-1.amazonaws.com with client ID 'basicPubSub'...
Connected!
Subscribing to topic 'sdk/test/Python'...
Subscribed with QoS.AT_LEAST_ONCE
Sending messages until program killed
Publishing message to topic 'sdk/test/Python': Hello World! [1]
Received message from topic 'sdk/test/Python': b'"Hello World! [1]"'
Publishing message to topic 'sdk/test/Python': Hello World! [2]
Received message from topic 'sdk/test/Python': b'"Hello World! [2]"'
Publishing message to topic 'sdk/test/Python': Hello World! [3]
Received message from topic 'sdk/test/Python': b'"Hello World! [3]"'
```

   Während das Beispielprogramm läuft, wird auch die Testnachricht `Hello World!` angezeigt. Die Testnachricht wird im Terminal oder Befehlsfenster auf Ihrem Gerät angezeigt.

   > **Note**
   >
   > Weitere Informationen zum Abonnieren und Veröffentlichen von Themen finden Sie im Beispielcode des von Ihnen ausgewählten SDK.

3. Um das Beispielprogramm erneut auszuführen, können Sie die Befehle aus Schritt 2 in der Konsole dieses Verfahrens wiederholen.

4. (Optional) Wenn Sie die Nachrichten von Ihrem IoT-Client in der AWS IoT Konsole sehen möchten, öffnen Sie den MQTT-Testclient auf der Testseite der AWS IoT Konsole. Wenn Sie Python SDK ausgewählt haben, geben Sie im MQTT-Testclient unter Themenfilter das Thema ein, beispielsweise **`sdk/test/python`**, um die Nachrichten von Ihrem Gerät zu abonnieren. Bei den Themenfiltern wird zwischen Groß- und Kleinschreibung unterschieden und sie hängen von der Programmiersprache des SDK ab, welches Sie in Schritt 1 ausgewählt haben. Weitere Informationen zum Abonnieren und Veröffentlichen von Themen finden Sie im Codebeispiel des von Ihnen ausgewählten SDK.

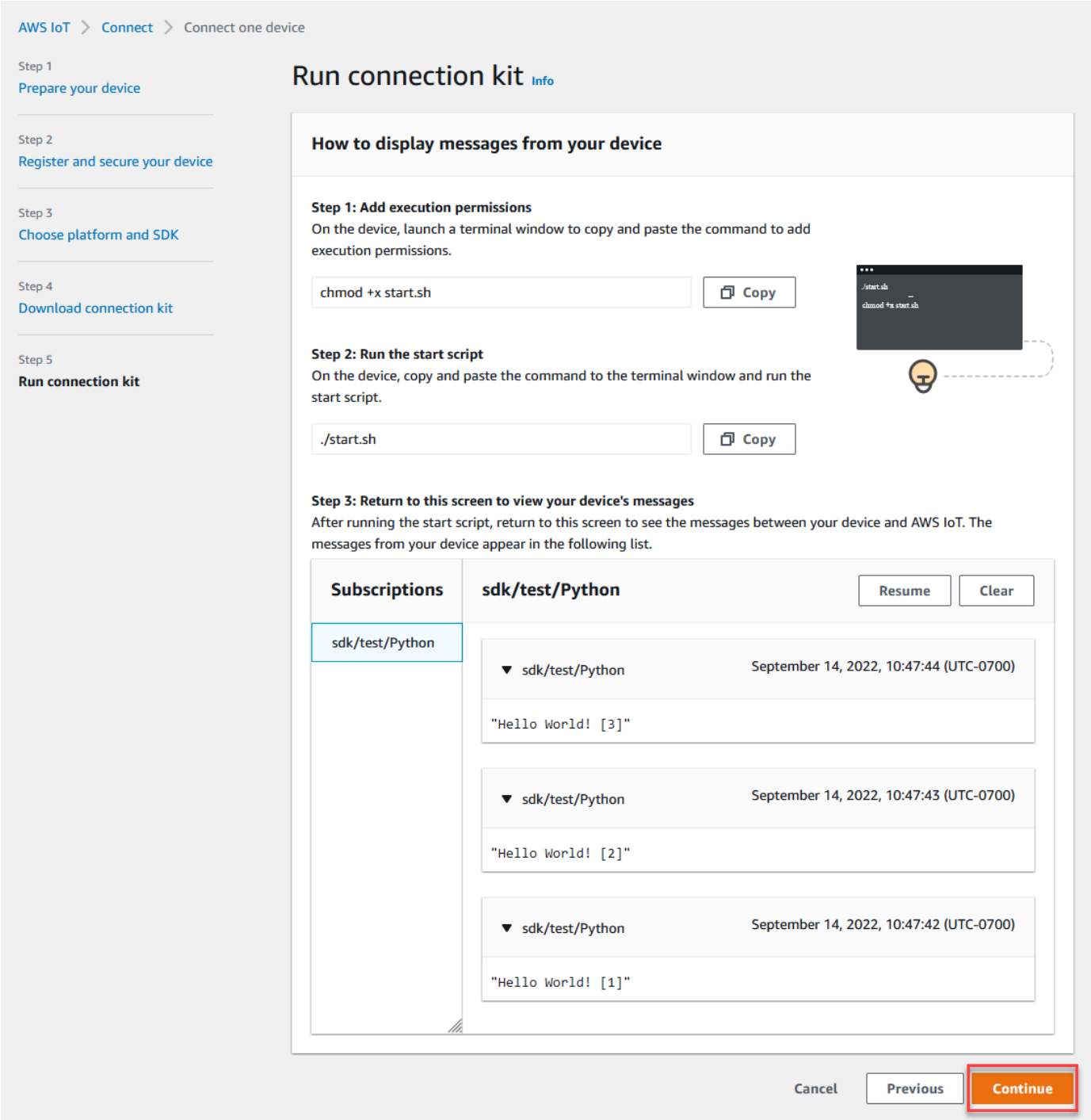
5. Nachdem Sie das Testthema abonniert haben, führen Sie ./start.sh auf Ihrem Gerät aus. Weitere Informationen finden Sie unter the section called “MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen”.

   Nach der Ausführung von ./start.sh werden im MQTT-Client Meldungen angezeigt, die den folgenden ähneln:

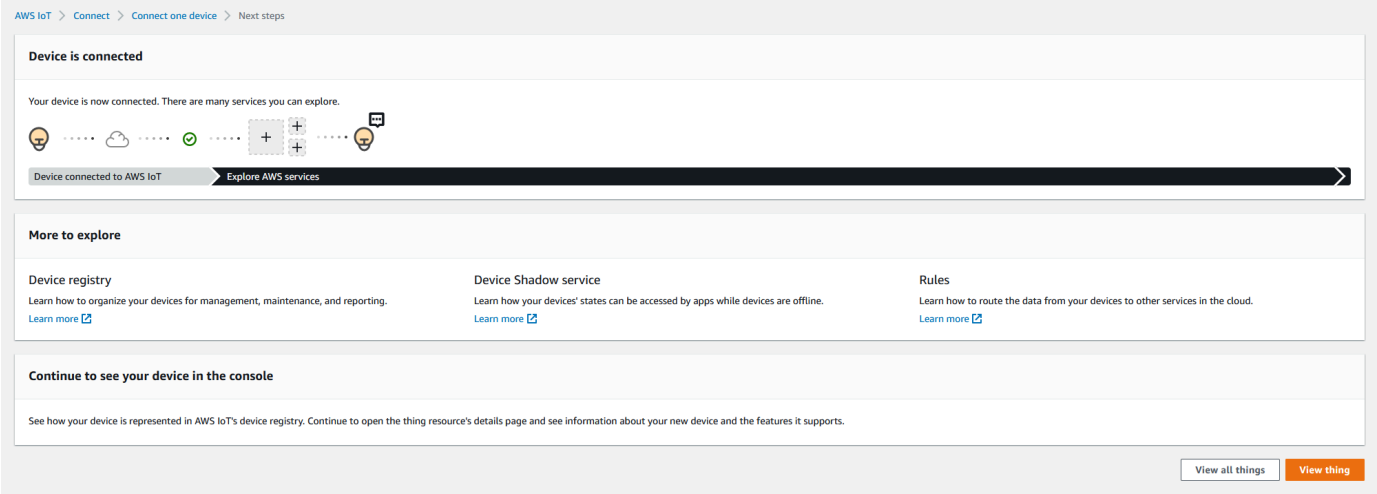
```
{
  "message": "Hello World!" [1]
}
```

Die `sequence` Zahl wird bei jedem Empfang einer neuen `Hello World!` Nachricht um `[]` erhöht und endet, wenn Sie das Programm beenden.

6. Um das Tutorial zu beenden und eine Zusammenfassung zu sehen, wählen Sie in der AWS IoT Konsole Weiter.




7. Eine Zusammenfassung Ihres AWS IoT Quick Connect-Tutorials wird nun angezeigt.




## Schritt 5. Weiter erkunden

Im Folgenden finden Sie einige Ideen, die Sie nach Abschluss des Schnellstarts AWS IoT weiter untersuchen sollten.

- So zeigen Sie MQTT-Nachrichten im MQTT-Client an

  Von der AWS IoT Konsole aus können Sie den MQTT-Client auf der Testseite der AWS IoT Konsole öffnen. Abonnieren Sie **#** im MQTT-Testclient und führen Sie es dann auf Ihrem Gerät aus, ./start.sh wie im vorherigen Schritt beschrieben. Weitere Informationen finden Sie unter the section called “MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen”.
- Führen Sie Tests auf Ihren Geräten mit Device Advisor durch

  Testen Sie mit Device Advisor, ob Ihre Geräte sicher und zuverlässig eine Verbindung herstellen und mit ihnen interagieren können AWS IoT.
- the section called “Interaktives Tutorial”

  Um das interaktive Tutorial zu starten, wählen Sie auf der Lernseite der AWS IoT Konsole in der Kachel „So AWS IoT funktioniert“ die Option Tutorial starten aus.
- Machen Sie sich bereit, weitere Tutorials zu entdecken

  Dieser Schnellstart gibt Ihnen nur ein Beispiel für AWS IoT. Wenn Sie mehr darüber erfahren und mehr über die Funktionen erfahren möchten, die sie zu einer leistungsstarken IoT-Lösungsplattform machen, beginnen Sie mit der Vorbereitung Ihrer Entwicklungsplattform durchErfahren Sie AWS IoT Core in praktischen Tutorials mehr. AWS IoT

# Testen Sie die Konnektivität mit Ihrem Gerätedatenendpunkt

In diesem Thema wird beschrieben, wie Sie die Verbindung eines Geräts mit dem Gerätedatenendpunkt Ihres Kontos testen, dem Endpunkt, mit dem Ihre IoT-Geräte eine Verbindung zu AWS IoT herstellen.

Führen Sie diese Verfahren auf dem Gerät aus, das Sie testen möchten, oder verwenden Sie eine SSH-Terminalsitzung, die mit dem Gerät verbunden ist, das Sie testen möchten.

Um die Konnektivität eines Geräts mit Ihrem Gerätedatenendpunkt zu testen.

- Finden Sie den Datenendpunkt Ihres Geräts
- Testen Sie die Verbindung schnell
- Laden Sie die App herunter, um die Verbindung zu Ihrem Gerätedatenendpunkt und Port zu testen
- Testen Sie die Verbindung zu Ihrem Gerätedatenendpunkt und Port

## Finden Sie den Datenendpunkt Ihres Geräts

In diesem Verfahren wird erklärt, wie Sie Ihren Gerätedatenendpunkt in der AWS IoT Konsole finden, um die Verbindung zu Ihrem IoT-Gerät zu testen.

So finden Sie Ihren Gerätedatenendpunkt

1. Gehen Sie in der AWS IoT Konsole im Bereich Connect zu Domain-Konfigurationen.
2. Gehen Sie auf der Seite Domain-Konfigurationen zum Container Domain-Konfigurationen und kopieren Sie den Domainnamen. Ihr Endpunktwert ist einzigartig für Sie AWS-Konto und ähnelt diesem Beispiel:`a3qEXAMPLEsffp-ats.iot.eu-west-1.amazonaws.com`.
3. Gehen Sie wie folgt vor, um Ihren Datenbank-Endpunkt für die Verwendung zu speichern.

## Testen Sie die Verbindung schnell

Dieses Verfahren testet die allgemeine Konnektivität mit Ihrem Gerätedatenendpunkt, nicht jedoch den spezifischen Port, den Ihre Geräte verwenden werden. Dieser Test verwendet ein gängiges Programm und reicht normalerweise aus, um herauszufinden, ob Ihre Geräte eine Verbindung mit AWS IoT herstellen können.

Wenn Sie die Konnektivität mit dem spezifischen Port testen möchten, den Ihre Geräte verwenden werden, überspringen Sie dieses Verfahren und fahren Sie mit Laden Sie die App herunter, um die Verbindung zu Ihrem Gerätedatenendpunkt und Port zu testen fort.

Um den Gerätedatenendpunkt schnell zu testen

1. Ersetzen Sie in einem Terminal- oder Befehlszeilenfenster auf Ihrem Gerät den Beispielendpunkt für Gerätedaten (*a3qEXAMPLEsffp-ats.iot.eu-west-1.amazonaws.com*) durch den Gerätedatenendpunkt für Ihr Konto und geben Sie dann diesen Befehl ein.

   Linux

   ```
   ping -c 5 a3qEXAMPLEsffp-ats.iot.eu-west-1.amazonaws.com
   ```

   Windows

   ```
   ping -n 5 a3qEXAMPLEsffp-ats.iot.eu-west-1.amazonaws.com
   ```

2. Wenn von `ping` eine Ausgabe ähnlich der folgenden angezeigt wird, wurde erfolgreich eine Verbindung zu Ihrem Gerätedatenendpunkt hergestellt. Es hat zwar nicht AWS IoT direkt mit dem Server kommuniziert, aber er hat den Server gefunden, und es AWS IoT ist wahrscheinlich, dass er über diesen Endpunkt erreichbar ist.

   ```
   PING a3qEXAMPLEsffp-ats.iot.eu-west-1.amazonaws.com (xx.xx.xxx.xxx) 56(84) bytes of
    data.
   64 bytes from ec2-EXAMPLE-218.eu-west-1.compute.amazonaws.com (xx.xx.xxx.xxx):
    icmp_seq=1 ttl=231 time=127 ms
   64 bytes from ec2-EXAMPLE-218.eu-west-1.compute.amazonaws.com (xx.xx.xxx.xxx):
    icmp_seq=2 ttl=231 time=127 ms
   64 bytes from ec2-EXAMPLE-218.eu-west-1.compute.amazonaws.com (xx.xx.xxx.xxx):
    icmp_seq=3 ttl=231 time=127 ms
   64 bytes from ec2-EXAMPLE-218.eu-west-1.compute.amazonaws.com (xx.xx.xxx.xxx):
    icmp_seq=4 ttl=231 time=127 ms
   64 bytes from ec2-EXAMPLE-218.eu-west-1.compute.amazonaws.com (xx.xx.xxx.xxx):
    icmp_seq=5 ttl=231 time=127 ms
   ```

   Wenn Sie mit diesem Ergebnis zufrieden sind, können Sie den Test hier beenden.

Wenn Sie die Konnektivität mit dem spezifischen Port testen möchten, der von AWS IoT verwendet wird, fahren Sie fort mit Laden Sie die App herunter, um die Verbindung zu Ihrem Gerätedatenendpunkt und Port zu testen.

3. Wenn von `ping` keine erfolgreiche Ausgabe zurückgegeben wurde, überprüfen Sie den Endpunktwert, um sicherzustellen, dass Sie den richtigen Endpunkt haben, und überprüfen Sie die Verbindung des Geräts mit dem Internet.

## Laden Sie die App herunter, um die Verbindung zu Ihrem Gerätedatenendpunkt und Port zu testen

Ein gründlicherer Konnektivitätstest kann mit `nmap` durchgeführt werden. Mit diesem Verfahren wird getestet, ob `nmap` auf Ihrem Gerät installiert ist.

Um auf dem Gerät nach **`nmap`** zu suchen

1. Geben Sie in einem Terminal- oder Befehlszeilenfenster auf dem Gerät, das Sie testen möchten, diesen Befehl ein, um zu überprüfen, ob `nmap` installiert ist.

   ```
   nmap --version
   ```

2. Wenn Sie eine Ausgabe ähnlich der folgenden sehen, ist `nmap` installiert und Sie können mit the section called “Testen Sie die Verbindung zu Ihrem Gerätedatenendpunkt und Port” fortfahren.

   ```
   Nmap version 6.40 ( http://nmap.org )
   Platform: x86_64-koji-linux-gnu
   Compiled with: nmap-liblua-5.2.2 openssl-1.0.2k libpcre-8.32 libpcap-1.5.3 nmap-
   libdnet-1.12 ipv6
   Compiled without:
   Available nsock engines: epoll poll select
   ```

3. Wird Ihnen keine ähnliche Antwort angezeigt wie im vorherigen Schritt, müssen Sie die Installation von `nmap` auf dem Gerät ausführen. Wählen Sie das Verfahren für das Betriebssystem Ihres Geräts aus.

### Linux

Dieser Vorgang erfordert, dass Sie über die Berechtigung verfügen, Software auf dem Computer zu installieren.

Um nmap auf Ihrem Linux-Computer zu installieren

1. Geben Sie in einem Terminal- oder Befehlszeilenfenster auf Ihrem Gerät den Befehl ein, der der Linux-Version entspricht, die auf dem Gerät ausgeführt wird.

   a. Debian oder Ubuntu:

   ```
   sudo apt install nmap
   ```

   b. Cent OS oder RHEL:

   ```
   sudo yum install nmap
   ```

2. Testen Sie die Installation mit diesem Befehl:

   ```
   nmap --version
   ```

3. Wenn Sie eine Ausgabe ähnlich der folgenden sehen, ist nmap installiert und Sie können mit the section called “Testen Sie die Verbindung zu Ihrem Gerätedatenendpunkt und Port” fortfahren.

   ```
   Nmap version 6.40 ( http://nmap.org )
   Platform: x86_64-koji-linux-gnu
   Compiled with: nmap-liblua-5.2.2 openssl-1.0.2k libpcre-8.32 libpcap-1.5.3 nmap-
   libdnet-1.12 ipv6
   Compiled without:
   Available nsock engines: epoll poll select
   ```

macOS

Dieser Vorgang erfordert, dass Sie über die Berechtigung verfügen, Software auf dem Computer zu installieren.

nmap-Installation auf Ihrem macOS-Computer

1. Öffnen Sie in einem Browser https://nmap.org/download#macosx und laden Sie das neueste stabile Installationsprogramm herunter.

   Wenn Sie dazu aufgefordert werden, wählen Sie Öffnen mit DiskImageInstaller.

2. Verschieben Sie das Paket im Installationsfenster in den Ordner Applications.

3. Suchen Sie im Finder das `nmap-xxxx-mpkg` Paket im Ordner Anwendungen. Ctrl-click Sie auf das Paket und wählen Sie Öffnen, um das Paket zu öffnen.
4. Überprüfen Sie das Sicherheitsdialogfeld. Wenn Sie bereit für die Installation von nmap sind, wählen Sie Öffnen, um nmap zu installieren.
5. Testen Sie in Terminal die Installation mit diesem Befehl.

   ```
   nmap --version
   ```

6. Wenn Sie eine Ausgabe ähnlich der folgenden sehen, ist `nmap` installiert und Sie können mit the section called “Testen Sie die Verbindung zu Ihrem Gerätedatenendpunkt und Port” fortfahren.

   ```
   Nmap version 7.92 ( https://nmap.org )
   Platform: x86_64-apple-darwin17.7.0
   Compiled with: nmap-liblua-5.3.5 openssl-1.1.1k nmap-libssh2-1.9.0 libz-1.2.11
    nmap-libpcre-7.6 nmap-libpcap-1.9.1 nmap-libdnet-1.12 ipv6 Compiled without:
   Available nsock engines: kqueue poll select
   ```

Windows

Dieser Vorgang erfordert, dass Sie über die Berechtigung verfügen, Software auf dem Computer zu installieren.

Um nmap auf Ihrem Windows-Computer zu installieren

1. Öffnen Sie in einem Browser https://nmap.org/download#windows und laden Sie die neueste stabile Version des Setup-Programms herunter.

   Wenn Sie dazu aufgefordert werden, wählen Sie Datei speichern. Nachdem die Datei heruntergeladen wurde, öffnen Sie sie im Download-Ordner.
2. Nachdem der Download der Setup-Datei abgeschlossen ist, öffnen Sie den Download nmap-xxxx-setup.exe um die App zu installieren.
3. Übernehmen Sie bei der Installation des Programms die Standardeinstellungen.

   Sie benötigen die Npcap-App für diesen Test nicht. Sie können diese Option deaktivieren, wenn Sie sie nicht installieren möchten.
4. Testen Sie in Command die Installation mit diesem Befehl.

```
nmap --version
```

5. Wenn Sie eine Ausgabe ähnlich der folgenden sehen, ist nmap installiert und Sie können mit the section called “Testen Sie die Verbindung zu Ihrem Gerätedatenendpunkt und Port” fortfahren.

```
Nmap version 7.92 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.3.5 openssl-1.1.1k nmap-libssh2-1.9.0 nmap-
libz-1.2.11 nmap-libpcre-7.6 Npcap-1.50 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: iocp poll select
```

## Testen Sie die Verbindung zu Ihrem Gerätedatenendpunkt und Port

Dieses Verfahren testet die Verbindung Ihres IoT-Geräts mit Ihrem Gerätedatenendpunkt über den ausgewählten Port.

Um den Endpunkt und den Port Ihrer Gerätedaten zu testen

1. Ersetzen Sie in einem Terminal- oder Befehlszeilenfenster auf Ihrem Gerät den Beispielendpunkt für Gerätedaten (*a3qEXAMPLEsffp-ats.iot.eu-west-1.amazonaws.com*) durch den Gerätedatenendpunkt für Ihr Konto und geben Sie dann diesen Befehl ein.

```
nmap -p 8443 a3qEXAMPLEsffp-ats.iot.eu-west-1.amazonaws.com
```

2. Wenn von nmap eine Ausgabe ähnlich der folgenden angezeigt wird, konnte am ausgewählten Port von nmap erfolgreich eine Verbindung zu Ihrem Gerätedatenendpunkt hergestellt werden.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-18 16:23 Pacific Standard Time
Nmap scan report for a3qEXAMPLEsffp-ats.iot.eu-west-1.amazonaws.com
 (xx.xxx.147.160)
Host is up (0.036s latency).
Other addresses for a3qEXAMPLEsffp-ats.iot.eu-west-1.amazonaws.com (not scanned):
 xx.xxx.134.144 xx.xxx.55.139 xx.xxx.110.235 xx.xxx.174.233 xx.xxx.74.65
 xx.xxx.122.179 xx.xxx.127.126
rDNS record for xx.xxx.147.160: ec2-EXAMPLE-160.eu-west-1.compute.amazonaws.com

PORT     STATE SERVICE
```

```
8443/tcp open  https-alt
MAC Address: 00:11:22:33:44:55 (Cimsys)

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
```

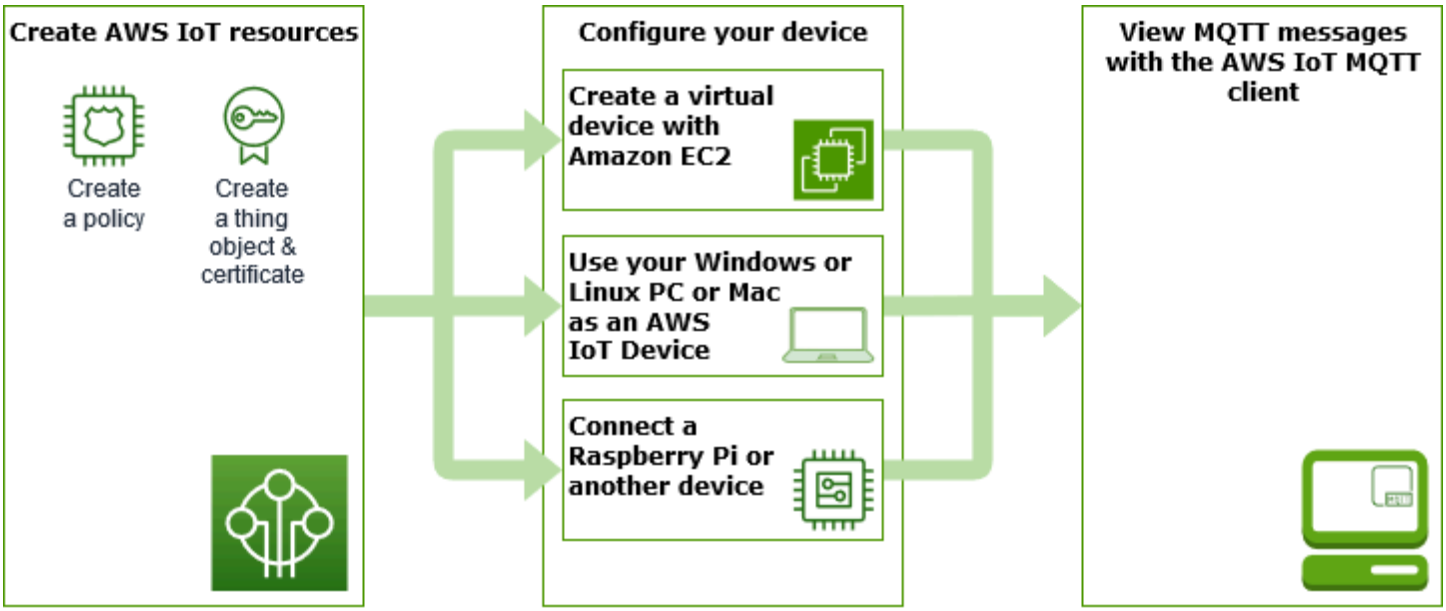
3. Wenn von nmap keine erfolgreiche Ausgabe zurückgegeben wurde, überprüfen Sie den Endpunktwert, um sicherzustellen, dass Sie den richtigen Endpunkt haben, und überprüfen Sie die Verbindung Ihres Geräts mit dem Internet.

Sie können andere Anschlüsse an Ihrem Gerätedatenendpunkt testen, z. B. Port 443, den primären HTTPS-Port, indem Sie den in Schritt 1 verwendeten Port durch den Port **8443** ersetzen, den Sie testen möchten.

## Erfahren Sie AWS IoT Core in praktischen Tutorials mehr

In diesem Tutorial installieren Sie die Software und erstellen die AWS IoT Ressourcen, die erforderlich sind, um ein Gerät anzuschließen, mit AWS IoT Core dem es MQTT-Nachrichten senden und empfangen kann. AWS IoT Core Sie werden die Nachrichten im MQTT-Client in der AWS IoT Konsole sehen.

Sie können damit rechnen, 20 bis 30 Minuten für dieses Tutorial aufzuwenden. Wenn Sie ein IoT-Gerät oder einen Raspberry Pi verwenden, kann dieses Tutorial länger dauern, wenn Sie beispielsweise das Betriebssystem installieren und das Gerät konfigurieren müssen.



Dieses Tutorial eignet sich am besten für Entwickler, die sich AWS IoT Core zunächst mit fortgeschritteneren Funktionen wie der Regel-Engine und Schatten vertraut machen möchten. Dieses Tutorial bereitet Sie darauf vor, mehr über andere Dienste zu erfahren AWS IoT Core und zu erfahren, wie es mit anderen AWS Diensten interagiert, indem es die Schritte detaillierter erklärt als das Schnellstart-Tutorial. Wenn Sie nur ein schnelles Hello World-Erlebnis suchen, probieren Sie Probieren Sie das AWS IoT Core Quick Connect-Tutorial aus aus.

Nachdem Sie Ihre AWS-Konto und AWS IoT Konsole eingerichtet haben, folgen Sie diesen Schritten, um zu erfahren, wie Sie ein Gerät anschließen und Nachrichten senden AWS IoT Core können.

Nächste Schritte

- Wählen Sie, welche Geräteoption für Sie am besten geeignet ist
- the section called “AWS IoT Ressourcen erstellen”wenn Sie kein virtuelles Gerät mit Amazon erstellen möchten EC2
- the section called “Konfigurieren Ihres Geräts”
- the section called “MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen”

Weitere Informationen zu AWS IoT Core finden Sie unter Was ist AWS IoT Core?

## Welche Geräteoption ist für Sie am besten geeignet?

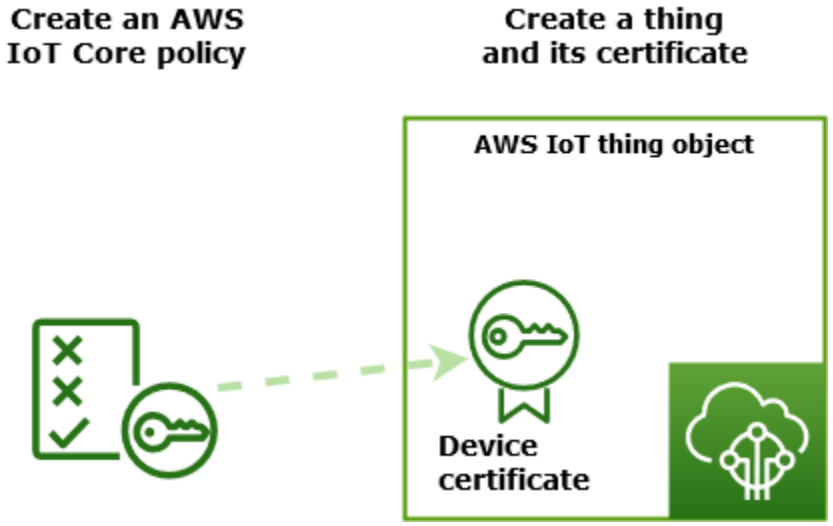
Wenn Sie sich nicht sicher sind, welche Option Sie wählen sollen, können Sie anhand der folgenden Liste der Vor- und Nachteile der einzelnen Optionen entscheiden, welche für Sie am besten geeignet ist.

| Option | Dies könnte eine gute Option sein, wenn: | Dies ist möglicherweise keine gute Option, wenn: |
| --- | --- | --- |
| the section called “Erstelle n Sie ein virtuelles Gerät mit Amazon EC2” | • Sie kein eigenes Gerät zum Testen haben.<br>• Sie keine Software auf Ihrem eigenen System installieren möchten.<br>• Sie auf einem Linux-Betriebssystem testen möchten. | • Sie mit einer Befehlsze ilenschnittstelle vertraut sind.<br>• Sie nicht möchten, dass zusätzliche AWS Gebühren anfallen. |

| Option | Dies könnte eine gute Option sein, wenn: | Dies ist möglicherweise keine gute Option, wenn: |
| --- | --- | --- |
| | | • Sie nicht auf einem Linux-Betriebssystem testen möchten. |
| the section called “Verwenden Sie Ihren Windows- oder Linux-PC oder Mac als Gerät AWS IoT” | • Sie nicht möchten, dass zusätzliche AWS Gebühren anfallen.<br>• Sie keine zusätzlichen Geräte konfigurieren möchten. | • Sie keine Software auf Ihrem PC installieren möchten.<br>• Sie eine repräsentativere Testplattform möchten. |
| the section called “Verbinden eines Raspberry Pi oder eines anderes Gerätes” | • Sie möchten AWS IoT mit einem echten Gerät testen.<br>• Sie bereits ein Gerät haben, mit dem Sie testen können.<br>• Sie mit der Integration von Hardware in Systeme Erfahrung haben. | • Sie kein Gerät kaufen oder konfigurieren möchten, nur um es auszuprobieren.<br>• Sie möchten vorerst AWS IoT so einfach wie möglich testen. |

## AWS IoT Ressourcen erstellen

In diesem Tutorial erstellen Sie die AWS IoT Ressourcen, die ein Gerät benötigt, um eine Verbindung zu Nachrichten herzustellen AWS IoT Core und sie auszutauschen.




1. Erstellen Sie ein AWS IoT Richtliniendokument, das Ihr Gerät zur Interaktion mit AWS IoT Diensten autorisiert.
2. Erstellen Sie ein Ding-Objekt AWS IoT und sein X.509-Gerätezertifikat und hängen Sie dann das Richtliniendokument an. Das Ding-Objekt ist die virtuelle Darstellung Ihres Geräts in der AWS IoT Registrierung. Das Zertifikat authentifiziert Ihr Gerät gegenüber AWS IoT Core, und das Richtliniendokument autorisiert Ihr Gerät zur Interaktion mit. AWS IoT

> **Note**
>
> Wenn Sie the section called “Erstellen Sie ein virtuelles Gerät mit Amazon EC2” planen, können Sie diese Seite überspringen und mit the section called “Konfigurieren Ihres Geräts”weitermachen. Sie werden diese Ressourcen erstellen, wenn Sie Ihr virtuelles Objekt erstellen.

In diesem Tutorial werden die Ressourcen mithilfe der AWS IoT Konsole erstellt. AWS IoT Wenn Ihr Gerät einen Webbrowser unterstützt, ist es möglicherweise einfacher, dieses Verfahren im Webbrowser des Geräts auszuführen, da Sie die Zertifikatsdateien direkt auf Ihr Gerät herunterladen können. Wenn Sie dieses Verfahren auf einem anderen Computer ausführen, müssen Sie die Zertifikatsdateien auf Ihr Gerät kopieren, bevor sie von der Beispiel-App verwendet werden können.

## Erstellen Sie eine AWS IoT Richtlinie

Geräte verwenden ein X.509-Zertifikat zur Authentifizierung. AWS IoT Core Mit dem Zertifikat AWS IoT sind Richtlinien verknüpft. Diese Richtlinien legen fest, welche AWS IoT Operationen, wie das

Abonnieren oder Veröffentlichen von MQTT-Themen, das Gerät ausführen darf. Ihr Gerät legt sein Zertifikat vor, wenn es eine Verbindung herstellt und Nachrichten an sendet AWS IoT Core.

Folgen Sie den Schritten, um eine Richtlinie zu erstellen, die es Ihrem Gerät ermöglicht, die zur Ausführung des Beispielprogramms erforderlichen AWS IoT -Vorgänge auszuführen. Sie müssen die AWS IoT -Richtlinie erstellen, bevor Sie sie an das Gerätezertifikat anhängen können, das Sie später erstellen werden.

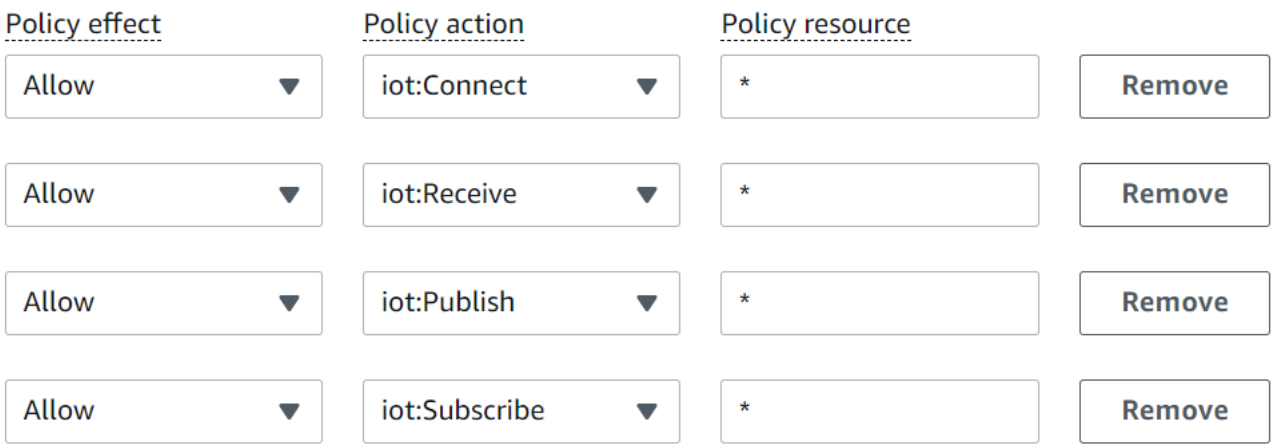
Um eine AWS IoT Richtlinie zu erstellen

1. Wählen Sie in der AWS IoT -Konsole im linken Menü Sicherheit und dann Richtlinien aus.
2. Wählen Sie auf der Seite Sie haben noch keine Richtlinie die Option Richtlinie erstellen.

   Wenn Ihr Konto bereits Richtlinien hat, wählen Sie Richtlinie erstellen aus.
3. Auf der Seite Richtlinie erstellen:

   1. Geben Sie im Abschnitt Richtlinieneigenschaften im Feld Richtlinienname einen Namen für die Richtlinie ein (z. B. **`My_Iot_Policy`**). Verwenden Sie keine personenbezogenen Informationen in Ihren Richtliniennamen.
   2. Erstellen Sie im Abschnitt Richtliniendokument die Richtlinienerklärungen, die Ressourcen den Zugriff auf AWS IoT Core -Operationen gewähren oder verweigern. Gehen Sie wie folgt vor, um eine Richtlinienerklärung zu erstellen, die allen Clients die Möglichkeit einräumt, **`iot:Connect`** auszuführen:
      - Wählen Sie im Feld Richtlinieneffekt die Option Zulassen aus. Dadurch können alle Clients, deren Zertifikat diese Richtlinie an ihr Zertifikat angehängt hat, die Aktion ausführen, die im Feld Richtlinienaktion aufgeführt ist.
      - Wählen Sie im Feld Richtlinienaktion eine Richtlinienaktion wie **`iot:Connect`**. Richtlinienaktionen sind die Aktionen, für deren Ausführung Ihr Gerät eine Genehmigung benötigt, wenn es das Beispielprogramm aus dem Geräte-SDK ausführt.
      - Geben Sie im Feld Richtlinienressource einen Amazon-Ressourcennamen (ARN) oder **`*`** ein. Ein **`*`**, um einen beliebigen Client (Gerät) auszuwählen.

      Um die Richtlinienerklärungen für **`iot:Receive`**, **`iot:Publish`** und **`iot:Subscribe`** zu erstellen, wählen Sie Neue Erklärung hinzufügen und wiederholen Sie die Schritte.




> **Note**
>
> In diesem Schnellstart wird der Einfachheit halber der Platzhalter (*) verwendet. Um die Sicherheit zu erhöhen, sollten Sie einschränken, welche Clients (Geräte) Verbindungen herstellen und Nachrichten veröffentlichen können, indem Sie einen Client-ARN anstelle des Platzhalterzeichens als Ressource angeben. Der Kunde ARNs folgt diesem Format:`arn:aws:iot:`*`your-region`*`:`*`your-aws-account`*`:client/`*`my-client-id`*.
> Sie müssen jedoch zuerst die Ressource (z. B. ein Client-Gerät oder einen Objektschatten) erstellen, bevor Sie ihren ARN einer Richtlinie zuweisen können. Weitere Informationen finden Sie unter AWS IoT Core -Aktionsressourcen.

4. Nachdem Sie die Informationen für Ihre Richtlinie eingegeben haben, wählen Sie Erstellen.

Weitere Informationen finden Sie unter Wie AWS IoT funktioniert mit IAM.

## Dies erstellt ein Objekt

Geräte, mit AWS IoT Core denen verbunden ist, werden durch Dingobjekte in der AWS IoT Registrierung dargestellt. Ein Objekt stellt ein bestimmtes Gerät oder eine logische Entität dar. Es kann ein physisches Gerät oder ein Sensor sein (beispielsweise eine Glühbirne oder ein Wandschalter). Es kann sich auch um eine logische Einheit handeln, z. B. eine Instanz einer Anwendung oder eine physische Entität AWS IoT, die keine Verbindung zu anderen Geräten herstellt, die dies tun (z. B. ein Auto mit Motorsensoren oder einem Bedienfeld).

Um ein Ding in der AWS IoT Konsole zu erstellen

1. Wählen Sie in der AWS IoT -Konsole im linken Menü Alle Geräte und dann Objekte aus.
2. Wählen Sie auf der Seite Objekte die Option Objekte erstellen aus.
3. Wählen Sie auf der Seite Objekte erstellen den Eintrag Einzelnes Objekt erstellen und dann Weiter aus.
4. Geben Sie auf der Seite Objekteigenschaften angeben unter Objektname einen Namen für Ihr Objekt ein, z. B. **`MyIotThing`**.

   Wählen Sie die Namen der Objekte sorgfältig aus, da Sie den Namen eines Objekts später nicht mehr ändern können.

   Um den Namen eines Objekts zu ändern, müssen Sie ein neues Objekt erstellen, diesem den neuen Namen geben und dann das alte Objekt löschen.

   > **Note**
   >
   > Verwenden Sie keine personenbezogenen Informationen in Ihren Objektnamen. Der Name der Sache kann in unverschlüsselten Mitteilungen und Berichten vorkommen.

5. Lassen Sie die restlichen Felder auf dieser Seite leer. Wählen Sie Weiter aus.
6. Wählen Sie auf der Seite Gerätezertifikat konfigurieren — optional die Option Neues Zertifikat automatisch generieren (empfohlen) aus. Wählen Sie Weiter aus.
7. Wählen Sie auf der Seite Richtlinien an Zertifikat anhängen — optional die Richtlinie aus, die Sie im vorherigen Abschnitt erstellt haben. In diesem Abschnitt erhielt die Richtlinie den Namen **`My_Iot_Policy`**. Wählen Sie Objekt erstellen aus.
8. Gehen Sie auf der Seite Zertifikate und Schlüssel herunterladen wie folgt vor:

   1. Laden Sie die einzelnen Zertifikat- und Schlüsseldateien herunter und speichern Sie sie für später. Sie müssen diese Dateien auf Ihrem Gerät installieren.

      Wenn Sie Ihre Zertifikatsdateien speichern, geben Sie ihnen die Namen in der folgenden Tabelle. Dies sind die Dateinamen, die in späteren Beispielen verwendet wurden.

Namen der Zertifikatsdateien

| Datei | Dateipfad |
|---|---|
| Privater Schlüssel | `private.pem.key` |
| Öffentlicher Schlüssel | (in diesen Beispielen nicht verwendet) |
| Gerätezertifikat | `device.pem.crt` |
| CA-Stammzertifikat | `Amazon-root-CA-1.pem` |

2. Um die Root-CA-Datei für diese Dateien herunterzuladen, wählen Sie den Download-Link der Root-CA-Zertifikatsdatei, die dem Typ des Datenendpunkts und der Cipher Suite entspricht, die Sie verwenden. Wählen Sie in diesem Tutorial rechts neben RSA 2048 bit key: Amazon Root CA 1 die Option Herunterladen und laden Sie die Zertifikatsdatei RSA 2048 bit key: Amazon Root CA 1 herunter.

   > **Important**
   >
   > Sie müssen die Zertifikatsdateien speichern, bevor Sie diese Seite verlassen. Nachdem Sie diese Seite in der Konsole verlassen haben, haben Sie keinen Zugriff mehr auf die Zertifikatsdateien.
   > Wenn Sie vergessen haben, die in diesem Schritt erstellten Zertifikatsdateien herunterzuladen, müssen Sie diesen Konsolenbildschirm verlassen, zur Liste der Objekte in der Konsole wechseln, das von Ihnen erstellte Objekt löschen und diesen Vorgang dann von vorne beginnen.

3. Wählen Sie Erledigt aus.

Nachdem Sie dieses Verfahren abgeschlossen haben, sollte das neue Objekt in Ihrer Liste der Objekte angezeigt werden.

## Konfigurieren Ihres Geräts

In diesem Abschnitt wird beschrieben, wie Sie Ihr Gerät für die Verbindung mit AWS IoT Core konfigurieren. Wenn Sie damit beginnen möchten, AWS IoT Core aber noch kein Gerät haben,

können Sie mithilfe von Amazon ein virtuelles Gerät erstellen EC2 oder Ihren Windows-PC oder Mac als IoT-Gerät verwenden.

Wählen Sie die beste Geräteoption aus, die Sie ausprobieren möchten AWS IoT Core. Natürlich können Sie alle ausprobieren, aber versuchen Sie es jeweils nur mit einer. Wenn Sie sich nicht sicher sind, welche Geräteoption für Sie am besten geeignet ist, lesen Sie, wie Sie die beste Geräteoption auswählen können, und kehren Sie dann zu dieser Seite zurück.

Geräteoptionen

- Erstellen Sie ein virtuelles Gerät mit Amazon EC2
- Verwenden Sie Ihren Windows- oder Linux-PC oder Mac als Gerät AWS IoT
- Verbinden eines Raspberry Pi oder eines anderes Gerätes

## Erstellen Sie ein virtuelles Gerät mit Amazon EC2

In diesem Tutorial erstellen Sie eine EC2 Amazon-Instanz, die als Ihr virtuelles Gerät in der Cloud dient.

Um dieses Tutorial abzuschließen, benötigen Sie eine AWS-Konto. Wenn dies nicht der Fall ist, führen Sie die unter Einrichten AWS-Konto beschriebenen Schritte aus, bevor Sie fortfahren.

In diesem Tutorial führen Sie die folgenden Aktivitäten durch:

- Eine EC2 Amazon-Instance einrichten
- Installieren Sie Git, Node.js und konfigurieren Sie AWS CLI
- Erstellen Sie AWS IoT Ressourcen für Ihr virtuelles Gerät
- Installieren Sie das AWS IoT Geräte-SDK für JavaScript
- Ausführen der Beispielanwendungen
- Nachrichten aus der Beispiel-App in der AWS IoT -Konsole anzeigen

### Eine EC2 Amazon-Instance einrichten

Die folgenden Schritte zeigen Ihnen, wie Sie eine EC2 Amazon-Instance erstellen, die anstelle eines physischen Geräts als Ihr virtuelles Gerät fungiert.

Wenn Sie zum ersten Mal eine EC2 Amazon-Instance erstellen, sind die Anweisungen unter Erste Schritte mit Amazon EC2 Linux-Instances möglicherweise hilfreicher.

So starten Sie eine Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Erweitern Sie im Konsolenmenü auf der linken Seite den Abschnitt Instances und wählen Sie Instances aus. Wählen Sie im Instances-Dashboard rechts die Option Instances starten aus, um eine Liste der Basiskonfigurationen anzuzeigen.
3. Geben Sie im Abschnitt Name und Tags einen Namen für die Instance ein und fügen Sie optional Tags hinzu.
4. Wählen Sie im Abschnitt Anwendungs- und Betriebssystem-Images (Amazon Machine Image) eine AMI-Vorlage für Ihre Instance aus, z. B. Amazon Linux 2 AMI (HVM). Diese AMIs sind als „Zur kostenlosen Nutzung berechtigt" gekennzeichnet.
5. Auf der Seite Instance Type können Sie die Hardware-Konfiguration Ihrer Instance auswählen. Wählen Sie den Typ `t2.micro` aus (Standardeinstellung). Beachten Sie, dass dieser Instance-Typ über die Berechtigung für das kostenlose Kontingent verfügt.
6. Wählen Sie im Abschnitt Schlüsselpaar (Anmeldung) einen Schlüsselpaar-Namen aus der Dropdown-Liste oder wählen Sie Neues Schlüsselpaar erstellen, um ein neues Schlüsselpaar zu erstellen. Wenn Sie ein neues Schlüsselpaar erstellen, stellen Sie sicher, dass Sie die private Schlüsseldatei herunterladen und an einem sicheren Ort speichern, da dies Ihre einzige Möglichkeit ist, sie herunterzuladen und zu speichern. Sie müssen den Namen für Ihr Schlüsselpaar beim Starten einer Instance angeben. Der entsprechende private Schlüssel muss jedes Mal angegeben werden, wenn Sie eine Verbindung mit der Instance herstellen.

   > ⚠ Warning
   >
   > Wählen Sie nicht die Option Ohne Schlüsselpaar fortfahren aus. Wenn Sie Ihre Instance ohne Schlüsselpaar starten, können Sie keine Verbindung zu ihr herstellen.

7. In den Abschnitten Netzwerkeinstellungen und Speicher konfigurieren können Sie die Standardeinstellungen beibehalten. Sobald Sie bereit sind, wählen Sie Instance starten aus.
8. Auf einer Bestätigungsseite wird Ihnen mitgeteilt, dass die Instance gestartet wird. Wählen Sie View Instances aus, um die Bestätigungsseite zu schließen und zur Konsole zurückzukehren.
9. Auf dem Bildschirm Instances können Sie den Status des Starts anzeigen. Es dauert einige Zeit, bis die Instance startet. Wenn Sie eine Instance starten, lautet ihr anfänglicher Status `pending`. Nachdem die Instance gestartet wurde, ändert sich der Status in `running`. Sie erhält dann einen öffentlichen DNS-Namen. (Wenn die Spalte Public DNS (IPv4) ausgeblendet ist, wählen Sie

Spalten ein-/ausblenden (das zahnradförmige Symbol) in der oberen rechten Ecke der Seite und wählen Sie dann Public DNS () aus.) IPv4

10. Es kann einige Minuten dauern, bis die Instance für die Verbindungsherstellung bereit ist. Prüfen Sie, ob die Instance die Statusprüfungen bestanden hat. Sie finden diese Information in der Spalte Status Checks.

    Nachdem Ihre neue Instance die Statusprüfungen bestanden hat, fahren Sie mit dem nächsten Verfahren fort und stellen Sie eine Verbindung zu ihr her.

So stellen Sie eine Verbindung zu Ihrer Instance her

Sie können über den browserbasierten Client eine Verbindung zu einer Instance herstellen, indem Sie die Instance in der EC2 Amazon-Konsole auswählen und die Verbindung über Amazon EC2 Instance Connect herstellen. Instance Connect verarbeitet die Berechtigungen und stellt eine erfolgreiche Verbindung bereit.

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Menü Instances aus.
3. Wählen Sie die Instance und Connect (Verbinden) aus.
4. Wählen Sie Amazon EC2 Instance Connect, Connect.

Sie sollten jetzt ein Amazon EC2 Instance Connect-Fenster haben, das bei Ihrer neuen EC2 Amazon-Instance angemeldet ist.

Installieren Sie Git, Node.js und konfigurieren Sie AWS CLI

In diesem Abschnitt installieren Sie Git und Node.js auf Ihrer Linux-Instance.

So installieren Sie Git

1. Aktualisieren Sie Ihre  EC2 Instance in Ihrem Amazon Instance Connect-Fenster mit dem folgenden Befehl.

   ```
   sudo yum update -y
   ```

2. Installieren Sie Git in Ihrem Amazon EC2 Instance Connect-Fenster mit dem folgenden Befehl.

   ```
   sudo yum install git -y
   ```

3. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Git installiert wurde und ob es sich um die aktuelle Version von Git handelt:

```
git --version
```

Installieren von Node.js

1. Installieren Sie in Ihrem Amazon EC2 Instance Connect-Fenster den Node Version Manager (nvm) mit dem folgenden Befehl.

```
curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.34.0/install.sh | bash
```

   Wir verwenden nvm zum Installieren von Node.js, da nvm mehrere Versionen von Node.js installieren kann und die Möglichkeit bietet, zwischen diesen zu wechseln.

2. Aktivieren Sie nvm in Ihrem Amazon EC2 Instance Connect-Fenster mit diesem Befehl.

```
. ~/.nvm/nvm.sh
```

3. Verwenden Sie in Ihrem Amazon EC2 Instance Connect-Fenster nvm, um die neueste Version von Node.js mithilfe dieses Befehls zu installieren.

```
nvm install 16
```

> **Note**
>
> Dadurch wird die neueste LTS-Version von Node.js installiert.

   Beim Installieren von Node.js wird auch der Node Package Manager (npm) installiert, sodass Sie bei Bedarf zusätzliche Module installieren können.

4. Testen Sie in Ihrem Amazon EC2 Instance Connect-Fenster, ob Node.js installiert ist und ordnungsgemäß ausgeführt wird, indem Sie diesen Befehl verwenden.

```
node -e "console.log('Running Node.js ' + process.version)"
```

Dieses Tutorial erfordert Node v10.0 oder neuer. Weitere Informationen finden Sie unter Tutorial: Node.js auf einer EC2 Amazon-Instance einrichten.

Um zu konfigurieren AWS CLI

Auf Ihrer EC2 Amazon-Instance ist der AWS CLI vorinstalliert. Sie müssen jedoch Ihr AWS CLI Profil vervollständigen. Weitere Informationen zum Konfigurieren Ihrer CLI finden Sie unter Konfiguration von AWS CLI.

1. Das folgende Beispiel zeigt Beispielwerte. Ersetzen Sie sie mit Ihren eigenen Werten. Sie finden diese Werte in Ihrer AWS -Konsole in Ihren Kontoinformationen unter Sicherheitsanmeldedaten.

   Geben Sie in Ihrem Amazon EC2 Instance Connect-Fenster diesen Befehl ein:

   ```
   aws configure
   ```

   Geben Sie dann an den angezeigten Eingabeaufforderungen die Werte aus Ihrem Konto ein.

   ```
   AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
   AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
   Default region name [None]: us-west-2
   Default output format [None]: json
   ```

2. Sie können Ihre AWS CLI Konfiguration mit diesem Befehl testen:

   ```
   aws iot describe-endpoint --endpoint-type iot:Data-ATS
   ```

   Wenn Ihr korrekt konfiguriert AWS CLI ist, sollte der Befehl eine Endpunktadresse von Ihrem zurückgeben AWS-Konto.

Erstellen Sie AWS IoT Ressourcen für Ihr virtuelles Gerät

In diesem Abschnitt wird beschrieben, wie Sie AWS CLI das Ding-Objekt und seine Zertifikatsdateien direkt auf dem virtuellen Gerät erstellen können. Dies erfolgt direkt auf dem Gerät, um mögliche Komplikationen zu vermeiden, die entstehen könnten, wenn sie von einem anderen Computer auf das Gerät kopiert werden. In diesem Abschnitt erstellen Sie die folgenden Ressourcen für Ihr virtuelles Gerät:

- Ein Ding-Objekt, in dem Ihr virtuelles Gerät dargestellt AWS IoT werden soll.
- Ein Zertifikat zur Authentifizierung Ihres virtuellen Geräts.
- Ein Richtliniendokument, mit dem Sie Ihr virtuelles Gerät autorisieren, eine Verbindung zu AWS IoT herzustellen und Nachrichten zu veröffentlichen, zu empfangen und zu abonnieren.

Um ein AWS IoT Ding-Objekt in Ihrer Linux-Instanz zu erstellen

Geräte, mit AWS IoT denen eine Verbindung besteht, werden durch Ding-Objekte in der AWS IoT Registrierung dargestellt. Ein Objekt stellt ein bestimmtes Gerät oder eine logische Entität dar. In diesem Fall repräsentiert Ihr Ding-Objekt Ihr virtuelles Gerät, diese EC2 Amazon-Instance.

1. Führen Sie in Ihrem Amazon EC2 Instance Connect-Fenster den folgenden Befehl aus, um Ihr Ding-Objekt zu erstellen.

   ```
   aws iot create-thing --thing-name "MyIotThing"
   ```

2. Die JSON-Antwort sollte wie folgt aussehen:

   ```
   {
       "thingArn": "arn:aws:iot:your-region:your-aws-account:thing/MyIotThing",
       "thingName": "MyIotThing",
       "thingId": "6cf922a8-d8ea-4136-f3401EXAMPLE"
   }
   ```

Um AWS IoT Schlüssel und Zertifikate in Ihrer Linux-Instance zu erstellen und anzuhängen

Der Befehl create-keys-and-certificate erstellt Clientzertifikate, die von der Amazon Root-Zertifizierungsstelle signiert wurden. Dieses Zertifikat wird verwendet, um die Identität Ihres virtuellen Geräts zu authentifizieren.

1. Erstellen Sie in Ihrem Amazon EC2 Instance Connect-Fenster ein Verzeichnis zum Speichern Ihres Zertifikats und Ihrer Schlüsseldateien.

   ```
   mkdir ~/certs
   ```

2. Laden Sie in Ihrem Amazon EC2 Instance Connect-Fenster mit diesem Befehl eine Kopie des Zertifikats der Amazon Certificate Authority (CA) herunter.

   ```
   curl -o ~/certs/Amazon-root-CA-1.pem \
   ```

```
    https://www.amazontrust.com/repository/AmazonRootCA1.pem
```

3. Führen Sie in Ihrem Amazon EC2 Instance Connect-Fenster den folgenden Befehl aus, um Ihre privaten Schlüssel-, öffentlichen Schlüssel- und X.509-Zertifikatsdateien zu erstellen. Dieser Befehl registriert und aktiviert auch das Zertifikat mit AWS IoT.

```
aws iot create-keys-and-certificate \
    --set-as-active \
    --certificate-pem-outfile "~/certs/device.pem.crt" \
    --public-key-outfile "~/certs/public.pem.key" \
    --private-key-outfile "~/certs/private.pem.key"
```

Die Antwort sieht wie folgt aus. Speichern Sie das `certificateArn`, damit Sie es in nachfolgenden Befehlen verwenden können. Sie benötigen es, um Ihr Zertifikat an Ihr Objekt anzuhängen und die Richtlinie in späteren Schritten an das Zertifikat anzuhängen.

```
{
    "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/9894ba17925e663f1d29c23af4582b8e3b7619c31f3fbd93adcb51ae54b83dc2",
    "certificateId":
 "9894ba17925e663f1d29c23af4582b8e3b7619c31f3fbd93adcb51ae54b83dc2",
    "certificatePem": "
-----BEGIN CERTIFICATE-----
MIICiTCCEXAMPLE6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgEXAMPLEAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSEXAMPLE2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYEXAMPLEb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCEXAMPLEJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDAEXAMPLEsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEXAMPLE25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+aEXAMPLE
EXAMPLEfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZEXAMPLELG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAEXAMPLEWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9qEXAMPLEyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDEXAMPLEBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----\n",
    "keyPair": {
        "PublicKey": "-----BEGIN PUBLIC
 KEY-----\nMIIBIjANBgkqhkEXAMPLEQEFAAOCAQ8AMIIBCgKCAQEAEXAMPLE1nnyJwKSMHw4h
\nMMEXAMPLEuuN/dMAS3fyce8DW/4+EXAMPLEyjmoF/YVF/
```

```
gHr99VEEXAMPLE5VF13\n59VK7cEXAMPLE67GK+y+jikqXOgHh/xJTwo
+sGpWEXAMPLEDz18xOd2ka4tCzuWEXAMPLEahJbYkCPUBSU8opVkR7qkEXAMPLE1DR6sx2HocliOOLtu6Fkw91swQWE
\GB3ZPrNh0PzQYvjUStZeccyNCx2EXAMPLEvp9mQOUXP6plfgxwKRX2fEXAMPLEDa
\nhJLXkX3rHU2xbxJSq7D+XEXAMPLEcw+LyFhI5mgFRl88eGdsAEXAMPLElnI9EesG\nFQIDAQAB\n-----
END PUBLIC KEY-----\n",
        "PrivateKey": "-----BEGIN RSA PRIVATE KEY-----\nkey omitted for security
 reasons\n-----END RSA PRIVATE KEY-----\n"
    }
}
```

4. Hängen Sie in Ihrem Amazon EC2 Instance Connect-Fenster Ihr Ding-Objekt mit dem Zertifikat an, das Sie gerade erstellt haben, indem Sie den *certificateArn* folgenden Befehl und die Antwort des vorherigen Befehls verwenden.

   ```
   aws iot attach-thing-principal \
       --thing-name "MyIotThing" \
       --principal "certificateArn"
   ```

   Dieser Befehl gibt keine Ausgabe zurück, wenn er erfolgreich ist.

Erstellen und Anfügen einer Richtlinie

1. Erstellen Sie in Ihrem Amazon EC2 Instance Connect-Fenster die Richtliniendatei, indem Sie dieses Richtliniendokument kopieren und in eine Datei mit dem Namen **~/policy.json** einfügen.

   Wenn Sie keinen bevorzugten Linux-Editor haben, können Sie nano mit diesem Befehl öffnen.

   ```
   nano ~/policy.json
   ```

   Fügen Sie das Richtliniendokument für `policy.json` ein. Speichern Sie die Datei und beenden Sie den nano-Editor (Strg+X).

   Kopieren Sie den Inhalt des Richtliniendokuments für `policy.json`.

   ```
   {
       "Version": "2012-10-17",
       "Statement": [
           {
               "Effect": "Allow",
   ```

```
            "Action": [
                "iot:Publish",
                "iot:Subscribe",
                "iot:Receive",
                "iot:Connect"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

2. Erstellen Sie in Ihrem Amazon EC2 Instance Connect-Fenster Ihre Richtlinie mit dem folgenden Befehl.

```
aws iot create-policy \
    --policy-name "MyIotThingPolicy" \
    --policy-document "file://~/policy.json"
```

Ausgabe:

```
{
    "policyName": "MyIotThingPolicy",
    "policyArn": "arn:aws:iot:your-region:your-aws-account:policy/
MyIotThingPolicy",
    "policyDocument": "{
        \"Version\": \"2012-10-17\",
        \"Statement\": [
            {
                \"Effect\": \"Allow\",
                \"Action\": [
                    \"iot:Publish\",
                    \"iot:Receive\",
                    \"iot:Subscribe\",
                    \"iot:Connect\"
                ],
                \"Resource\": [
                    \"*\"
                ]
            }
        ]
    }",
```

```
    "policyVersionId": "1"
}
```

3. Fügen Sie in Ihrem Amazon EC2 Instance Connect-Fenster die Richtlinie mithilfe des folgenden Befehls dem Zertifikat Ihres virtuellen Geräts hinzu.

```
aws iot attach-policy \
    --policy-name "MyIotThingPolicy" \
    --target "certificateArn"
```

Dieser Befehl gibt keine Ausgabe zurück, wenn er erfolgreich ist.

### Installieren Sie das AWS IoT Geräte-SDK für JavaScript

In diesem Abschnitt installieren Sie das AWS IoT Geräte-SDK für JavaScript. Es enthält den Code, mit dem Anwendungen kommunizieren können, AWS IoT sowie die Beispielprogramme. Weitere Informationen finden Sie im AWS IoT Geräte-SDK für das JavaScript GitHub Repository.

Um das AWS IoT Geräte-SDK für JavaScript auf Ihrer Linux-Instance zu installieren

1. Klonen Sie in Ihrem Amazon EC2 Instance Connect-Fenster mit diesem Befehl das AWS IoT `aws-iot-device-sdk-js-v2` Geräte-SDK für das JavaScript Repository in das Verzeichnis Ihres Home-Verzeichnisses.

```
cd ~
git clone https://github.com/aws/aws-iot-device-sdk-js-v2.git
```

2. Navigieren Sie zum `aws-iot-device-sdk-js-v2`-Verzeichnis, das Sie im vorherigen Schritt erstellt haben.

```
cd aws-iot-device-sdk-js-v2
```

3. Verwenden Sie zum Installieren der SDK npm.

```
npm install
```

Ausführen der Beispielanwendungen

Bei den Befehlen im nächsten Abschnitt wird davon ausgegangen, dass Ihr Schlüssel und Ihr Zertifikatdateien wie in dieser Tabelle gezeigt auf Ihrem virtuellen Gerät gespeichert sind.

Namen der Zertifikatsdateien

| Datei | Dateipfad |
|---|---|
| Privater Schlüssel | `~/certs/private.pem.key` |
| Gerätezertifikat | `~/certs/device.pem.crt` |
| CA-Stammzertifikat | `~/certs/Amazon-root-CA-1.pem` |

In diesem Abschnitt installieren und führen Sie die `pub-sub.js` Beispiel-App aus, die Sie im `aws-iot-device-sdk-js-v2/samples/node` Verzeichnis des AWS IoT Geräte-SDK für finden JavaScript. Diese App zeigt, wie ein Gerät, Ihre EC2 Amazon-Instance, die MQTT-Bibliothek verwendet, um MQTT-Nachrichten zu veröffentlichen und zu abonnieren. Die `pub-sub.js`-Beispiel-App abonniert ein Thema, `topic_1`, veröffentlicht 10 Nachrichten zu diesem Thema und zeigt die Nachrichten so an, wie sie vom Message Broker empfangen wurden.

Um die Beispiel-App zu installieren und auszuführen

1. Navigieren Sie in Ihrem Amazon EC2 Instance Connect-Fenster zu dem `aws-iot-device-sdk-js-v2/samples/node/pub_sub` Verzeichnis, das das SDK erstellt hat, und installieren Sie die Beispiel-App mithilfe dieser Befehle.

   ```
   cd ~/aws-iot-device-sdk-js-v2/samples/node/pub_sub
   npm install
   ```

2. Rufen Sie in Ihrem Amazon EC2 Instance Connect-Fenster mit diesem Befehl AWS IoT von *`your-iot-endpoint`* ab.

   ```
   aws iot describe-endpoint --endpoint-type iot:Data-ATS
   ```

3. Fügen Sie in Ihrem Amazon EC2 Instance Connect-Fenster *`your-iot-endpoint`* wie angegeben den Befehl ein und führen Sie ihn aus.

```
node dist/index.js --topic topic_1 --ca_file ~/certs/Amazon-root-CA-1.pem --cert ~/
certs/device.pem.crt --key ~/certs/private.pem.key --endpoint your-iot-endpoint
```

Die Beispiel-App:

1. Stellt eine Verbindung AWS IoT Core zu Ihrem Konto her.
2. Das Nachrichtenthema topic_1 abonniert und die Nachrichten anzeigt, die es zu diesem Thema erhält.
3. 10 Nachrichten zum Thema topic_1 veröffentlicht.
4. Ihre Ausgabe sieht ähnlich aus wie:

```
Publish received. topic:"topic_1" dup:false qos:1 retain:false
{"message":"Hello world!","sequence":1}
Publish received. topic:"topic_1" dup:false qos:1 retain:false
{"message":"Hello world!","sequence":2}
Publish received. topic:"topic_1" dup:false qos:1 retain:false
{"message":"Hello world!","sequence":3}
Publish received. topic:"topic_1" dup:false qos:1 retain:false
{"message":"Hello world!","sequence":4}
Publish received. topic:"topic_1" dup:false qos:1 retain:false
{"message":"Hello world!","sequence":5}
Publish received. topic:"topic_1" dup:false qos:1 retain:false
{"message":"Hello world!","sequence":6}
Publish received. topic:"topic_1" dup:false qos:1 retain:false
{"message":"Hello world!","sequence":7}
Publish received. topic:"topic_1" dup:false qos:1 retain:false
{"message":"Hello world!","sequence":8}
Publish received. topic:"topic_1" dup:false qos:1 retain:false
{"message":"Hello world!","sequence":9}
Publish received. topic:"topic_1" dup:false qos:1 retain:false
{"message":"Hello world!","sequence":10}
```

Wenn Probleme bei der Ausführung der Beispiel-App auftreten, überprüfen Sie the section called “Beheben Sie Probleme mit der Beispielanwendung”.

Sie können den Parameter `--verbosity debug` auch zur Befehlszeile hinzufügen, sodass die Beispiel-App detaillierte Meldungen darüber anzeigt, was sie tut. Diese Informationen bieten Ihnen möglicherweise die Hilfe, die Sie zur Behebung des Problems benötigen.

Nachrichten aus der Beispiel-App in der AWS IoT -Konsole anzeigen

Mithilfe des MQTT-Testclients in der AWS IoT -Konsole können Sie die Nachrichten der Beispiel-App sehen, während sie den Message Broker durchlaufen.

Um die von der Beispiel-App veröffentlichten MQTT-Nachrichten anzuzeigen

1. Sehen Sie sich MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen an. Auf diese Weise lernen Sie, wie Sie den MQTT-Testclient in der AWS IoT -Konsole verwenden, um MQTT-Nachrichten anzuzeigen, während sie den Message Broker passieren.
2. Öffnen Sie den MQTT-Testclient in der AWS IoT -Konsole.
3. Unter Thema abonnieren, Thema abonnieren, topic_1.
4. Führen Sie in Ihrem Amazon EC2 Instance Connect-Fenster die Beispiel-App erneut aus und sehen Sie sich die Nachrichten im MQTT-Testclient in der AWS IoT Konsole an.

```
cd ~/aws-iot-device-sdk-js-v2/samples/node/pub_sub
node dist/index.js --topic topic_1 --ca_file ~/certs/Amazon-root-CA-1.pem --cert ~/
certs/device.pem.crt --key ~/certs/private.pem.key --endpoint your-iot-endpoint
```

Weitere Informationen zu MQTT und zur AWS IoT Core Unterstützung des Protokolls finden Sie unter MQTT.

## Verwenden Sie Ihren Windows- oder Linux-PC oder Mac als Gerät AWS IoT

In diesem Tutorial konfigurieren Sie einen PC für die Verwendung mit AWS IoT. Diese Anweisungen unterstützen Windows, Linux PCs und Macs. Um dies zu erreichen, müssen Sie einige Software auf Ihrem Computer installieren. Wenn Sie keine Software auf Ihrem Computer installieren möchten, können Sie mit Erstellen Sie ein virtuelles Gerät mit Amazon EC2 versuchen, die gesamte Software auf einer virtuellen Maschine zu installieren.

In diesem Tutorial führen Sie die folgenden Aktivitäten durch:

- Einrichten Ihres PCs
- Installieren Sie Git, Python und das AWS IoT Geräte-SDK für Python
- Konfigurieren Sie die Richtlinie und führen Sie die Beispielanwendung aus
- Nachrichten aus der Beispiel-App in der AWS IoT -Konsole anzeigen
- Führen Sie das Beispiel „Shared Subscription“ in Python aus

Einrichten Ihres PCs

Um dieses Tutorial abzuschließen, benötigen Sie einen Windows- oder Linux-PC oder einen Mac mit Internetverbindung.

Bevor Sie mit dem nächsten Schritt fortfahren, stellen Sie sicher, dass Sie ein Befehlszeilenfenster auf Ihrem Computer öffnen können. cmd.exe auf einem Windows-PC verwenden. Verwenden Sie auf einem Linux-PC oder Mac Terminal.

Installieren Sie Git, Python und das AWS IoT Geräte-SDK für Python

In diesem Abschnitt installieren Sie Python und das AWS IoT Device SDK für Python auf Ihrem Computer.

Installieren Sie die neueste Version von Git und Python

Dieses Verfahren erklärt, wie Sie die neueste Version von Git und Python auf Ihrem PC installieren.

Um Git und Python herunterzuladen und auf Ihrem Computer zu installieren

1. Überprüfen Sie, ob Git auf Ihrem Computer installiert ist. Geben Sie an der Befehlszeile den folgenden Befehl ein.

   ```
   git --version
   ```

   Wird mit dem Befehl die Git-Version angezeigt, ist Git installiert und Sie können mit dem nächsten Schritt fortfahren.

   Wenn der Befehl einen Fehler anzeigt, öffnen Sie https://git-scm.com/download und installieren Sie Git für Ihren Computer.
2. Überprüfen Sie, ob Python bereits installiert ist. Geben Sie in der Kommandozeile den Befehl ein.

   ```
   python -V
   ```

   > **Note**
   >
   > Wenn dieser Befehl einen Fehler: `Python was not found` ausgibt, liegt das möglicherweise daran, dass Ihr Betriebssystem die ausführbare Python v3.x-Datei als

`Python3` aufruft. Ersetzen Sie in diesem Fall alle Instanzen von `python` durch `python3` und fahren Sie mit dem Rest dieses Tutorials fort.

Wenn der Befehl die Python-Version anzeigt, ist Python bereits installiert. Dieses Skript erfordert Python 3.7 oder höher.

3. Wenn Python installiert ist, können Sie die restlichen Schritte in diesem Abschnitt überspringen. Wenn nicht, fahren Sie fort.
4. Öffnen Sie https://www.python.org/downloads/ und laden Sie das Installationsprogramm für Ihren Computer herunter.
5. Wenn der Download nicht automatisch mit der Installation gestartet wurde, führen Sie das heruntergeladene Programm aus, um Python zu installieren.
6. Überprüfen Sie die Installation von Python.

```
python -V
```

Vergewissern Sie sich, dass der Befehl die Python-Version anzeigt. Wenn die Python-Version nicht angezeigt wird, versuchen Sie erneut, Python herunterzuladen und zu installieren.

### Installieren Sie das AWS IoT Geräte-SDK für Python

So installieren Sie das AWS IoT Device SDK für Python auf Ihrem Computer

1. Installieren Sie Version 2 des AWS IoT Geräte-SDK für Python.

```
python3 -m pip install awsiotsdk
```

2. Klonen Sie das AWS IoT Device SDK for Python-Repository in das Verzeichnis aws-iot-device-sdk -python-v2 Ihres Home-Verzeichnisses. Dieses Verfahren bezieht sich auf das Basisverzeichnis für die Dateien, unter denen Sie die Installation durchführen. *home*

   Der tatsächliche Speicherort des *home* Verzeichnisses hängt von Ihrem Betriebssystem ab.

   Linux/macOS

   In macOS und Linux ist das *home* Verzeichnis~.

```
cd ~
```

```
git clone https://github.com/aws/aws-iot-device-sdk-python-v2.git
```

Windows

In Windows können Sie den *home* Verzeichnispfad finden, indem Sie diesen Befehl im `cmd` Fenster ausführen.

```
echo %USERPROFILE%
cd %USERPROFILE%
git clone https://github.com/aws/aws-iot-device-sdk-python-v2.git
```

> **Note**
>
> Wenn Sie Windows PowerShell anstelle von verwendencmd.exe, verwenden Sie den folgenden Befehl.
>
> ```
> echo $home
> ```

Weitere Informationen finden Sie im GitHub Repository AWS IoT Device SDK for Python.

Vorbereiten der Ausführung von Beispielanwendungen

Vorbereiten der Ausführung von Beispielanwendungen

- Erstellen des `certs` Verzeichnisses. Kopieren Sie die Dateien für den privaten Schlüssel, das Gerätezertifikat und das Stammzertifikat der Zertifizierungsstelle, die Sie bei der Erstellung und Registrierung des Objekts gespeichert haben, in the section called “AWS IoT Ressourcen erstellen” des `certs` Verzeichnisses. Die Dateinamen der einzelnen Dateien im Zielverzeichnis sollten mit denen in der Tabelle übereinstimmen.

  Bei den Befehlen im nächsten Abschnitt wird davon ausgegangen, dass Ihr Schlüssel und Ihre Zertifikatdateien wie in dieser Tabelle gezeigt auf dem Gerät gespeichert sind.

  Linux/macOS

  Führen Sie diesen Befehl aus, um das Unterverzeichnis `certs` zu erstellen, das Sie beim Ausführen der Beispielanwendungen verwenden werden.

```
mkdir ~/certs
```

Kopieren Sie die Dateien in das neue Unterverzeichnis in die Zieldateipfade, die in der folgenden Tabelle aufgeführt sind.

Namen der Zertifikatsdateien

| Datei | Dateipfad |
| --- | --- |
| Privater Schlüssel | `~/certs/private.pem.key` |
| Gerätezertifikat | `~/certs/device.pem.crt` |
| CA-Stammzertifikat | `~/certs/Amazon-root-CA-1.pem` |

Führen Sie diesen Befehl aus, um die Dateien im Verzeichnis `certs` aufzulisten und sie mit den in der Tabelle aufgeführten Dateien zu vergleichen.

```
ls -l ~/certs
```

Windows

Führen Sie diesen Befehl aus, um das Unterverzeichnis `certs` zu erstellen, das Sie beim Ausführen der Beispielanwendungen verwenden werden.

```
mkdir %USERPROFILE%\certs
```

Kopieren Sie die Dateien in das neue Unterverzeichnis in die Zieldateipfade, die in der folgenden Tabelle aufgeführt sind.

Namen der Zertifikatsdateien

| Datei | Dateipfad |
| --- | --- |
| Privater Schlüssel | `%USERPROFILE%\certs\private.pem.key` |

| Datei | Dateipfad |
| --- | --- |
| Gerätezertifikat | `%USERPROFILE%\certs\device.pem.crt` |
| CA-Stammzertifikat | `%USERPROFILE%\certs\Amazon-root-CA-1.pem` |

Führen Sie diesen Befehl aus, um die Dateien im Verzeichnis `certs` aufzulisten und sie mit den in der Tabelle aufgeführten Dateien zu vergleichen.

```
dir %USERPROFILE%\certs
```

Konfigurieren Sie die Richtlinie und führen Sie die Beispielanwendung aus

In diesem Abschnitt richten Sie Ihre Richtlinie ein und führen das `pubsub.py` Beispielskript aus, das sich im `aws-iot-device-sdk-python-v2/samples` Verzeichnis von befindet AWS IoT-Geräte-SDK for Python. Dieses Skript zeigt, wie Ihr Gerät die MQTT-Bibliothek verwendet, um MQTT-Nachrichten zu veröffentlichen und zu abonnieren.

Die `pubsub.py` Beispiel-App abonniert ein Thema, `test/topic`, veröffentlicht 10 Nachrichten zu diesem Thema und zeigt die Nachrichten so an, wie sie vom Message Broker empfangen wurden.

Zur Ausführung der Beispielanwendung `pubsub.py` benötigen Sie die folgenden Informationen:

Anwendungsparameterwerte

| Parameter | Wo der Wert gefunden werden kann |
| --- | --- |
| *your-iot-endpoint* | 1. Wählen Sie in der AWS IoT -Konsole im linken Menü Einstellungen.<br>2. Auf der Seite Einstellungen wird Ihr Endpunkt im Abschnitt Gerätedatenendpunkt angezeigt. |

Der *your-iot-endpoint* Wert hat das Format:*endpoint_id*-ats.iot.*region*.amazonaws.com, zum Beispiela3qj468EXAMPLE-ats.iot.us-west-2.amazonaws.com.

Bevor Sie das Skript ausführen, stellen Sie sicher, dass die Richtlinie für Ihr Objekt die Berechtigungen für das Beispielskript zum Herstellen einer Verbindung, zum Abonnieren, Veröffentlichen und Empfangen vorsieht.

Um das Richtliniendokument für eine Objektressource zu finden und zu überprüfen

1. Suchen Sie in der AWS IoT -Konsole in der Liste Objekte nach der Objektressource, die Ihrem Gerät entspricht.
2. Wählen Sie den Link Name der Objektressource, die für Ihr Gerät steht, um die Seite mit den Objektdetails zu öffnen.
3. Wählen Sie auf der Seite mit den Objektdetails auf der Registerkarte Zertifikate das Zertifikat aus, das an die Objektressource angehängt ist. Die Liste sollte nur ein Zertifikat enthalten. Wenn es mehrere gibt, wählen Sie das Zertifikat aus, dessen Dateien auf Ihrem Gerät installiert sind und mit dem eine Verbindung zu AWS IoT Core hergestellt werden soll.

   Wählen Sie auf der Seite mit den Zertifikatsdetails auf der Registerkarte Richtlinien die Richtlinie aus, die mit dem Zertifikat verknüpft ist. Es sollte nur eine geben. Wenn es mehrere gibt, wiederholen Sie den nächsten Schritt für alle, um sicherzustellen, dass mindestens eine Richtlinie den erforderlichen Zugriff gewährt.
4. Suchen Sie auf der Seite mit der Richtlinienübersicht den JSON-Editor und wählen Sie Richtliniendokument bearbeiten aus, um das Richtliniendokument nach Bedarf zu überprüfen und zu bearbeiten.
5. Das Richtlinien-JSON wird im folgenden Beispiel angezeigt. Ersetzen Sie das `"Resource"` Element *region:account* durch Ihr AWS-Region und AWS-Konto in jedem der `Resource` Werte.

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

```
            "Resource": [
                "arn:aws:iot:region:account:topic/test/topic"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:region:account:topicfilter/test/topic"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:region:account:client/test-*"
            ]
        }
    ]
}
```

Linux/macOS

Um das Beispielskript unter Linux/macOS auszuführen

1. Navigieren Sie in Ihrem Befehlszeilenfenster zu dem `~/aws-iot-device-sdk-python-v2/samples/node/pub_sub`-Verzeichnis, das das SDK mithilfe dieser Befehle erstellt hat.

   ```
   cd ~/aws-iot-device-sdk-python-v2/samples
   ```

2. Ersetzen Sie in Ihrem Befehlszeilenfenster *`your-iot-endpoint`* wie angegeben und führen Sie diesen Befehl aus.

   ```
   python3 pubsub.py --endpoint your-iot-endpoint --ca_file ~/certs/Amazon-root-CA-1.pem --cert ~/certs/device.pem.crt --key ~/certs/private.pem.key
   ```

Windows

Um die Beispiel-App auf einem Windows-PC auszuführen

1. Navigieren Sie in Ihrem Befehlszeilenfenster zu dem `%USERPROFILE%\aws-iot-device-sdk-python-v2\samples`-Verzeichnis, das das SDK erstellt hat, und installieren Sie die Beispiel-App mithilfe dieser Befehle.

   ```
   cd %USERPROFILE%\aws-iot-device-sdk-python-v2\samples
   ```

2. Ersetzen Sie in Ihrem Befehlszeilenfenster *`your-iot-endpoint`* wie angegeben und führen Sie diesen Befehl aus.

   ```
   python3 pubsub.py --endpoint your-iot-endpoint --ca_file %USERPROFILE%
   \certs\Amazon-root-CA-1.pem --cert %USERPROFILE%\certs\device.pem.crt --key
    %USERPROFILE%\certs\private.pem.key
   ```

Das Beispielskript:

1. Stellt eine Verbindung mit dem AWS IoT Core für Ihr Konto her.
2. Abonniert das Nachrichtenthema test/topic und zeigt die Nachrichten an, die es zu diesem Thema erhält.
3. Veröffentlicht 10 Nachrichten zum Thema test/topic.
4. Die Ausgabe sieht ähnlich aus wie:

```
Connected!
Subscribing to topic 'test/topic'...
Subscribed with QoS.AT_LEAST_ONCE
Sending 10 message(s)
Publishing message to topic 'test/topic': Hello World! [1]
Received message from topic 'test/topic': b'"Hello World! [1]"'
Publishing message to topic 'test/topic': Hello World! [2]
Received message from topic 'test/topic': b'"Hello World! [2]"'
Publishing message to topic 'test/topic': Hello World! [3]
Received message from topic 'test/topic': b'"Hello World! [3]"'
Publishing message to topic 'test/topic': Hello World! [4]
Received message from topic 'test/topic': b'"Hello World! [4]"'
Publishing message to topic 'test/topic': Hello World! [5]
Received message from topic 'test/topic': b'"Hello World! [5]"'
```

```
Publishing message to topic 'test/topic': Hello World! [6]
Received message from topic 'test/topic': b'"Hello World! [6]"'
Publishing message to topic 'test/topic': Hello World! [7]
Received message from topic 'test/topic': b'"Hello World! [7]"'
Publishing message to topic 'test/topic': Hello World! [8]
Received message from topic 'test/topic': b'"Hello World! [8]"'
Publishing message to topic 'test/topic': Hello World! [9]
Received message from topic 'test/topic': b'"Hello World! [9]"'
Publishing message to topic 'test/topic': Hello World! [10]
Received message from topic 'test/topic': b'"Hello World! [10]"'
10 message(s) received.
Disconnecting...
Disconnected!
```

Wenn Probleme bei der Ausführung der Beispiel-App auftreten, überprüfen Sie the section called “Beheben Sie Probleme mit der Beispielanwendung”.

Sie können den Parameter `--verbosity Debug` auch zur Befehlszeile hinzufügen, sodass die Beispiel-App detaillierte Meldungen darüber anzeigt, was sie tut. Diese Informationen können Ihnen bei der Behebung des Problems helfen.

Nachrichten aus der Beispiel-App in der AWS IoT -Konsole anzeigen

Mithilfe des MQTT-Testclients in der AWS IoT -Konsole können Sie die Nachrichten der Beispiel-App sehen, während sie den Message Broker durchlaufen.

Um die von der Beispiel-App veröffentlichten MQTT-Nachrichten anzuzeigen

1. Sehen Sie sich MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen an. Auf diese Weise lernen Sie, wie Sie den MQTT-Testclient in der AWS IoT -Konsole verwenden, um MQTT-Nachrichten anzuzeigen, während sie den Message Broker passieren.
2. Öffnen Sie den MQTT-Testclient in der AWS IoT -Konsole.
3. Abonnieren Sie unter Thema abonnieren das Thema Test/Thema.
4. Führen Sie in Ihrem Befehlszeilenfenster die Beispiel-App erneut aus und sehen Sie sich die Nachrichten im MQTT-Client in der AWS IoT -Konsole an.

   Linux/macOS

   ```
   cd ~/aws-iot-device-sdk-python-v2/samples
   ```

```
python3 pubsub.py --topic test/topic --ca_file ~/certs/Amazon-root-CA-1.pem --
cert ~/certs/device.pem.crt --key ~/certs/private.pem.key --endpoint your-iot-
endpoint
```

Windows

```
cd %USERPROFILE%\aws-iot-device-sdk-python-v2\samples
python3 pubsub.py --topic test/topic --ca_file %USERPROFILE%\certs\Amazon-root-
CA-1.pem --cert %USERPROFILE%\certs\device.pem.crt --key %USERPROFILE%\certs
\private.pem.key --endpoint your-iot-endpoint
```

Weitere Informationen zu MQTT und zur AWS IoT Core Unterstützung des Protokolls finden Sie unter MQTT.

Führen Sie das Beispiel „Shared Subscription“ in Python aus

AWS IoT Core unterstützt Shared Subscriptions sowohl für MQTT 3 als auch für MQTT 5. Gemeinsame Abonnements ermöglichen es mehreren Clients, ein Abonnement für ein Thema gemeinsam zu nutzen, und nur ein Client erhält Nachrichten, die zu diesem Thema veröffentlicht wurden, nach dem Zufallsprinzip. Um gemeinsame Abonnements zu verwenden, abonnieren Clients den Themenfilter eines gemeinsamen Abonnements: `$share/{ShareName}/{TopicFilter}`.

So konfigurieren Sie die Richtlinie und führen das Beispiel für ein geteiltes Abonnement aus

1. Um das Beispiel Gemeinsame Abonnements auszuführen, müssen Sie die Richtlinie Ihres Objekts so einrichten, wie es in MQTT 5 Gemeinsame Abonnements dokumentiert ist.
2. Führen Sie die folgenden Befehle aus, um das Gemeinsame Abonnements-Beispiel auszuführen.

   Linux/macOS

   Um das Beispielskript unter Linux/macOS auszuführen

   1. Navigieren Sie in Ihrem Befehlszeilenfenster zu dem `~/aws-iot-device-sdk-python-v2/samples`-Verzeichnis, das das SDK mithilfe dieser Befehle erstellt hat.

      ```
      cd ~/aws-iot-device-sdk-python-v2/samples
      ```

   2. Ersetzen Sie in Ihrem Befehlszeilenfenster *your-iot-endpoint* wie angegeben und führen Sie diesen Befehl aus.

```
python3 mqtt5_shared_subscription.py --endpoint your-iot-endpoint --ca_file
 ~/certs/Amazon-root-CA-1.pem --cert ~/certs/device.pem.crt --key ~/certs/
private.pem.key --group_identifier consumer
```

Windows

Um die Beispiel-App auf einem Windows-PC auszuführen

1. Navigieren Sie in Ihrem Befehlszeilenfenster zu dem `%USERPROFILE%\aws-iot-device-sdk-python-v2\samples`-Verzeichnis, das das SDK erstellt hat, und installieren Sie die Beispiel-App mithilfe dieser Befehle.

   ```
   cd %USERPROFILE%\aws-iot-device-sdk-python-v2\samples
   ```

2. Ersetzen Sie in Ihrem Befehlszeilenfenster *`your-iot-endpoint`* wie angegeben und führen Sie diesen Befehl aus.

   ```
   python3 mqtt5_shared_subscription.py --endpoint your-iot-endpoint --ca_file
    %USERPROFILE%\certs\Amazon-root-CA-1.pem --cert %USERPROFILE%\certs
   \device.pem.crt --key %USERPROFILE%\certs\private.pem.key --group_identifier
    consumer
   ```

> **Note**
>
> Sie können optional eine Gruppen-ID angeben, die Ihren Anforderungen entspricht, wenn Sie das Beispiel ausführen (z. B. `--group_identifier consumer`). Wenn Sie kein angeben, ist `python-sample` der Standardgruppen-Identifier.

3. Die Ausgabe in Ihrer Befehlszeile kann wie folgt aussehen:

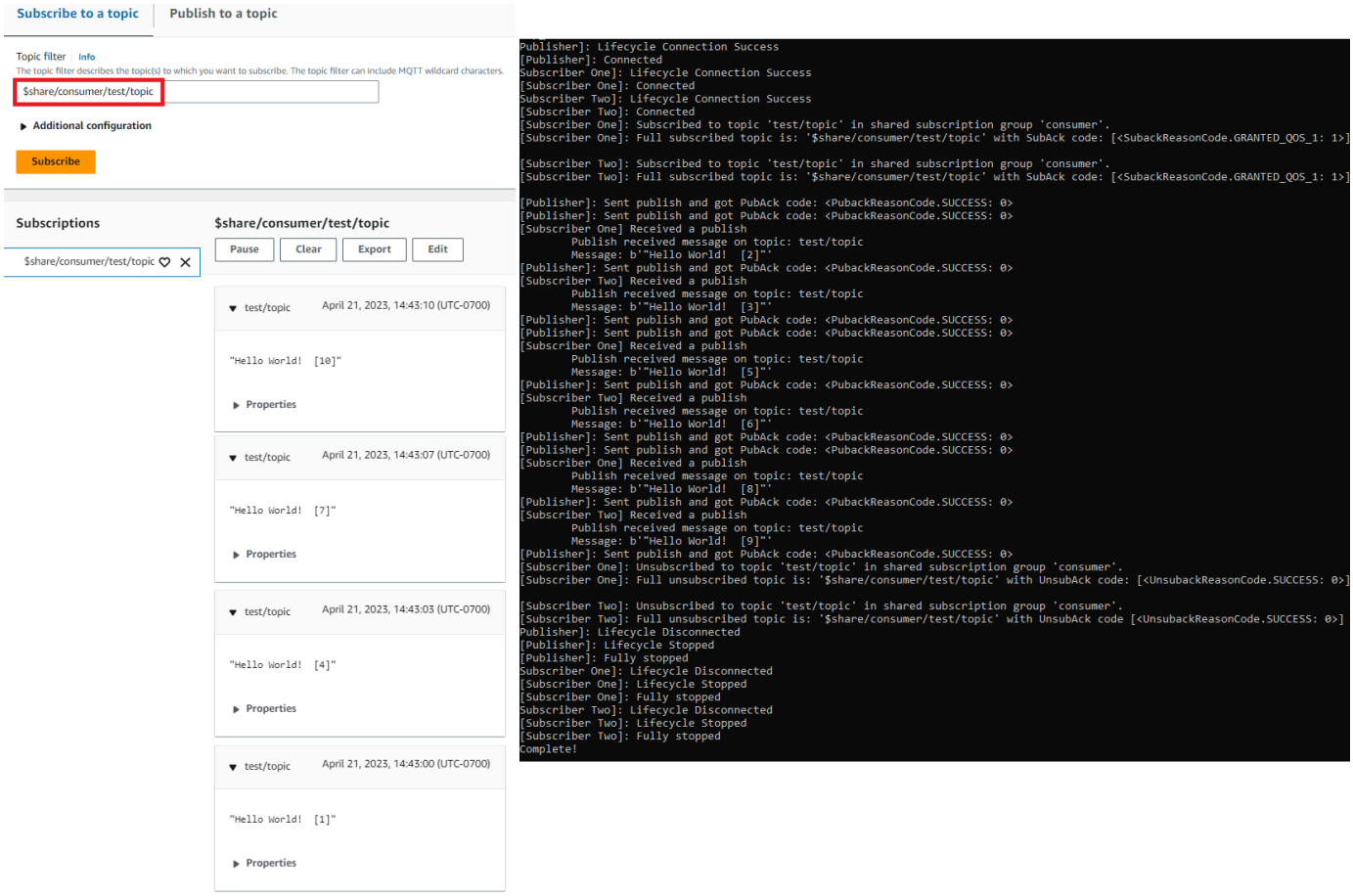
```
Publisher]: Lifecycle Connection Success
[Publisher]: Connected
Subscriber One]: Lifecycle Connection Success
[Subscriber One]: Connected
Subscriber Two]: Lifecycle Connection Success
[Subscriber Two]: Connected
[Subscriber One]: Subscribed to topic 'test/topic' in shared subscription group
 'consumer'.
```

```
[Subscriber One]: Full subscribed topic is: '$share/consumer/test/topic' with
 SubAck code: [<SubackReasonCode.GRANTED_QOS_1: 1>]
[Subscriber Two]: Subscribed to topic 'test/topic' in shared subscription group
 'consumer'.
[Subscriber Two]: Full subscribed topic is: '$share/consumer/test/topic' with
 SubAck code: [<SubackReasonCode.GRANTED_QOS_1: 1>]
[Publisher]: Sent publish and got PubAck code: <PubackReasonCode.SUCCESS: 0>
[Subscriber Two] Received a publish
        Publish received message on topic: test/topic
        Message: b'"Hello World!  [1]"'
[Publisher]: Sent publish and got PubAck code: <PubackReasonCode.SUCCESS: 0>
[Subscriber One] Received a publish
        Publish received message on topic: test/topic
        Message: b'"Hello World!  [2]"'
[Publisher]: Sent publish and got PubAck code: <PubackReasonCode.SUCCESS: 0>
[Subscriber Two] Received a publish
        Publish received message on topic: test/topic
        Message: b'"Hello World!  [3]"'
[Publisher]: Sent publish and got PubAck code: <PubackReasonCode.SUCCESS: 0>
[Subscriber One] Received a publish
        Publish received message on topic: test/topic
        Message: b'"Hello World!  [4]"'
[Publisher]: Sent publish and got PubAck code: <PubackReasonCode.SUCCESS: 0>
[Subscriber Two] Received a publish
        Publish received message on topic: test/topic
        Message: b'"Hello World!  [5]"'
[Publisher]: Sent publish and got PubAck code: <PubackReasonCode.SUCCESS: 0>
[Subscriber One] Received a publish
        Publish received message on topic: test/topic
        Message: b'"Hello World!  [6]"'
[Publisher]: Sent publish and got PubAck code: <PubackReasonCode.SUCCESS: 0>
[Subscriber Two] Received a publish
        Publish received message on topic: test/topic
        Message: b'"Hello World!  [7]"'
[Publisher]: Sent publish and got PubAck code: <PubackReasonCode.SUCCESS: 0>
[Subscriber One] Received a publish
        Publish received message on topic: test/topic
        Message: b'"Hello World!  [8]"'
[Publisher]: Sent publish and got PubAck code: <PubackReasonCode.SUCCESS: 0>
[Subscriber Two] Received a publish
        Publish received message on topic: test/topic
        Message: b'"Hello World!  [9]"'
[Publisher]: Sent publish and got PubAck code: <PubackReasonCode.SUCCESS: 0>
[Subscriber One] Received a publish
```

```
        Publish received message on topic: test/topic
        Message: b'"Hello World!  [10]"'
[Subscriber One]: Unsubscribed to topic 'test/topic' in shared subscription group
 'consumer'.
[Subscriber One]: Full unsubscribed topic is: '$share/consumer/test/topic' with
 UnsubAck code: [<UnsubackReasonCode.SUCCESS: 0>]
[Subscriber Two]: Unsubscribed to topic 'test/topic' in shared subscription group
 'consumer'.
[Subscriber Two]: Full unsubscribed topic is: '$share/consumer/test/topic' with
 UnsubAck code [<UnsubackReasonCode.SUCCESS: 0>]
Publisher]: Lifecycle Disconnected
[Publisher]: Lifecycle Stopped
[Publisher]: Fully stopped
Subscriber One]: Lifecycle Disconnected
[Subscriber One]: Lifecycle Stopped
[Subscriber One]: Fully stopped
Subscriber Two]: Lifecycle Disconnected
[Subscriber Two]: Lifecycle Stopped
[Subscriber Two]: Fully stopped
Complete!
```

4. Öffnen Sie den MQTT-Testclient in der AWS IoT -Konsole. Abonnieren Sie unter Thema abonnieren das Thema des gemeinsamen Abonnements, z. B.: `$share/consumer/test/topic`. Sie können bei der Ausführung des Beispiels eine Gruppen-ID angeben, die Ihren Anforderungen entspricht (z. B. `--group_identifier consumer`). Wenn Sie keine Gruppen-ID angeben, ist der Standardwert `python-sample`. Weitere Informationen finden Sie im Python-Beispiel für MQTT 5 Shared Subscription und im AWS IoT Core Developer Guide unter Shared Subscriptions.

   Führen Sie in Ihrem Befehlszeilenfenster die Beispiel-App erneut aus und beobachten Sie die Verteilung der Nachrichten in Ihrem MQTT-Testclient der AWS IoT -Konsole und der Befehlszeile.




## Verbinden eines Raspberry Pi oder eines anderes Gerätes

In diesem Abschnitt konfigurieren wir einen Raspberry Pi für die Verwendung mit AWS IoT. Wenn Sie ein anderes Gerät haben, das Sie anschließen möchten, finden Sie in der Anleitung für den Raspberry Pi Hinweise, die Ihnen helfen können, diese Anweisungen an Ihr Gerät anzupassen.

Dies dauert normalerweise etwa 20 Minuten, kann aber länger dauern, wenn Sie viele Systemsoftware-Upgrades installieren müssen.

In diesem Tutorial führen Sie die folgenden Aktivitäten durch:

- Einrichten Ihres Geräts
- Installieren Sie die erforderlichen Tools und Bibliotheken für das AWS IoT Geräte-SDK
- Installieren Sie AWS IoT das Geräte-SDK
- Installieren und Ausführen der Beispiel-App
- Nachrichten aus der Beispiel-App in der AWS IoT Konsole anzeigen

> **Important**
>
> Die Anpassung dieser Anweisungen an andere Geräte und Betriebssysteme kann schwierig sein. Sie müssen Ihr Gerät gut genug verstehen, um diese Anweisungen interpretieren und auf Ihr Gerät anwenden zu können.
> Wenn Sie bei der Konfiguration Ihres Geräts für auf Schwierigkeiten stoßen AWS IoT, können Sie alternativ eine der anderen Geräteoptionen ausprobieren, z. B. Erstellen Sie ein virtuelles Gerät mit Amazon EC2 oderVerwenden Sie Ihren Windows- oder Linux-PC oder Mac als Gerät AWS IoT.

## Einrichten Ihres Geräts

Ziel dieses Schritts ist es, alles zu sammeln, was Sie benötigen, um Ihr Gerät so zu konfigurieren, dass es das Betriebssystem (OS) starten, eine Verbindung zum Internet herstellen und Ihnen die Interaktion mit dem Gerät über eine Befehlszeilenschnittstelle ermöglichen kann.

Zum Durcharbeiten dieses Tutorials ist Folgendes erforderlich:

- Ein AWS-Konto. Wenn dies nicht der Fall ist, führen Sie die unter Einrichten AWS-Konto beschriebenen Schritte aus, bevor Sie fortfahren.
- Ein Raspberry Pi 3 Modell B oder ein neueres Modell. Dies funktioniert möglicherweise auf früheren Versionen des Raspberry Pi, diese wurden jedoch nicht getestet.
- Raspberry Pi OS (32-Bit) oder höher. Wir empfehlen die neueste Version des Raspberry Pi OS zu verwenden. Frühere Versionen des Betriebssystems funktionieren möglicherweise, wurden jedoch nicht getestet.

  Um dieses Beispiel auszuführen, müssen Sie den Desktop nicht mit der grafischen Benutzeroberfläche (GUI) installieren. Wenn Sie jedoch mit dem Raspberry Pi noch nicht vertraut sind und Ihre Raspberry Pi-Hardware ihn unterstützt, ist es möglicherweise einfacher, den Desktop mit der GUI zu verwenden.
- Ein Ethernet oder eine WiFi Verbindung.
- Tastatur, Maus, Monitor, Kabel, Netzteile und andere Hardware, die für Ihr Gerät erforderlich ist.

> **Important**
>
> Bevor Sie mit dem nächsten Schritt fortfahren, muss das Betriebssystem Ihres Geräts installiert, konfiguriert und ausgeführt werden. Das Gerät muss mit dem Internet verbunden sein und Sie müssen über die Befehlszeilenschnittstelle auf das Gerät zugreifen können. Der Befehlszeilenzugriff kann über eine direkt verbundene Tastatur, Maus und einen Monitor oder über eine SSH-Terminal-Fernschnittstelle erfolgen.

Wenn Sie auf Ihrem Raspberry Pi ein Betriebssystem mit grafischer Benutzeroberfläche (GUI) ausführen, öffnen Sie ein Terminalfenster auf dem Gerät und führen Sie in diesem Fenster die folgenden Anweisungen aus. Andernfalls, wenn Sie über ein Remote-Terminal wie PuTTY eine Verbindung zu Ihrem Gerät herstellen, öffnen Sie ein Remote-Terminal für Ihr Gerät und verwenden Sie dieses.

Installieren Sie die erforderlichen Tools und Bibliotheken für das AWS IoT Geräte-SDK

Bevor Sie das AWS IoT Geräte-SDK und den Beispielcode installieren, stellen Sie sicher, dass Ihr System auf dem neuesten Stand ist und über die erforderlichen Tools und Bibliotheken für die Installation von verfügt SDKs.

1. Aktualisieren Sie das Betriebssystem und installieren Sie die erforderlichen Bibliotheken

   Bevor Sie ein AWS IoT Geräte-SDK installieren, führen Sie diese Befehle in einem Terminalfenster auf Ihrem Gerät aus, um das Betriebssystem zu aktualisieren und die erforderlichen Bibliotheken zu installieren.

   ```
   sudo apt-get update
   ```

   ```
   sudo apt-get upgrade
   ```

   ```
   sudo apt-get install cmake
   ```

   ```
   sudo apt-get install libssl-dev
   ```

2. Installieren Sie Git

Wenn auf dem Betriebssystem Ihres Geräts Git nicht installiert ist, müssen Sie es installieren, um das AWS IoT Geräte-SDK für zu installieren JavaScript.

a. Testen Sie, ob Git bereits installiert ist, indem Sie diesen Befehl ausführen.

```
git --version
```

b. Wenn der vorherige Befehl die Git-Version anzeigt, ist Git bereits installiert und Sie können mit Schritt 3 fortfahren.

c. Wenn bei der Ausführung des Befehls git ein Fehler angezeigt wird, installieren Sie Git, indem Sie diesen Befehl ausführen.

```
sudo apt-get install git
```

d. Testen Sie erneut, ob Git installiert ist, indem Sie diesen Befehl ausführen.

```
git --version
```

e. Wenn Git installiert ist, fahren Sie mit dem nächsten Abschnitt fort. Wenn nicht, beheben Sie den Fehler und korrigieren Sie ihn, bevor Sie fortfahren. Sie benötigen Git, um das AWS IoT Device SDK für zu installieren JavaScript.

Installieren Sie AWS IoT das Geräte-SDK

Installieren Sie das AWS IoT Geräte-SDK.

Python

In diesem Abschnitt installieren Sie Python, seine Entwicklungstools und das AWS IoT Device SDK für Python auf Ihrem Gerät. Diese Anweisungen gelten für einen Raspberry Pi, auf dem das neueste Raspberry Pi-Betriebssystem ausgeführt wird. Wenn Sie mit einem anderen Gerät arbeiten oder ein anderes Betriebssystem verwenden, müssen Sie diese Anweisungen für Ihr Gerät anpassen.

1. Installieren Sie Python und seine Entwicklungstools

   Für das AWS IoT Device SDK für Python muss Python v3.5 oder höher auf Ihrem Raspberry Pi installiert sein.

Führen Sie diese Befehle in einem Terminalfenster auf Ihrem Gerät aus.

1. Führen Sie diesen Befehl aus, um die auf Ihrem Gerät installierte Python-Version zu bestimmen.

   ```
   python3 --version
   ```

   Wenn Python installiert ist, wird seine Version angezeigt.
2. Wenn die angezeigte Version `Python 3.5` oder höher ist, können Sie mit Schritt 2 fortfahren.
3. Wenn die angezeigte Version niedriger als `Python 3.5` ist, können Sie die richtige Version installieren, indem Sie diesen Befehl ausführen.

   ```
   sudo apt install python3
   ```
4. Führen Sie diesen Befehl aus, um zu bestätigen, dass die richtige Version von Python jetzt installiert ist.

   ```
   python3 --version
   ```

2. Testen Sie auf pip3

Führen Sie diese Befehle in einem Terminalfenster Ihres Geräts aus.

1. Führen Sie diesen Befehl aus, um zu sehen, ob pip3 installiert ist.

   ```
   pip3 --version
   ```
2. Wenn der Befehl eine Versionsnummer zurückgibt, ist pip3 installiert und Sie können mit Schritt 3 fortfahren.
3. Wenn der vorherige Befehl einen Fehler zurückgibt, führen Sie diesen Befehl zur Installation von pip3 aus.

   ```
   sudo apt install python3-pip
   ```
4. Führen Sie diesen Befehl aus, um zu sehen, ob pip3 installiert ist.

   ```
   pip3 --version
   ```

3. Installieren Sie das aktuelle AWS IoT Geräte-SDK für Python

   Installieren Sie das AWS IoT Device SDK für Python und laden Sie die Beispiel-Apps auf Ihr Gerät herunter.

   Führen Sie diese Befehle auf Ihrem Gerät aus.

   ```
   cd ~
   python3 -m pip install awsiotsdk
   ```

   ```
   git clone https://github.com/aws/aws-iot-device-sdk-python-v2.git
   ```

JavaScript

In diesem Abschnitt installieren Sie Node.js, den npm-Paketmanager und das AWS IoT Geräte-SDK für JavaScript auf Ihrem Gerät. Diese Anweisungen gelten für einen Raspberry Pi, auf dem das Raspberry Pi OS ausgeführt wird. Wenn Sie mit einem anderen Gerät arbeiten oder ein anderes Betriebssystem verwenden, müssen Sie diese Anweisungen für Ihr Gerät anpassen.

1. Installieren der neuesten Version von Node.js

   Für das AWS IoT Geräte-SDK für JavaScript müssen Node.js und der npm-Paketmanager auf Ihrem Raspberry Pi installiert sein.

   a. Laden Sie die aktuelle Version des Knoten-Repositorys herunter, indem Sie einen der folgenden Befehle eingeben.

      ```
      cd ~
      curl -sL https://deb.nodesource.com/setup_12.x | sudo -E bash -
      ```

   b. Installieren Sie Node und npm.

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

   c. Überprüfen Sie die Installation von Node.

      ```
      node -v
      ```

Vergewissern Sie sich, dass der Befehl die Node-Version anzeigt. Dieses Tutorial erfordert Node v10.0 oder neuer. Wenn die Node-Version nicht angezeigt wird, versuchen Sie erneut, das Node-Repository herunterzuladen.

d. Überprüfen Sie die Installation von npm.

```
npm -v
```

Vergewissern Sie sich, dass der Befehl die npm-Version anzeigt. Wenn die npm-Version nicht angezeigt wird, versuchen Sie erneut, Node und npm zu installieren.

e. Starten Sie das Gerät neu.

```
sudo shutdown -r 0
```

Fahren Sie nach dem Neustart des Geräts fort.

2. Installieren Sie das AWS IoT Geräte-SDK für JavaScript

Installieren Sie das AWS IoT Geräte-SDK für JavaScript auf Ihrem Raspberry Pi.

a. Klonen Sie das AWS IoT Geräte-SDK für das JavaScript Repository in das `aws-iot-device-sdk-js-v2` Verzeichnis Ihres *home* Verzeichnisses. Auf dem Raspberry Pi ist das *home* Verzeichnis`~/`, das in den folgenden Befehlen als *home* Verzeichnis verwendet wird. Wenn Ihr Gerät einen anderen Pfad für das *home* Verzeichnis verwendet, müssen Sie es in `~/` den folgenden Befehlen durch den richtigen Pfad für Ihr Gerät ersetzen.

Diese Befehle erstellen das Verzeichnis `~/aws-iot-device-sdk-js-v2` und kopieren den SDK-Code hinein.

```
cd ~
git clone https://github.com/aws/aws-iot-device-sdk-js-v2.git
```

b. Wechseln Sie zu dem Verzeichnis `aws-iot-device-sdk-js-v2`, das Sie im vorherigen Schritt erstellt haben, und führen Sie `npm install` aus, um das SDK zu installieren. Der Befehl `npm install` ruft den Build der Bibliothek `aws-crt` auf, der einige Minuten in Anspruch nehmen kann.

```
cd ~/aws-iot-device-sdk-js-v2
```

```
npm install
```

### Installieren und Ausführen der Beispiel-App

In diesem Abschnitt installieren und führen Sie die `pubsub` Beispiel-App aus dem AWS IoT Geräte-SDK aus. Diese App zeigt, wie Ihr Gerät die MQTT-Bibliothek verwendet, um MQTT-Nachrichten zu veröffentlichen und zu abonnieren. Die Beispiel-App abonniert ein Thema, `topic_1`, veröffentlicht 10 Nachrichten zu diesem Thema und zeigt die Nachrichten so an, wie sie vom Message Broker empfangen wurden.

#### Installieren Sie die Zertifikatdateien

Für die Beispiel-App müssen die Zertifikatsdateien, die das Gerät authentifizieren, auf dem Gerät installiert sein.

Um die Gerätezertifikatsdateien für die Beispiel-App zu installieren

1. Erstellen Sie ein `certs` Unterverzeichnis in Ihrem *`home`* Verzeichnis, indem Sie diese Befehle ausführen.

   ```
   cd ~
   mkdir certs
   ```

2. Kopieren Sie das Zertifikat, den privaten Schlüssel und das Stammzertifikat, das Sie in `~/certs` erstellt haben, in das Verzeichnis the section called “AWS IoT Ressourcen erstellen”.

   Wie Sie die Zertifikatsdateien auf Ihr Gerät kopieren, hängt vom Gerät und Betriebssystem ab und wird hier nicht beschrieben. Wenn Ihr Gerät jedoch eine grafische Benutzeroberfläche (GUI) unterstützt und über einen Webbrowser verfügt, können Sie das unter the section called “AWS IoT Ressourcen erstellen” beschriebene Verfahren vom Webbrowser Ihres Geräts aus ausführen, um die resultierenden Dateien direkt auf Ihr Gerät herunterzuladen.

   Bei den Befehlen im nächsten Abschnitt wird davon ausgegangen, dass Ihr Schlüssel und Ihr Zertifikatdateien wie in dieser Tabelle gezeigt auf dem Gerät gespeichert sind.

   Namen der Zertifikatsdateien

| Datei | Dateipfad |
| --- | --- |
| CA-Stammzertifikat | `~/certs/Amazon-root-CA-1.pem` |

| Datei | Dateipfad |
| --- | --- |
| Gerätezertifikat | `~/certs/device.pem.crt` |
| Privater Schlüssel | `~/certs/private.pem.key` |

Zur Ausführung der Beispielanwendung benötigen Sie die folgenden Informationen:

Anwendungsparameterwerte

| Parameter | Wo der Wert gefunden werden kann |
| --- | --- |
| *`your-iot-endpoint`* | Wählen Sie in der AWS IoT -Konsole Alle Geräte und dann Objekte aus.<br><br>Auf der Einstellungsseite im AWS IoT Menü. Ihr Endpunkt wird im Abschnitt Gerätedaten-Endpunkt angezeigt. |

Der *`your-iot-endpoint`* Wert hat das Format:*`endpoint_id`*`-ats.iot.`*`region`*`.amazonaws.com`, zum Beispiel`a3qj468EXAMPLE-ats.iot.us-west-2.amazonaws.com`.

Python

Um die Beispiel-App zu installieren und auszuführen

1. Navigieren Sie zum Beispielverzeichnis.

   ```
   cd ~/aws-iot-device-sdk-python-v2/samples
   ```

2. Ersetzen Sie im Befehlszeilenfenster *`your-iot-endpoint`* wie angegeben und führen Sie diesen Befehl aus.

   ```
   python3 pubsub.py --topic topic_1 --ca_file ~/certs/Amazon-root-CA-1.pem --
   cert ~/certs/device.pem.crt --key ~/certs/private.pem.key --endpoint your-iot-
   endpoint
   ```

3. Beachten Sie, dass die Beispiel-App:

1. Stellt eine Verbindung mit dem AWS IoT Dienst für Ihr Konto her.
2. Das Nachrichtenthema topic_1 abonniert und die Nachrichten anzeigt, die es zu diesem Thema erhält.
3. 10 Nachrichten zum Thema topic_1 veröffentlicht.
4. Ihre Ausgabe sieht ähnlich aus wie:

```
Connecting to a3qEXAMPLEffp-ats.iot.us-west-2.amazonaws.com with client ID
 'test-0c8ae2ff-cc87-49d2-a82a-ae7ba1d0ca5a'...
Connected!
Subscribing to topic 'topic_1'...
Subscribed with QoS.AT_LEAST_ONCE
Sending 10 message(s)
Publishing message to topic 'topic_1': Hello World! [1]
Received message from topic 'topic_1': b'Hello World! [1]'
Publishing message to topic 'topic_1': Hello World! [2]
Received message from topic 'topic_1': b'Hello World! [2]'
Publishing message to topic 'topic_1': Hello World! [3]
Received message from topic 'topic_1': b'Hello World! [3]'
Publishing message to topic 'topic_1': Hello World! [4]
Received message from topic 'topic_1': b'Hello World! [4]'
Publishing message to topic 'topic_1': Hello World! [5]
Received message from topic 'topic_1': b'Hello World! [5]'
Publishing message to topic 'topic_1': Hello World! [6]
Received message from topic 'topic_1': b'Hello World! [6]'
Publishing message to topic 'topic_1': Hello World! [7]
Received message from topic 'topic_1': b'Hello World! [7]'
Publishing message to topic 'topic_1': Hello World! [8]
Received message from topic 'topic_1': b'Hello World! [8]'
Publishing message to topic 'topic_1': Hello World! [9]
Received message from topic 'topic_1': b'Hello World! [9]'
Publishing message to topic 'topic_1': Hello World! [10]
Received message from topic 'topic_1': b'Hello World! [10]'
10 message(s) received.
Disconnecting...
Disconnected!
```

Wenn Probleme bei der Ausführung der Beispiel-App auftreten, überprüfen Sie the section called “Beheben Sie Probleme mit der Beispielanwendung”.

Sie können den Parameter `--verbosity Debug` auch zur Befehlszeile hinzufügen, sodass die Beispiel-App detaillierte Meldungen darüber anzeigt, was sie tut. Diese Informationen bieten Ihnen möglicherweise die Hilfe, die Sie zur Behebung des Problems benötigen.

JavaScript

Um die Beispiel-App zu installieren und auszuführen

1. Navigieren Sie in Ihrem Befehlszeilenfenster zu dem `~/aws-iot-device-sdk-js-v2/samples/node/pub_sub`-Verzeichnis, das das SDK erstellt hat, und installieren Sie die Beispiel-App mithilfe dieser Befehle. Der Befehl `npm install` ruft den Build der `aws-crt` Bibliothek auf, der einige Minuten in Anspruch nehmen kann.

```
cd ~/aws-iot-device-sdk-js-v2/samples/node/pub_sub
npm install
```

2. Ersetzen Sie im Befehlszeilenfenster *`your-iot-endpoint`* wie angegeben und führen Sie diesen Befehl aus.

```
node dist/index.js --topic topic_1 --ca_file ~/certs/Amazon-root-CA-1.pem --
cert ~/certs/device.pem.crt --key ~/certs/private.pem.key --endpoint your-iot-
endpoint
```

3. Beachten Sie, dass die Beispiel-App:

   1. Stellt eine Verbindung mit dem AWS IoT Dienst für Ihr Konto her.
   2. Das Nachrichtenthema topic_1 abonniert und die Nachrichten anzeigt, die es zu diesem Thema erhält.
   3. 10 Nachrichten zum Thema topic_1 veröffentlicht.
   4. Ihre Ausgabe sieht ähnlich aus wie:

```
Publish received on topic topic_1
{"message":"Hello world!","sequence":1}
Publish received on topic topic_1
{"message":"Hello world!","sequence":2}
Publish received on topic topic_1
{"message":"Hello world!","sequence":3}
Publish received on topic topic_1
```

```
{"message":"Hello world!","sequence":4}
Publish received on topic topic_1
{"message":"Hello world!","sequence":5}
Publish received on topic topic_1
{"message":"Hello world!","sequence":6}
Publish received on topic topic_1
{"message":"Hello world!","sequence":7}
Publish received on topic topic_1
{"message":"Hello world!","sequence":8}
Publish received on topic topic_1
{"message":"Hello world!","sequence":9}
Publish received on topic topic_1
{"message":"Hello world!","sequence":10}
```

Wenn Probleme bei der Ausführung der Beispiel-App auftreten, überprüfen Sie the section called “Beheben Sie Probleme mit der Beispielanwendung”.

Sie können den Parameter `--verbosity Debug` auch zur Befehlszeile hinzufügen, sodass die Beispiel-App detaillierte Meldungen darüber anzeigt, was sie tut. Diese Informationen bieten Ihnen möglicherweise die Hilfe, die Sie zur Behebung des Problems benötigen.

Nachrichten aus der Beispiel-App in der AWS IoT Konsole anzeigen

Mithilfe des MQTT-Testclients in der AWS IoT -Konsole können Sie die Nachrichten der Beispiel-App sehen, während sie den Message Broker durchlaufen.

Um die von der Beispiel-App veröffentlichten MQTT-Nachrichten anzuzeigen

1. Sehen Sie sich MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen an. Auf diese Weise lernen Sie, wie Sie den MQTT-Testclient in der AWS IoT -Konsole verwenden, um MQTT-Nachrichten anzuzeigen, während sie den Message Broker passieren.
2. Öffnen Sie den MQTT-Testclient in der AWS IoT -Konsole.
3. Abonnieren Sie das Thema topic_1.
4. Führen Sie in Ihrem Befehlszeilenfenster die Beispiel-App erneut aus und sehen Sie sich die Nachrichten im MQTT-Client in der AWS IoT -Konsole an.

   Python

   ```
   cd ~/aws-iot-device-sdk-python-v2/samples
   ```

```
python3 pubsub.py --topic topic_1 --ca_file ~/certs/Amazon-root-CA-1.pem --
cert ~/certs/device.pem.crt --key ~/certs/private.pem.key --endpoint your-iot-
endpoint
```

JavaScript

```
cd ~/aws-iot-device-sdk-js-v2/samples/node/pub_sub
node dist/index.js --topic topic_1 --ca_file ~/certs/Amazon-root-CA-1.pem --
cert ~/certs/device.pem.crt --key ~/certs/private.pem.key --endpoint your-iot-
endpoint
```

## Beheben Sie Probleme mit der Beispielanwendung

Wenn beim Versuch, die Beispiel-App auszuführen, ein Fehler auftritt, sollten Sie Folgendes überprüfen.

Überprüfen Sie das Zertifikat

Wenn das Zertifikat nicht aktiv ist, AWS IoT werden keine Verbindungsversuche akzeptiert, bei denen es für die Autorisierung verwendet wird. Bei der Erstellung Ihres Zertifikats ist es leicht, die Schaltfläche Aktivieren zu übersehen. Zum Glück können Sie Ihr Zertifikat von der AWS IoT -Konsole aus aktivieren.

Um die Aktivierung Ihres Zertifikats zu überprüfen

1. Wählen Sie in der AWS IoT -Konsole im linken Menü die Option Sicher und dann Zertifikate aus.
2. Suchen Sie in der Liste der Zertifikate nach dem Zertifikat, das Sie für die Übung erstellt haben, und überprüfen Sie seinen Status in der Spalte Status.

   Wenn Sie sich nicht an den Namen des Zertifikats erinnern, suchen Sie nach den Zertifikaten, die inaktiv sind, um festzustellen, ob es sich dabei möglicherweise um das Zertifikat handelt, das Sie verwenden.

   Wählen Sie das Zertifikat in der Liste aus, um die Detailseite zu öffnen. Auf der Detailseite können Sie das Erstellungsdatum sehen, damit Sie das Zertifikat leichter identifizieren können.
3. Um ein inaktives Zertifikat zu aktivieren, wählen Sie auf der Detailseite des Zertifikats Aktionen und dann Aktivieren aus.

Wenn Sie das richtige Zertifikat gefunden haben und es aktiv ist, Sie aber immer noch Probleme beim Ausführen der Beispiel-App haben, überprüfen Sie die Richtlinien, wie im nächsten Schritt beschrieben.

Sie können auch versuchen, eine neue Sache und ein neues Zertifikat zu erstellen, indem Sie die Schritte unter the section called “Dies erstellt ein Objekt” befolgen. Wenn Sie eine neue Sache erstellen, müssen Sie ihr einen neuen Namen geben und die neuen Zertifikatsdateien auf Ihr Gerät herunterladen.

Prüfen Sie die dem Zertifikat angefügte Richtlinie

Richtlinien autorisieren Aktionen in AWS IoT. Wenn das Zertifikat, mit dem eine Verbindung zu AWS IoT hergestellt wird, keine Richtlinie hat oder nicht über eine Richtlinie verfügt, die das Herstellen einer Verbindung ermöglicht, wird die Verbindung verweigert, auch wenn das Zertifikat aktiv ist.

Um die einem Zertifikat beigefügten Richtlinien zu überprüfen

1. Suchen Sie das Zertifikat, wie im vorherigen Artikel beschrieben, und öffnen Sie die zugehörige Detailseite.
2. Wählen Sie im linken Menü der Detailseite des Zertifikats die Option Richtlinien aus, um die mit dem Zertifikat verknüpften Richtlinien anzuzeigen.
3. Wenn dem Zertifikat keine Richtlinien zugeordnet sind, fügen Sie eine hinzu, indem Sie das Menü Aktionen und dann Richtlinie anhängen wählen.

   Wählen Sie die Regel aus, die Sie zuvor in the section called “AWS IoT Ressourcen erstellen” erstellt haben.
4. Wenn eine Richtlinie angehängt ist, wählen Sie die Richtlinienkachel aus, um die Detailseite zu öffnen.

   Überprüfen Sie auf der Detailseite das Richtliniendokument, um sicherzustellen, dass es dieselben Informationen enthält wie das, in dem Sie es in the section called “Erstellen Sie eine AWS IoT Richtlinie” erstellt haben.

Überprüfen Sie die Befehlszeile

Stellen Sie sicher, dass Sie die richtige Befehlszeile für Ihr System verwendet haben. Die auf Linux- und MacOS-Systemen verwendeten Befehle unterscheiden sich häufig von denen, die auf Windows-Systemen verwendet werden.

Überprüfen Sie die Endpunktadresse

Überprüfen Sie den Befehl, den Sie eingegeben haben, und überprüfen Sie die Endpunktadresse in Ihrem Befehl noch einmal mit der Adresse in Ihrer AWS IoT -Konsole.

Überprüfen Sie die Dateinamen der Zertifikatsdateien

Vergleichen Sie die Dateinamen in dem Befehl, den Sie eingegeben haben, mit den Dateinamen der Zertifikatsdateien im Verzeichnis `certs`.

Bei einigen Systemen müssen die Dateinamen möglicherweise in Anführungszeichen gesetzt werden, damit sie korrekt funktionieren.

Überprüfen Sie die SDK-Installation

Stellen Sie sicher, dass Ihre SDK-Installation vollständig und korrekt ist.

Installieren Sie im Zweifelsfall das SDK erneut auf Ihrem Gerät. In den meisten Fällen müssen Sie den Abschnitt des Tutorials mit dem Titel Installieren des AWS IoT Geräte-SDK für finden *`SDK language`* und das Verfahren erneut ausführen.

Wenn Sie das AWS IoT Geräte-SDK für verwenden JavaScript, denken Sie daran, die Beispiel-Apps zu installieren, bevor Sie versuchen, sie auszuführen. Durch die Installation des SDK werden die Beispiel-Apps nicht automatisch installiert. Die Beispiel-Apps müssen nach der Installation des SDK manuell installiert werden.

# MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen

In diesem Abschnitt wird beschrieben, wie Sie den AWS IoT MQTT-Testclient in der AWS IoT Konsole verwenden, um die von gesendeten und empfangenen MQTT-Nachrichten zu beobachten. AWS IoT Das in diesem Abschnitt verwendete Beispiel bezieht sich auf die in verwendeten Beispiele. Sie können das in den Beispielen *`topicName`* verwendete Beispiel jedoch durch einen beliebigen Themennamen oder Themenfilter ersetzenErste Schritte mit AWS IoT Core Tutorials, der von Ihrer IoT-Lösung verwendet wird.

Geräte veröffentlichen MQTT-Nachrichten, die durch Themen gekennzeichnet sind, um ihnen ihren Status mitzuteilen AWS IoT, und veröffentlichen AWS IoT MQTT-Nachrichten, um die Geräte und Apps über Änderungen und Ereignisse zu informieren. Sie können den MQTT-Client verwenden, um diese Themen zu abonnieren und die Nachrichten zu beobachten, sobald sie auftreten. Sie können

den MQTT-Testclient auch verwenden, um MQTT-Nachrichten auf abonnierten Geräten und Diensten in Ihrem zu veröffentlichen. AWS-Konto

Inhalt

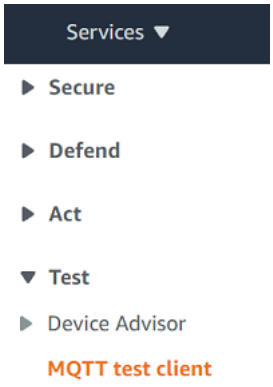

- Anzeigen von MQTT-Nachrichten im MQTT-Client
- Veröffentlichen von MQTT-Nachrichten vom MQTT-Client
- Testen von geteilten Abonnements im MQTT-Client


## Anzeigen von MQTT-Nachrichten im MQTT-Client

Das folgende Verfahren erklärt, wie Sie ein bestimmtes MQTT-Thema abonnieren, für das Ihr Gerät Nachrichten veröffentlicht, und wie Sie diese Nachrichten in der Konsole anzeigen können.AWS IoT

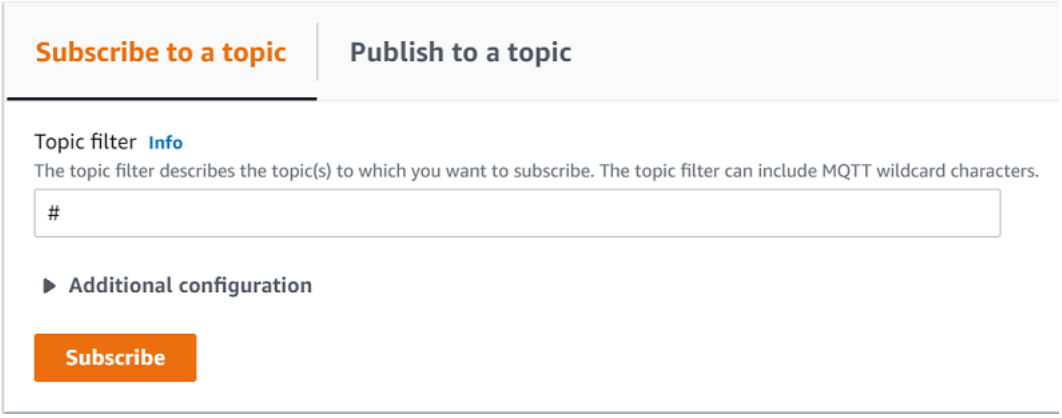
So zeigen Sie MQTT-Nachrichten im MQTT-Testclient an

1. Öffnen Sie die AWS IoT -Konsole und wählen Sie im linken Menü Test, um den MQTT-Client zu öffnen.

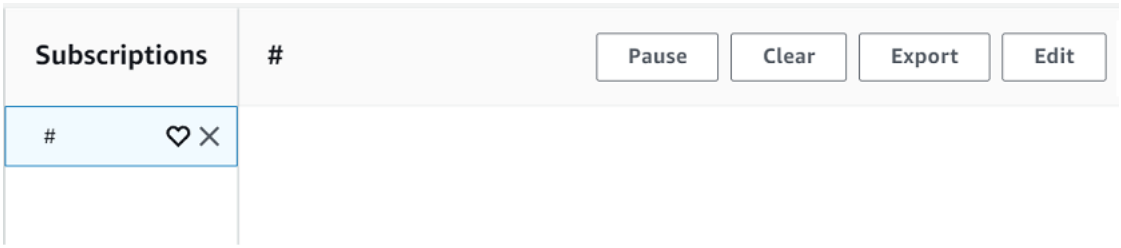



2. Geben Sie auf der Registerkarte Thema abonnieren die Option ein, *topicName* um das Thema zu abonnieren, zu dem Ihr Gerät veröffentlicht. Abonnieren Sie für die Beispiel-App „Erste Schritte“ **#**, womit alle Nachrichtenthemen abonniert werden.

   Um mit dem Beispiel Erste Schritte fortzufahren, geben Sie auf der Registerkarte Thema abonnieren im Feld Themenfilter **#** ein, und wählen Sie dann Abonnieren aus.




Die Protokollseite der Themennachricht, #, wird geöffnet und **#** wird in der Abonnementliste angezeigt. Wenn das Gerät, auf dem Sie konfiguriert haben, das Beispielprogramm ausführt, sollten Sie die Nachrichten, an die es sendet, AWS IoT im # Message-Log sehen. the section called “Konfigurieren Ihres Geräts” Die Nachrichtenprotokolleinträge werden unter dem Abschnitt Veröffentlichen angezeigt, wenn Nachrichten mit dem abonnierten Thema bei eingegangen AWS IoT sind.




3. Auf der Seite # Nachrichtenprotokoll können Sie auch Nachrichten zu einem Thema veröffentlichen, dafür müssen Sie jedoch den Namen des Themas angeben. Veröffentlichen Sie eine Benachrichtigung für das Thema #.

   Nachrichten, die zu abonnierten Themen veröffentlicht wurden, werden im Nachrichtenprotokoll angezeigt, sobald sie empfangen wurden, wobei die neueste Nachricht an erster Stelle steht.

## Fehlerbehebung für MQTT-Nachrichten

### Verwenden Sie den Themenfilter mit Platzhaltern

Wenn Ihre Nachrichten nicht wie erwartet im Nachrichtenprotokoll angezeigt werden, versuchen Sie, wie unter Filter für Themennamen beschrieben, ein Platzhalter-Thema zu abonnieren. Der mehrstufige MQTT-Wildcard-Themenfilter ist das Hash- oder Rautenzeichen (#) und kann als Themenfilter im Themenfeld Abonnementsthemen verwendet werden.

Wenn Sie den # Themenfilter abonnieren, abonnieren Sie jedes Thema, das der Message Broker empfängt. Sie können den Filter eingrenzen, indem Sie Elemente des Themenfilterpfads durch ein # Platzhalterzeichen mit mehreren Ebenen oder das einstufige Platzhalterzeichen '+' ersetzen.

Bei der Verwendung von Platzhaltern in einem Themenfilter

- Das Platzhalterzeichen mit mehreren Ebenen muss das letzte Zeichen im Themenfilter sein.
- Der Themenfilterpfad kann nur ein Platzhalterzeichen mit einer Ebene pro Themenebene enthalten.

Beispielsweise:

| Themenfilter | Zeigt Nachrichten an mit |
|---|---|
| # | Beliebiger Themenname |
| `topic_1/#` | Ein Themenname, der mit `topic_1/` beginnt |
| `topic_1/level_2/#` | Ein Themenname, der mit `topic_1/level_2/` beginnt |
| `topic_1/+/level_3` | Ein Themenname, der mit `topic_1/` beginnt, mit `/level_3` endet und dazwischen ein Element beliebigen Wertes enthält. |

Weitere Informationen zu Filtern finden Sie unter Filter für Themennamen.

Suchen Sie nach Fehlern beim Themennamen

MQTT-Themennamen und Themenfilter berücksichtigen Groß- und Kleinschreibung. Wenn Ihr Gerät beispielsweise Nachrichten an `Topic_1` (mit einem großen T) statt an `topic_1`, das Thema, das Sie abonniert haben, veröffentlicht, werden seine Nachrichten nicht im MQTT-Testclient angezeigt. Wenn Sie jedoch den Themenfilter mit Platzhaltern abonnieren, wird angezeigt, dass das Gerät gerade Nachrichten veröffentlicht, und Sie könnten sehen, dass es einen Themennamen verwendet, der nicht dem entspricht, den Sie erwartet haben.

# Veröffentlichen von MQTT-Nachrichten vom MQTT-Client

So veröffentlichen Sie eine Nachricht in einem MQTT-Thema

1. Geben Sie auf der Seite des MQTT-Testclients auf der Registerkarte In einem Thema veröffentlichen im Feld Themenname den Text *topicName* Ihrer Nachricht ein. Verwenden Sie **my/topic** in diesem Beispiel.

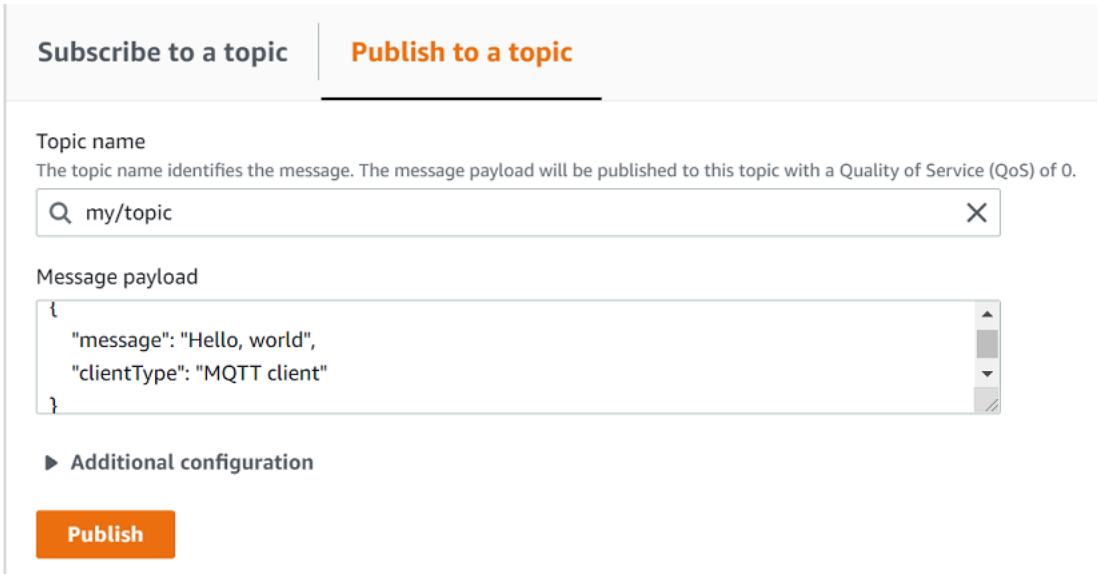
   > **Note**
   >
   > Verwenden Sie keine persönlich identifizierbaren Informationen in Themennamen, unabhängig davon, ob Sie sie im MQTT-Testclient oder in Ihrer Systemimplementierung verwenden. Themennamen können in unverschlüsselten Mitteilungen und Berichten vorkommen.

2. Geben Sie im Abschnitt für die Nachrichten-Nutzlast den folgenden JSON-Code ein:

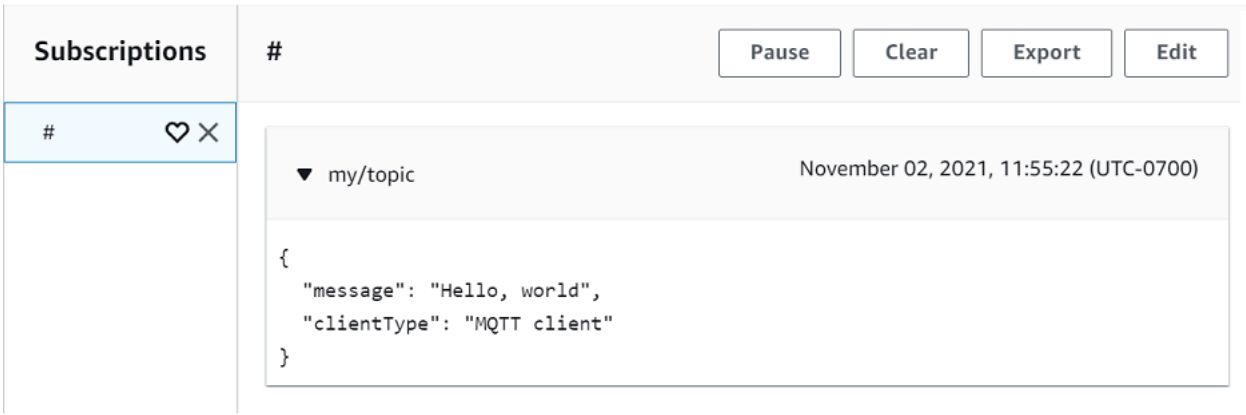
   ```
   {
       "message": "Hello, world",
       "clientType": "MQTT test client"
   }
   ```

3. Wählen Sie Veröffentlichen aus, um Ihre Nachricht in AWS IoT zu veröffentlichen.

   > **Note**
   >
   > Vergewissern Sie sich, dass Sie das Thema my/topic abonniert haben, bevor Sie Ihre Nachricht veröffentlichen.




4. Wählen Sie in der Spalte Abonnement die Option my/topic aus, um die Nachricht anzuzeigen. Sie sollten sehen, dass die Nachricht im MQTT-Testclient unter dem Payload-Fenster für die Nachrichtenveröffentlichung erscheint.




Sie können MQTT-Nachrichten zu anderen Themen veröffentlichen, indem Sie das *topicName* im Feld Themenname ändern und die Schaltfläche Veröffentlichen wählen.

> **Important**
>
> Wenn Sie mehrere Abonnements mit sich überschneidenden Themen erstellen (z. B. Sonde1/Temperatur und Sonde1/#), besteht die Möglichkeit, dass eine einzelne Nachricht, die zu einem Thema veröffentlicht wurde, das beiden Abonnements entspricht, mehrfach zugestellt wird, einmal für jedes überlappende Abonnement.

# Testen von geteilten Abonnements im MQTT-Client

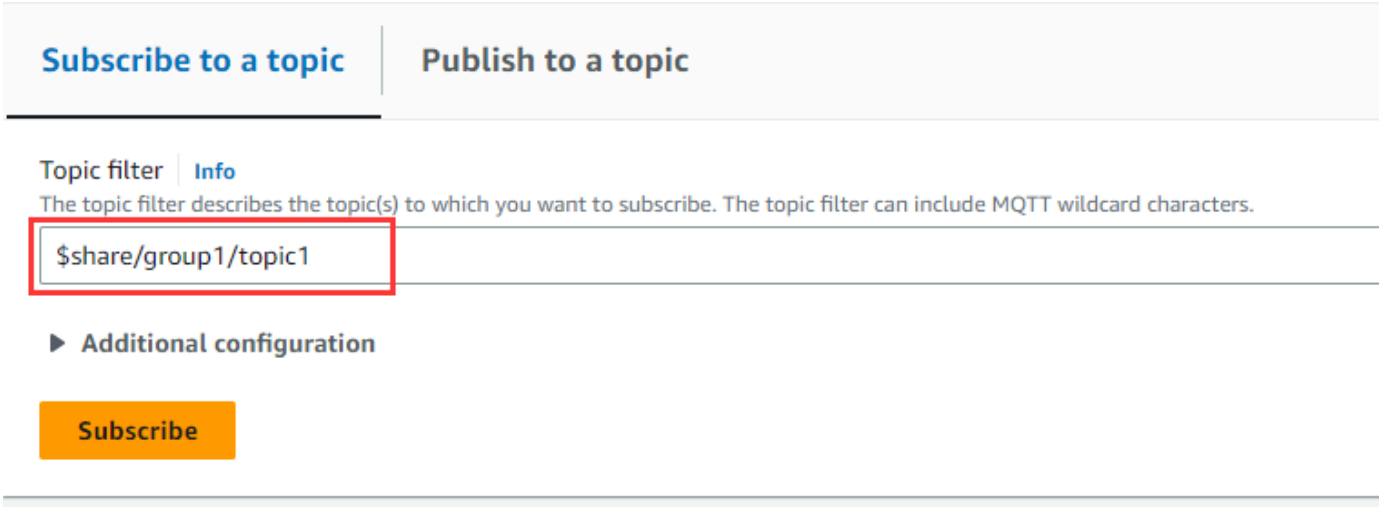
In diesem Abschnitt wird beschrieben, wie Sie den AWS IoT MQTT-Client in der AWS IoT Konsole verwenden, um die mit Shared Subscriptions gesendeten und empfangenen MQTT-Nachrichten anzusehen. AWS IoT ???ermöglicht es mehreren Clients, ein Abonnement für ein Thema gemeinsam zu nutzen, wobei nur ein Client Nachrichten erhält, die zu diesem Thema veröffentlicht wurden, und zwar nach dem Zufallsprinzip. Um zu simulieren, dass mehrere MQTT-Clients (in diesem Beispiel zwei MQTT-Clients) dasselbe Abonnement nutzen, öffnen Sie den AWS IoT MQTT-Client in der AWS IoT Konsole von mehreren Webbrowsern aus. Das in diesem Abschnitt verwendete Beispiel bezieht sich nicht auf die in Erste Schritte mit AWS IoT Core Tutorials verwendeten Beispiele. Weitere Informationen finden Sie unter Geteilte Abonnements.

Um ein Abonnement für ein MQTT-Thema zu teilen

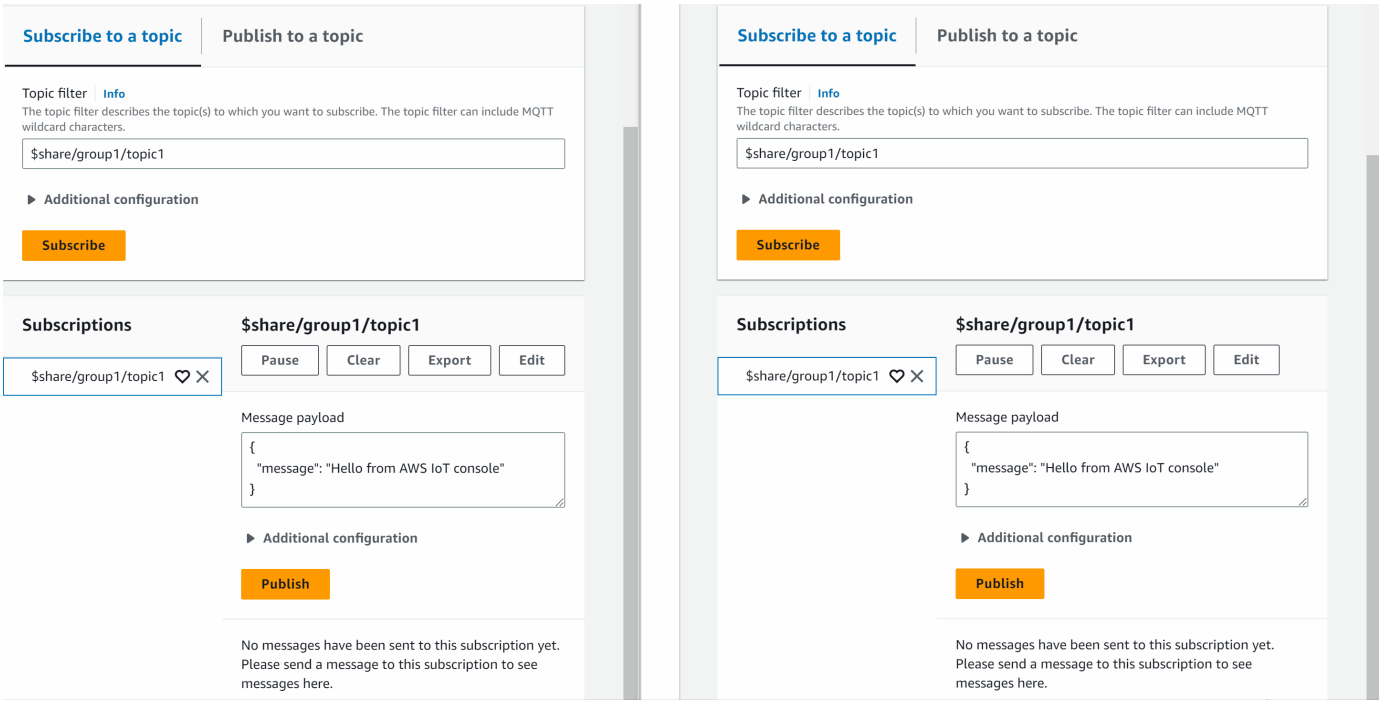
1. Wählen Sie in der AWS IoT -Konsole im Navigationsbereich Test und dann MQTT-Testclient aus.
2. Geben Sie auf der Registerkarte Thema abonnieren den ein, *topicName* um das Thema zu abonnieren, zu dem Ihr Gerät veröffentlicht. Um geteilte Abonnements zu verwenden, abonnieren Sie den Themenfilter eines geteilten Abonnements wie folgt:

   ```
   $share/{ShareName}/{TopicFilter}
   ```

   Ein Beispiel für einen Themenfilter kann **$share/group1/topic1** sein, der das Nachrichtenthema **topic1** abonniert.



3. Öffnen Sie einen anderen Webbrowser und wiederholen Sie Schritt 1 und Schritt 2. Auf diese Weise simulieren Sie zwei verschiedene MQTT-Clients, die dasselbe Abonnement **`$share/group1/topic1`** verwenden.
4. Wählen Sie einen MQTT-Client aus und geben Sie auf der Registerkarte In einem Thema veröffentlichen im Feld Themenname den Text *`topicName`* Ihrer Nachricht ein. Verwenden Sie **`topic1`** in diesem Beispiel. Versuchen Sie, die Nachricht ein paar Mal zu veröffentlichen. Aus der Abonnementliste der beiden MQTT-Clients sollten Sie erkennen können, dass die Clients die Nachricht mit einer zufälligen Verteilung empfangen. In diesem Beispiel veröffentlichen wir dreimal dieselbe Nachricht „Hallo von der AWS IoT Konsole“. Der MQTT-Client auf der linken Seite hat die Nachricht zweimal empfangen und der MQTT-Client auf der rechten Seite hat die Nachricht einmal erhalten.



# AWS IoT Anleitungen

Die AWS IoT Tutorials sind in zwei Lernpfade unterteilt, um zwei unterschiedliche Ziele zu erreichen. Wählen Sie den Lernpfad, der am besten zu Ihrem Ziel passt.

- Sie möchten eine AWS IoT Lösungsidee erstellen proof-of-concept, um sie zu testen oder zu demonstrieren

  Folgen Sie dem the section called “Demos mit dem AWS IoT Device Client erstellen” Lernpfad, um allgemeine IoT-Aufgaben und -Anwendungen mit dem AWS IoT Device Client auf Ihren Geräten zu demonstrieren. Der AWS IoT Device Client bietet Gerätesoftware, mit der Sie Ihre eigenen Cloud-Ressourcen einsetzen können, um eine end-to-end Lösung mit minimalem Entwicklungsaufwand zu demonstrieren.

  Informationen zum AWS IoT Geräteclient finden Sie unter AWS IoT Geräteclient.
- Sie möchten lernen, wie Sie Produktionssoftware für die Implementierung Ihrer Lösung erstellen

  Folgen Sie dem the section called “Mit dem AWS IoT Gerät Lösungen entwickeln SDKs” Lernpfad, um mithilfe eines AWS IoT Geräte-SDK Ihre eigene Lösungssoftware zu erstellen, die Ihren spezifischen Anforderungen entspricht.

  Informationen zum verfügbaren AWS IoT Gerät finden Sie SDKs unter???. Informationen zu den finden Sie unter Tools AWS SDKs, auf denen Sie aufbauen können AWS.

AWS IoT Optionen des Lernpfads für Tutorials

- Demos mit dem AWS IoT Device Client erstellen
- Mit dem AWS IoT Gerät Lösungen entwickeln SDKs

## Demos mit dem AWS IoT Device Client erstellen

Die Tutorials in diesem Lernpfad führen Sie durch die Schritte zur Entwicklung von Demonstrationssoftware mithilfe des AWS IoT Device Client. Der AWS IoT Device Client bietet Software, die auf Ihrem IoT-Gerät ausgeführt wird, um Aspekte einer darauf aufbauenden IoT-Lösung zu testen und zu demonstrieren AWS IoT.

Ziel dieser Tutorials ist es, die Erkundung und das Experimentieren zu erleichtern, damit Sie sicher sein können, dass diese Lösung AWS IoT unterstützt, bevor Sie Ihre Gerätesoftware entwickeln.

Was Sie in diesen Tutorials lernen werden:

- So bereiten Sie einen Raspberry Pi für die Verwendung als IoT-Gerät vor mit AWS IoT
- So demonstrieren Sie AWS IoT Funktionen mithilfe des AWS IoT Geräteclients auf Ihrem Gerät

In diesem Lernpfad installieren Sie den AWS IoT Device Client auf Ihrem eigenen Raspberry Pi und erstellen die AWS IoT Ressourcen in der Cloud, um IoT-Lösungsideen zu demonstrieren. In den Tutorials in diesem Lernpfad werden zwar Features anhand eines Raspberry Pi demonstriert, aber sie erläutern die Ziele und Verfahren, um Sie bei der Anpassung an andere Geräte zu unterstützen.

## Voraussetzungen für die Erstellung von Demos mit dem AWS IoT Geräte-Client

In diesem Abschnitt wird beschrieben, was Sie benötigen, bevor Sie mit den Tutorials in diesem Lernpfad beginnen.

Um die Tutorials in diesem Lernpfad abzuschließen, benötigen Sie:

- Ein AWS-Konto

  Sie können Ihre vorhandenen verwenden AWS-Konto, sofern Sie über eine verfügen. Möglicherweise müssen Sie jedoch zusätzliche Rollen oder Berechtigungen hinzufügen, um die AWS IoT Funktionen nutzen zu können, die in diesen Tutorials verwendet werden.

  Wenn Sie eine neue erstellen müssen AWS-Konto, finden Sie weitere Informationen unterthe section called “Einrichten AWS-Konto”.
- Ein Raspberry Pi oder ein kompatibles IoT-Gerät

  In den Tutorials wird ein Raspberry Pi verwendet, da er in verschiedenen Formfaktoren erhältlich ist, allgegenwärtig ist und es sich um ein relativ kostengünstiges Demonstrationsgerät handelt. Die Tutorials wurden auf dem Raspberry Pi 3 Model B+, dem Raspberry Pi 4 Model B und auf einer EC2 Amazon-Instance getestet, auf der Ubuntu Server 20.04 LTS (HVM) läuft. Um die Befehle zu verwenden AWS CLI und auszuführen, empfehlen wir Ihnen, die neueste Version des Raspberry Pi-Betriebssystems (Raspberry Pi OS (64-Bit) oder OS Lite) zu verwenden. Frühere Versionen des Betriebssystems funktionieren möglicherweise, aber wir haben sie nicht getestet.

> **Note**
>
> In den Tutorials werden die Ziele der einzelnen Schritte erklärt, um Ihnen zu helfen, sie an IoT-Hardware anzupassen, auf der wir sie noch nicht getestet haben. Sie beschreiben jedoch nicht speziell, wie Sie sie an andere Geräte anpassen können.

- Vertrautheit mit dem Betriebssystem des IoT-Geräts

  Bei den Schritten in diesen Tutorials wird davon ausgegangen, dass Sie mit der Verwendung grundlegender Linux-Befehle und -Operationen über die von einem Raspberry Pi unterstützte Befehlszeilenschnittstelle vertraut sind. Wenn Sie mit diesen Vorgängen nicht vertraut sind, sollten Sie sich vielleicht mehr Zeit nehmen, um die Tutorials abzuschließen.

  Um diese Tutorials abzuschließen, sollten Sie bereits wissen, wie Sie:

  - grundlegende Geräteoperationen wie das Zusammenbauen und Anschließen von Komponenten, das Anschließen des Geräts an die erforderlichen Stromquellen und das Installieren und Entfernen von Speicherkarten sicher durchführen.
  - Systemsoftware und Dateien auf das Gerät hoch- und herunterladen. Wenn Ihr Gerät kein Wechselspeichergerät wie eine microSD-Karte verwendet, müssen Sie wissen, wie Sie eine Verbindung zu Ihrem Gerät herstellen und Systemsoftware und Dateien auf das Gerät hoch- und herunterladen.
  - Verbinden Sie Ihr Gerät mit den Netzwerken, in denen Sie es verwenden möchten.
  - Stellen Sie über ein SSH-Terminal oder ein ähnliches Programm von einem anderen Computer aus eine Verbindung zu Ihrem Gerät her.
  - Verwenden Sie eine Befehlszeilenschnittstelle, um Dateien und Verzeichnisse auf dem Gerät zu erstellen, zu kopieren, zu verschieben, umzubenennen und deren Berechtigungen festzulegen.
  - Installieren Sie neue Programme auf dem Gerät.
  - Übertragen Sie Dateien mit Tools wie FTP oder SCP zu und von Ihrem Gerät.
- Eine Entwicklungs- und Testumgebung für Ihre IoT-Lösung

  In den Tutorials wird die erforderliche Software und Hardware beschrieben. In den Tutorials wird jedoch davon ausgegangen, dass Sie Operationen ausführen können, die möglicherweise nicht explizit beschrieben werden. Zu den Beispielen für solche Hardware und Operationen gehören:

  - Ein lokaler Host-Computer zum Herunterladen und Speichern von Dateien

Für den Raspberry Pi ist dies normalerweise ein PC oder Laptop, der microSD-Speicherkarten lesen und auf sie schreiben kann. Der lokale Host-Computer muss:

- mit dem Internet verbunden sein.
- AWS CLI installiert und konfiguriert haben.
- Verfügen Sie über einen Webbrowser, der die AWS Konsole unterstützt.

- Eine Möglichkeit, Ihren lokalen Host-Computer mit Ihrem Gerät zu verbinden, um mit ihm zu kommunizieren, Befehle einzugeben und Dateien zu übertragen

  Auf dem Raspberry Pi erfolgt dies häufig mithilfe von SSH und SCP vom lokalen Host-Computer aus.

- Ein Monitor und eine Tastatur zum Anschluss an Ihr IoT-Gerät

  Diese können hilfreich sein, sind aber nicht erforderlich, um die Tutorials abzuschließen.

- Eine Möglichkeit für Ihren lokalen Host-Computer und Ihre IoT-Geräte, sich mit dem Internet zu verbinden

  Dies kann eine verkabelte oder eine drahtlose Netzwerkverbindung zu einem Router oder Gateway sein, der mit dem Internet verbunden ist. Der lokale Host muss eine Verbindung zum Raspberry Pi herstellen können. Dazu müssen sie sich möglicherweise im selben lokalen Netzwerk befinden. Die Tutorials können Ihnen nicht zeigen, wie Sie dies für Ihr spezielles Gerät oder Ihre Gerätekonfiguration einrichten, aber sie zeigen, wie Sie diese Konnektivität testen können.

- Zugriff auf den Router Ihres lokalen Netzwerks, um die angeschlossenen Geräte anzuzeigen

  Um die Tutorials in diesem Lernpfad abschließen zu können, müssen Sie in der Lage sein, die IP-Adresse Ihres IoT-Geräts zu ermitteln.

  In einem lokalen Netzwerk können Sie dazu auf die Admin-Oberfläche des Netzwerk-Routers zugreifen, mit dem Ihre Geräte verbunden sind. Wenn Sie Ihrem Gerät im Router eine feste IP-Adresse zuweisen können, können Sie die Wiederverbindung nach jedem Neustart des Geräts vereinfachen.

  Wenn Sie eine Tastatur und einen Monitor an das Gerät angeschlossen haben, kann ifconfig die IP-Adresse des Geräts angezeigt werden.

  Wenn keine dieser Optionen in Frage kommt, müssen Sie einen Weg finden, die IP-Adresse des Geräts nach jedem Neustart zu ermitteln.

Wenn Sie alle Ihre Materialien haben, fahren Sie mit the section called “Vorbereitung der Verwendung des IoT Device Client” fort.

Tutorials in diesem Lernpfad

- Tutorial: Vorbereiten Ihrer Geräte für den AWS IoT Device Client
- Tutorials: Installieren und Konfigurieren des AWS IoT Device Clients
- Tutorial: Demonstrieren MQTT Sie die Nachrichtenkommunikation mit dem AWS IoT Device Client
- Tutorial: Demonstrieren von Remote-Aktionen (Jobs) mit dem AWS IoT Device Client
- Tutorial: Aufräumen nach dem Ausführen der AWS IoT Device Client-Tutorials

## Tutorial: Vorbereiten Ihrer Geräte für den AWS IoT Device Client

Dieses Tutorial führt Sie durch die Initialisierung Ihres Raspberry Pi, um ihn auf die nachfolgenden Tutorials in diesem Lernpfad vorzubereiten.

Ziel dieses Tutorials ist es, die aktuelle Version des Betriebssystems des Geräts zu installieren und sicherzustellen, dass Sie im Kontext Ihrer Entwicklungsumgebung mit Ihrem Gerät kommunizieren können.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, stellen Sie sicher, dass die unter aufgeführten Elemente the section called “Voraussetzungen für die Erstellung von Demos mit dem AWS IoT Geräte-Client” verfügbar und einsatzbereit sind.

Für dieses Tutorial brauchen Sie ungefähr 90 Minuten.

In diesem Tutorial führen Sie die folgenden Aktivitäten durch:

- Installieren und aktualisieren Sie das Betriebssystem Ihres Geräts.
- Installieren und überprüfen Sie alle zusätzliche Software, die für die Ausführung der Tutorials erforderlich ist.
- Testen Sie die Konnektivität Ihres Geräts und installieren Sie die erforderlichen Zertifikate.

Nachdem Sie dieses Tutorial abgeschlossen haben, bereitet das nächste Tutorial Ihr Gerät auf die Demos vor, die den AWS IoT Device Client verwenden.

Verfahren in diesem Tutorial

- Installieren und aktualisieren Sie das Betriebssystem des Geräts
- Installieren und überprüfen Sie die erforderliche Software auf Ihrem Gerät
- Testen Sie Ihr Gerät und speichern Sie das Amazon CA-Zertifikat

## Installieren und aktualisieren Sie das Betriebssystem des Geräts

Die Verfahren in diesem Abschnitt beschreiben, wie Sie die microSD-Karte initialisieren, die der Raspberry Pi für sein Systemlaufwerk verwendet. Die microSD-Karte des Raspberry Pi enthält die Betriebssystemsoftware (OS) sowie Speicherplatz für die Anwendungsdateien. Wenn Sie keinen Raspberry Pi verwenden, folgen Sie den Anweisungen des Geräts, um die Betriebssystemsoftware des Geräts zu installieren und zu aktualisieren.

Nachdem Sie diesen Abschnitt abgeschlossen haben, sollten Sie in der Lage sein, Ihr IoT-Gerät zu starten und über das Terminalprogramm auf Ihrem lokalen Host-Computer eine Verbindung herzustellen.

Erforderliche Ausstattung:

- Ihre lokale Entwicklungs- und Testumgebung
- Ein Raspberry Pi oder Ihr IoT-Gerät, das eine Verbindung zum Internet herstellen kann
- Eine microSD-Speicherkarte mit einer Kapazität von mindestens 8 GB oder ausreichend Speicherplatz für das Betriebssystem und die erforderliche Software.

> **Note**
>
> Wählen Sie für diese Übungen eine microSD-Karte, die so groß wie nötig, aber so klein wie möglich ist.
> Eine kleine SD-Karte lässt sich schneller sichern und aktualisieren. Auf dem Raspberry Pi benötigen Sie für diese Tutorials nicht mehr als eine microSD-Karte mit 8 GB. Wenn Sie mehr Speicherplatz für Ihre spezifische Anwendung benötigen, können Sie mit den kleineren Image-Dateien, die Sie in diesen Tutorials speichern, die Größe des Dateisystems auf einer größeren Karte ändern, sodass der gesamte unterstützte Speicherplatz der von Ihnen ausgewählten Karte genutzt wird.

Optionale Ausstattung:

- Eine USB Tastatur, die an den Raspberry Pi angeschlossen ist

- Ein HDMI Monitor und ein Kabel zum Anschließen des Monitors an den Raspberry Pi

Verfahren in diesem Abschnitt:

- Herunterladen des Betriebssystems des Geräts auf die microSD-Karte
- Starten Ihres IoT-Geräts mit dem neuen Betriebssystem
- Verbinden Ihres Geräts mit Ihrem lokalen Host-Computer

Herunterladen des Betriebssystems des Geräts auf die microSD-Karte

Bei diesem Verfahren wird der lokale Host-Computer verwendet, um das Betriebssystem des Geräts auf eine microSD-Karte zu laden.

> **Note**
>
> Wenn Ihr Gerät kein Wechselspeichermedium für sein Betriebssystem verwendet, installieren Sie das Betriebssystem anhand des Verfahrens für dieses Gerät und fahren Sie fort mit the section called “Starten Sie Ihr IoT-Gerät”.

So installieren Sie das Betriebssystem auf Ihrem Raspberry Pi:

1. Laden Sie das Raspberry-Pi-Betriebssystem-Image, das Sie verwenden möchten, auf Ihren lokalen Host-Computer herunter und entpacken Sie es. Die neuesten Versionen sind unter https://www.raspberrypi.com/software/operating-systems/ erhältlich

   Auswahl einer Version des Raspberry Pi OS

   In diesem Tutorial wird die Lite-Version des Raspberry Pi OS verwendet, da dies die kleinste Version ist, die die Tutorials in diesem Lernpfad unterstützt. Diese Version des Raspberry Pi OS hat nur eine Befehlszeilenschnittstelle und keine grafische Benutzeroberfläche. Eine Version des neuesten Raspberry-Pi-Betriebssystems mit grafischer Benutzeroberfläche kann im Rahmen dieser Tutorials auch verwendet werden. Die in diesem Lernpfad beschriebenen Verfahren verwenden jedoch nur die Befehlszeilenschnittstelle zur Durchführung von Vorgängen auf dem Raspberry Pi.
2. Legen Sie die microSD-Karte in den lokalen Host-Computer ein.
3. Schreiben Sie die entpackte OS-Image-Datei mit einem SD-Karten-Imaging-Tool auf die microSD-Karte.

4. Nach dem Schreiben des Raspberry-Pi-OS-Images auf die microSD-Karte:

   a. Öffnen Sie die BOOT Partition auf der microSD-Karte in einem Befehlszeilenfenster oder einem Datei-Explorer-Fenster.

   b. Erstellen Sie in der BOOT Partition der microSD-Karte im Stammverzeichnis eine leere Datei `ssh` mit dem Namen ohne Dateierweiterung und ohne Inhalt. Dadurch wird der Raspberry Pi angewiesen, die SSH Kommunikation beim ersten Start zu aktivieren.

5. Werfen Sie die microSD-Karte aus und entfernen Sie sie sicher vom lokalen Host-Computer.

Ihre microSD-Karte ist nun einsatzbereit für the section called “Starten Sie Ihr IoT-Gerät”.

Starten Ihres IoT-Geräts mit dem neuen Betriebssystem

Dieses Verfahren installiert die microSD-Karte und startet Ihren Raspberry Pi zum ersten Mal mit dem heruntergeladenen Betriebssystem.

So starten Sie Ihr IoT-Gerät mit dem neuen Betriebssystem:

1. Trennen Sie das Gerät von der Stromversorgung und legen Sie die microSD-Karte aus dem vorherigen Schritt, the section called “Laden Sie das Betriebssystem”, in den Raspberry Pi ein.
2. Verbinden Sie das Gerät mit einem kabelgebundenen Netzwerk.
3. Diese Tutorials interagieren mit Ihrem Raspberry Pi von Ihrem lokalen Host-Computer aus über ein SSH Terminal.

   Wenn Sie auch direkt mit dem Gerät interagieren möchten, können Sie:

   a. Connect einen HDMI Monitor an, um die Konsolenmeldungen des Raspberry Pi anzusehen, bevor Sie das Terminalfenster auf Ihrem lokalen Host-Computer mit Ihrem Raspberry Pi verbinden können.

   b. Connect eine USB Tastatur an, wenn Sie direkt mit dem Raspberry Pi interagieren möchten.

4. Einen Raspberry Pi an die Stromversorgung anschließen und etwa eine Minute warten, bis er initialisiert ist

   Wenn Sie einen Monitor an Ihren Raspberry Pi angeschlossen haben, können Sie den Startvorgang darauf verfolgen.

5. Finden Sie die IP-Adresse Ihres Geräts heraus:

- Wenn Sie einen HDMI Monitor an den Raspberry Pi angeschlossen haben, erscheint die IP-Adresse in den auf dem Monitor angezeigten Meldungen
- Wenn Sie Zugriff auf den Router haben, mit dem Ihr Raspberry Pi verbunden ist, können Sie dessen Adresse in der Admin-Oberfläche des Routers sehen.

Wenn Sie die IP-Adresse Ihres Raspberry Pi haben, sind Sie bereit für the section called “Connect Ihren Host-Computer”.

Verbinden Ihres Geräts mit Ihrem lokalen Host-Computer

Bei diesem Verfahren wird das Terminalprogramm auf Ihrem lokalen Host-Computer verwendet, um eine Verbindung zu Ihrem Raspberry Pi herzustellen und das Standardpasswort zu ändern.

So verbinden Sie Ihr Gerät mit Ihrem lokalen Host-Computer:

1. Öffnen Sie auf Ihrem lokalen Host-Computer das SSH Terminalprogramm:

   - Windows: `PuTTY`
   - Linux/macOS: `Terminal`

   > **Note**
   >
   > Pu wird unter Windows TTY nicht automatisch installiert. Wenn es sich nicht auf Ihrem Computer befindet, müssen Sie es möglicherweise herunterladen und installieren.

2. Verbinden Sie das Terminalprogramm mit der IP-Adresse Ihres Raspberry Pi und melden Sie sich mit den Standardanmeldeinformationen an.

   ```
   username: pi
   password: raspberry
   ```

3. Nachdem Sie sich bei Ihrem Raspberry Pi angemeldet haben, ändern Sie das Passwort für den Benutzer `pi`.

   ```
   passwd
   ```

   Folgen Sie den Eingabeaufforderungen, um das Passwort zu ändern.

```
Changing password for pi.
Current password: raspberry
New password: YourNewPassword
Retype new password: YourNewPassword
passwd: password updated successfully
```

Nachdem Sie die Befehlszeilenaufforderung des Raspberry Pi im Terminalfenster angezeigt und das Passwort geändert haben, können Sie mit the section called “Installieren und verifizieren Sie die erforderliche Software” fortfahren.

## Installieren und überprüfen Sie die erforderliche Software auf Ihrem Gerät

Die Verfahren in diesem Abschnitt setzen mit dem vorherigen Abschnitt fort, um das Betriebssystem Ihres Raspberry Pi auf den neuesten Stand zu bringen und die Software auf dem Raspberry Pi zu installieren, die im nächsten Abschnitt zur Erstellung und Installation des AWS IoT Geräteclients verwendet wird.

Nachdem Sie diesen Abschnitt abgeschlossen haben, verfügt Ihr Raspberry Pi über ein up-to-date Betriebssystem, die Software, die für die Tutorials in diesem Lernpfad erforderlich ist, und es wird für Ihren Standort konfiguriert.

Erforderliche Ausstattung:

- Ihre lokale Entwicklungs- und Testumgebung aus dem vorherigen Abschnitt
- Der Raspberry Pi, den Sie im vorherigen Abschnitt verwendet haben
- Die microSD-Speicherkarte aus dem vorherigen Abschnitt

> **Note**
>
> Raspberry Pi Model 3+ und das Raspberry Pi Model 4 können alle in diesem Lernpfad beschriebenen Befehle ausführen. Wenn Ihr IoT-Gerät keine Software kompilieren oder ausführen kann AWS Command Line Interface, müssen Sie möglicherweise die erforderlichen Compiler auf Ihrem lokalen Host-Computer installieren, um die Software zu erstellen und sie dann auf Ihr IoT-Gerät zu übertragen. Weitere Informationen zum Installieren und Erstellen der Software für Ihr Gerät finden Sie in der Dokumentation für Ihre Gerätesoftware.

Verfahren in diesem Abschnitt:

- Aktualisieren Sie die Betriebssystemsoftware
- Installieren der erforderlichen Anwendungen und Bibliotheken
- (Optional) Speichern des microSD-Karten-Images

Aktualisieren Sie die Betriebssystemsoftware

Mit diesem Verfahren wird die Betriebssystemsoftware aktualisiert.

So aktualisieren Sie die Betriebssystemsoftware auf dem Raspberry Pi:

Führen Sie diese Schritte im Terminalfenster Ihres lokalen Host-Computers aus.

1. Geben Sie diese Befehle ein, um die Systemsoftware auf Ihrem Raspberry Pi zu aktualisieren.

   ```
   sudo apt-get -y update
   sudo apt-get -y upgrade
   sudo apt-get -y autoremove
   ```

2. Aktualisieren Sie die Gebietsschema- und Zeitzoneneinstellungen des Raspberry Pi (optional).

   Geben Sie diesen Befehl ein, um die Gebietsschema- und Zeitzoneneinstellungen des Geräts zu aktualisieren.

   ```
   sudo raspi-config
   ```

   a. So legen Sie das Gebietsschema des Geräts fest:

      i. Wählen Sie im Bildschirm Raspberry Pi Software Configuration Tool (raspi-config) Option 5.

         **5 Localisation Options Configure language and regional settings**

         Verwenden Sie die Tab-Taste, um <Select> zu bewegen, und drücken Sie dann die space bar.

      ii. Wählen Sie im Menü mit den Lokalisierungsoptionen die Option L1 aus.

         **L1 Locale Configure language and regional settings**

Verwenden Sie die Tab-Taste, um <Select> zu bewegen, und drücken Sie dann die space bar.

iii. Wählen Sie in der Liste der Gebietsschemaoptionen die Gebietsschemas aus, die Sie auf Ihrem Raspberry Pi installieren möchten, indem Sie mit den Pfeiltasten blättern und dann die gewünschten Gebietsschemas mit der space bar markieren.

In den Vereinigten Staaten ist **`en_US.UTF-8`** eine gute Wahl.

iv. Nachdem Sie die Gebietsschemas für Ihr Gerät ausgewählt haben, wählen Sie mit der Tab-Taste <OK>, und drücken Sie dann die space bar, um die Bestätigungsseite für die Konfiguration der Gebietsschemas aufzurufen.

b. So legen Sie die Zeitzone des Geräts fest:

i. Wählen Sie im Bildschirm raspi-config Option 5.

```
5 Localisation Options Configure language and regional settings
```

Verwenden Sie die Tab-Taste, um <Select> zu bewegen, und drücken Sie dann die space bar.

ii. Wählen Sie im Menü mit den Lokalisierungsoptionen mit der Pfeiltaste die Option L2 aus:

```
L2 time zone Configure time zone
```

Verwenden Sie die Tab-Taste, um <Select> zu bewegen, und drücken Sie dann die space bar.

iii. Wählen Sie im Menü Konfiguration von tzdata Ihr geografisches Gebiet aus der Liste aus.

Verwenden Sie die Tab-Taste, um zu <OK> zu gehen, und drücken Sie dann die space bar.

iv. Wählen Sie in der Liste der Städte mit den Pfeiltasten eine Stadt in Ihrer Zeitzone aus.

Um die Zeitzone festzulegen, verwenden Sie die Tab-Taste, um zu <OK> zu gehen, und drücken Sie dann die space bar.

c. Wenn Sie mit der Aktualisierung der Einstellungen fertig sind, wechseln Sie mit der Tab-Taste zu <Finish>, und drücken Sie dann auf space bar, um die App raspi-config zu schließen.

3. Geben Sie diesen Befehl ein, um Ihren Raspberry Pi neu zu starten.

```
sudo shutdown -r 0
```

4. Warten Sie, bis Ihr Raspberry Pi neu gestartet wird.
5. Nachdem Ihr Raspberry Pi neu gestartet wurde, verbinden Sie das Terminalfenster auf Ihrem lokalen Host-Computer erneut mit Ihrem Raspberry Pi.

Ihre Raspberry-Pi-Systemsoftware ist jetzt konfiguriert und Sie können mit the section called “Installieren Sie Anwendungen und Bibliotheken” fortfahren.

Installieren der erforderlichen Anwendungen und Bibliotheken

Mit diesem Verfahren werden die Anwendungssoftware und die Bibliotheken installiert, die in den nachfolgenden Tutorials verwendet werden.

Wenn Sie einen Raspberry Pi verwenden oder die erforderliche Software auf Ihrem IoT-Gerät kompilieren können, führen Sie diese Schritte im Terminalfenster auf Ihrem lokalen Host-Computer aus. Wenn Sie Software für Ihr IoT-Gerät auf Ihrem lokalen Host-Computer kompilieren müssen, lesen Sie in der Softwaredokumentation für Ihr IoT-Gerät nach, wie Sie diese Schritte auf Ihrem Gerät ausführen.

So installieren Sie die Anwendungssoftware und die Bibliotheken auf Ihrem Raspberry Pi:

1. Geben Sie diesen Befehl ein, um die Anwendungssoftware und die Bibliotheken zu installieren.

```
sudo apt-get -y install build-essential libssl-dev cmake unzip git python3-pip
```

2. Geben Sie diese Befehle ein, um zu bestätigen, dass die richtige Version der Software installiert wurde.

```
gcc --version
cmake --version
openssl version
git --version
```

3. Vergewissern Sie sich, dass diese Versionen der Anwendungssoftware installiert sind:

   - `gcc`: 9.3.0 oder höher
   - `cmake`: 3.10.x oder höher

- `OpenSSL`: 1.1.1 oder höher
- `git`: 2.20.1 oder höher

Wenn Ihr Raspberry Pi über akzeptable Versionen der erforderlichen Anwendungssoftware verfügt, können Sie mit the section called “(Optional) Speichern Sie das microSD-Bild” fortfahren.

(Optional) Speichern des microSD-Karten-Images

In den Tutorials in diesem Lernpfad werden Sie auf diese Verfahren stoßen, um eine Kopie des microSD-Karten-Images des Raspberry Pi in einer Datei auf Ihrem lokalen Host-Computer zu speichern. Sie werden zwar empfohlen, sind aber keine Pflichtaufgaben. Wenn Sie das microSD-Karten-Image an der empfohlenen Stelle speichern, können Sie die Verfahren überspringen, die dem Speichern in diesem Lernpfad vorausgehen. Dies kann Zeit sparen, wenn Sie etwas erneut versuchen müssen. Wenn Sie das microSD-Karten-Image nicht regelmäßig speichern, müssen Sie die Tutorials im Lernpfad möglicherweise von Anfang an neu beginnen, wenn Ihre microSD-Karte beschädigt ist oder wenn Sie versehentlich eine App oder deren Einstellungen falsch konfigurieren.

Die microSD-Karte Ihres Raspberry Pi verfügt jetzt über ein aktualisiertes Betriebssystem und die grundlegende Anwendungssoftware ist geladen. Sie können die Zeit sparen, die Sie für die Ausführung der vorherigen Schritte benötigen, indem Sie den Inhalt der microSD-Karte jetzt in einer Datei speichern. Wenn Sie das aktuelle Image des microSD-Karten-Images Ihres Geräts haben, können Sie von diesem Punkt aus beginnen, um ein Tutorial oder einen Vorgang fortzusetzen oder erneut zu versuchen, ohne die Software von Grund auf neu installieren und aktualisieren zu müssen.

So speichern Sie das Image der microSD-Karte in einer Datei:

1. Geben Sie diesen Befehl ein, um den Raspberry Pi herunterzufahren.

   ```
   sudo shutdown -h 0
   ```

2. Nachdem der Raspberry Pi vollständig heruntergefahren ist, trennen Sie ihn von der Stromversorgung.
3. Entfernen Sie die microSD-Karte aus dem Raspberry Pi.
4. Auf Ihrem lokalen Host-Computer:

   a. Legen Sie die microSD-Karte ein.
   b. Speichern Sie das Image der microSD-Karte mithilfe des Imaging-Tools für die SD-Karte in eine Datei.

c. Nachdem das Image der microSD-Karte gespeichert wurde, werfen Sie die Karte aus dem lokalen Host-Computer aus.

5. Trennen Sie den Raspberry Pi von der Stromversorgung und legen Sie die microSD-Karte in den Raspberry Pi ein.
6. Schließen Sie den Raspberry Pi an die Stromversorgung an.
7. Nachdem Sie etwa eine Minute gewartet haben, verbinden Sie erneut das Terminalfenster auf dem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden war, und melden Sie sich dann beim Raspberry Pi an.

## Testen Sie Ihr Gerät und speichern Sie das Amazon CA-Zertifikat

Die Verfahren in diesem Abschnitt sind die Fortsetzung des vorherigen Abschnitts zur Installation des Zertifikats AWS Command Line Interface und des Zertifikats der Zertifizierungsstelle, mit dem AWS IoT Core Ihre Verbindungen authentifiziert wurden.

Nachdem Sie diesen Abschnitt abgeschlossen haben, wissen Sie, dass Ihr Raspberry Pi über die erforderliche Systemsoftware für die Installation des AWS IoT Device Clients verfügt und dass er über eine funktionierende Verbindung zum Internet verfügt.

Erforderliche Ausstattung:

- Ihre lokale Entwicklungs- und Testumgebung aus dem vorherigen Abschnitt
- Der Raspberry Pi, den Sie im vorherigen Abschnitt verwendet haben
- Die microSD-Speicherkarte aus dem vorherigen Abschnitt

Verfahren in diesem Abschnitt:

- Installieren Sie das AWS Command Line Interface
- Konfigurieren Sie Ihre AWS-Konto Anmeldedaten
- Herunterladen des Amazon-Root-CA-Zertifikats
- (Optional) Speichern des microSD-Karten-Images

### Installieren Sie das AWS Command Line Interface

Dieses Verfahren installiert das AWS CLI auf Ihrem Raspberry Pi.

Wenn Sie einen Raspberry Pi verwenden oder Software auf Ihrem IoT-Gerät kompilieren können, führen Sie diese Schritte im Terminalfenster auf Ihrem lokalen Host-Computer aus. Wenn Sie Software für Ihr IoT-Gerät auf Ihrem lokalen Host-Computer kompilieren müssen, lesen Sie in der Softwaredokumentation für Ihr IoT-Gerät nach, welche Bibliotheken dafür erforderlich sind.

Um das AWS CLI auf Ihrem Raspberry Pi zu installieren

1. Führen Sie den folgenden Befehl aus, um die AWS CLI herunterzuladen und zu installieren.

```
export PATH=$PATH:~/.local/bin # configures the path to include the directory with
 the AWS CLI
git clone https://github.com/aws/aws-cli.git # download the AWS CLI code from
 GitHub
cd aws-cli && git checkout v2 # go to the directory with the repo and checkout
 version 2
pip3 install -r requirements.txt # install the prerequisite software
```

2. Führen Sie diesen Befehl aus, um den zu installieren AWS CLI. Die Ausführung dieses Befehls kann bis zu 15 Minuten dauern.

```
pip3 install . # install the AWS CLI
```

3. Führen Sie diesen Befehl aus, um zu bestätigen, dass die richtige Version von installiert AWS CLI wurde.

```
aws --version
```

   Die Version von AWS CLI sollte 2.2 oder höher sein.

Wenn die aktuelle Version AWS CLI angezeigt wird, können Sie fortfahrenthe section called “Konfigurieren Sie die Kontoanmeldeinformationen”.

Konfigurieren Sie Ihre AWS-Konto Anmeldedaten

In diesem Verfahren erhalten Sie AWS-Konto Anmeldeinformationen und fügen sie für die Verwendung auf Ihrem Raspberry Pi hinzu.

Um Ihre AWS-Konto Anmeldeinformationen zu Ihrem Gerät hinzuzufügen

1. Besorgen Sie sich von Ihrem eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel AWS-Konto , um sie AWS CLI auf Ihrem Gerät zu authentifizieren.

   Falls Sie noch nicht damit vertraut sind AWS IAM, beschreibt das https://aws.amazon.com/premiumsupport/Knowledge-center/create-access-key/den Prozess, der in der AWS Konsole ausgeführt werden muss, um AWS IAM Anmeldeinformationen für Ihr Gerät zu erstellen.
2. Gehen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, mit den Anmeldeinformationen Zugriffsschlüssel-ID und Geheimer Zugriffsschlüssel für Ihr Gerät folgendermaßen vor:

   a. Führen Sie die AWS Configure-App mit diesem Befehl aus:

   ```
   aws configure
   ```

   b. Geben Sie Ihre Anmeldeinformationen und Konfigurationsinformationen ein, wenn Sie dazu aufgefordert werden:

   ```
   AWS Access Key ID: your Access Key ID
   AWS Secret Access Key: your Secret Access Key
   Default region name: your AWS-Region code
   Default output format: json
   ```
3. Führen Sie diesen Befehl aus, um den Zugriff Ihres Geräts auf Ihren AWS IoT Core Endpunkt AWS-Konto zu testen.

   ```
   aws iot describe-endpoint --endpoint-type iot:Data-ATS
   ```

   Es sollte Ihren AWS-Konto-spezifischen AWS IoT Datenendpunkt zurückgeben, wie in diesem Beispiel:

   ```
   {
       "endpointAddress": "a3EXAMPLEffp-ats.iot.us-west-2.amazonaws.com"
   }
   ```

Wenn Sie Ihren AWS-Konto-spezifischen AWS IoT Datenendpunkt sehen, verfügt Ihr Raspberry Pi über die Konnektivität und die erforderlichen Berechtigungen, um damit fortzufahren. the section called “Herunterladen des Amazon-Root-CA-Zertifikats”

> **Important**
>
> Ihre AWS-Konto Anmeldeinformationen sind jetzt auf der microSD-Karte in Ihrem Raspberry Pi gespeichert. Dies erleichtert Ihnen und der Software, die Sie in diesen Tutorials erstellen, future Interaktionen, sie werden jedoch standardmäßig auch in allen microSD-Kartenbildern gespeichert und dupliziert, die Sie nach diesem Schritt erstellen. AWS
> Um die Sicherheit Ihrer AWS-Konto Anmeldeinformationen zu gewährleisten, sollten Sie vor dem Speichern weiterer microSD-Kartenbilder erwägen, die Anmeldeinformationen zu löschen, indem Sie `aws configure` erneut ausführen und zufällige Zeichen für die Access Key ID und den Secret Access Key eingeben, um zu verhindern, dass Ihre AWS-Konto Anmeldeinformationen kompromittiert werden.
> Wenn Sie feststellen, dass Sie Ihre AWS-Konto Anmeldeinformationen versehentlich gespeichert haben, können Sie sie in der Konsole deaktivieren. AWS IAM

### Herunterladen des Amazon-Root-CA-Zertifikats

Bei diesem Verfahren wird eine Kopie eines Zertifikats der Amazon Root Certificate Authority (CA) heruntergeladen und gespeichert. Durch das Herunterladen dieses Zertifikats wird es zur Verwendung in den nachfolgenden Tutorials gespeichert. Außerdem wird die Konnektivität Ihres Geräts mit AWS -Diensten getestet.

So laden Sie das Amazon-Root-CA-Zertifikat herunter und speichern es:

1. Führen Sie den folgenden Befehl aus, um ein Verzeichnis für das Zertifikat zu erstellen.

   ```
   mkdir ~/certs
   ```

2. Führen Sie diesen Befehl aus, um das Amazon-Root-CA-Zertifikat herunterzuladen.

   ```
   curl -o ~/certs/AmazonRootCA1.pem https://www.amazontrust.com/repository/
   AmazonRootCA1.pem
   ```

3. Führen Sie diese Befehle aus, um den Zugriff auf das Zertifikatsverzeichnis und die zugehörige Datei festzulegen.

```
chmod 745 ~
chmod 700 ~/certs
chmod 644 ~/certs/AmazonRootCA1.pem
```

4. Führen Sie diesen Befehl aus, um die CA-Zertifikatsdatei im neuen Verzeichnis anzuzeigen.

   ```
   ls -l ~/certs
   ```

   Sie sollten einen Eintrag wie diesen sehen. Das Datum und die Uhrzeit werden unterschiedlich sein. Die Dateigröße und alle anderen Informationen sollten jedoch mit den hier abgebildeten übereinstimmen.

   ```
   -rw-r--r-- 1 pi pi 1188 Oct 28 13:02 AmazonRootCA1.pem
   ```

   Wenn die Dateigröße nicht 1188 beträgt, überprüfen Sie die curl-Befehlsparameter. Möglicherweise haben Sie eine falsche Datei heruntergeladen.

(Optional) Speichern des microSD-Karten-Images

Die microSD-Karte Ihres Raspberry Pi verfügt jetzt über ein aktualisiertes Betriebssystem und die grundlegende Anwendungssoftware ist geladen.

So speichern Sie das Image der microSD-Karte in einer Datei:

1. Löschen Sie im Terminalfenster auf Ihrem lokalen Host-Computer Ihre AWS -Anmeldeinformationen.

   a. Führen Sie die AWS Configure-App mit diesem Befehl aus:

      ```
      aws configure
      ```

   b. Ersetzen Sie Ihre Anmeldeinformationen, wenn Sie dazu aufgefordert werden. Sie können den Standardregionsnamen und das Standardausgabeformat unverändert lassen, indem Sie die Eingabetaste drücken.

      ```
      AWS Access Key ID [****************YT2H]: XYXYXYXYX
      AWS Secret Access Key [****************9plH]: XYXYXYXYX
      Default region name [us-west-2]:
      ```

```
Default output format [json]:
```

2. Geben Sie diesen Befehl ein, um den Raspberry Pi herunterzufahren.

```
sudo shutdown -h 0
```

3. Nachdem der Raspberry Pi vollständig heruntergefahren ist, trennen Sie ihn von der Stromversorgung.
4. Entfernen Sie die microSD-Karte aus Ihrem Gerät.
5. Auf Ihrem lokalen Host-Computer:
   a. Legen Sie die microSD-Karte ein.
   b. Speichern Sie das Image der microSD-Karte mithilfe des Imaging-Tools für die SD-Karte in eine Datei.
   c. Nachdem das Image der microSD-Karte gespeichert wurde, werfen Sie die Karte aus dem lokalen Host-Computer aus.
6. Trennen Sie den Raspberry Pi von der Stromversorgung und legen Sie die microSD-Karte in den Raspberry Pi ein.
7. Schließen Sie das Gerät an die Stromversorgung an.
8. Starten Sie nach etwa einer Minute auf dem lokalen Host-Computer die Terminalfenstersitzung neu und melden Sie sich beim Gerät an.

   Geben Sie Ihre AWS-Konto Anmeldeinformationen noch nicht erneut ein.

Nachdem Sie Ihren Raspberry Pi neu gestartet und sich angemeldet haben, können Sie mit the section called “Installation und Konfiguration des IoT-Geräteclients” fortfahren.

## Tutorials: Installieren und Konfigurieren des AWS IoT Device Clients

Dieses Tutorial führt Sie durch die Installation und Konfiguration des AWS IoT Geräteclients und die Erstellung von AWS IoT Ressourcen, die Sie in dieser und anderen Demos verwenden werden.

So beginnen Sie dieses Tutorial:

- Halten Sie Ihren lokalen Host-Computer und den Raspberry Pi aus dem vorherigen Tutorial bereit.

Dieses Tutorial kann bis zu 90 Minuten dauern.

Wenn Sie mit diesem Thema fertig sind:

- Ihr IoT-Gerät kann in anderen AWS IoT Device Client-Demos verwendet werden.
- Sie haben Ihr IoT-Gerät in AWS IoT Core bereitgestellt.
- Sie haben den AWS IoT Geräteclient heruntergeladen und auf Ihrem Gerät installiert.
- Sie haben ein Image der microSD-Karte Ihres Geräts gespeichert, das in nachfolgenden Tutorials verwendet werden kann.

Erforderliche Ausstattung:

- Ihre lokale Entwicklungs- und Testumgebung aus dem vorherigen Abschnitt
- Der Raspberry Pi, den Sie im vorherigen Abschnitt verwendet haben
- Die microSD-Speicherkarte des Raspberry Pi, die Sie im vorherigen Abschnitt verwendet haben

Verfahren in diesem Tutorial

- Laden Sie den AWS IoT Geräteclient herunter und speichern Sie ihn
- Stellen Sie Ihren Raspberry Pi bereit in AWS IoT
- Konfigurieren Sie den AWS IoT Geräteclient, um die Konnektivität zu testen

## Laden Sie den AWS IoT Geräteclient herunter und speichern Sie ihn

Mit den Verfahren in diesem Abschnitt wird der AWS IoT Device Client heruntergeladen, kompiliert und auf Ihrem Raspberry Pi installiert. Nachdem Sie die Installation getestet haben, können Sie das Image der microSD-Karte des Raspberry Pi speichern, um es später zu verwenden, wenn Sie die Tutorials erneut ausprobieren möchten.

Verfahren in diesem Abschnitt:

- Herunterladen und Erstellen des AWS IoT Device Clients
- Erstellen der in den Tutorials verwendeten Verzeichnisse
- (Optional) Speichern des microSD-Karten-Images

Herunterladen und Erstellen des AWS IoT Device Clients

Mit diesem Verfahren wird der AWS IoT Device Client auf Ihrem Raspberry Pi installiert.

Führen Sie diese Befehle im Terminalfenster auf Ihrem lokalen Host-Computer aus, der mit Ihrem Raspberry Pi verbunden ist.

Um den AWS IoT Device Client auf Ihrem Raspberry Pi zu installieren

1. Geben Sie diese Befehle ein, um den AWS IoT Geräteclient herunterzuladen und auf Ihrem Raspberry Pi zu erstellen.

   ```
   cd ~
   git clone https://github.com/awslabs/aws-iot-device-client aws-iot-device-client
   mkdir ~/aws-iot-device-client/build && cd ~/aws-iot-device-client/build
   cmake ../
   ```

2. Führen Sie diesen Befehl aus, um den AWS IoT Geräteclient zu erstellen. Die Ausführung dieses Befehls kann bis zu 15 Minuten dauern.

   ```
   cmake --build . --target aws-iot-device-client
   ```

   Die Warnmeldungen, die beim Kompilieren des AWS IoT Geräteclients angezeigt werden, können ignoriert werden.

   Diese Tutorials wurden mit dem AWS IoT Device Client getestetgcc, auf dem der Device Client basiert, Version (Raspbian 10.2.1-6+rpi1) 10.2.1 20210110 auf der Version von Raspberry Pi OS (bullseye) auf, Version (Raspbian 8.3.0-6+rpi1) 8.3.0 auf gcc der Version des Raspberry Pi OS (Buster) vom 7. Mai 2021.

3. Nachdem AWS IoT der Geräteclient fertig gebaut wurde, testen Sie ihn, indem Sie diesen Befehl ausführen.

   ```
   ./aws-iot-device-client --help
   ```

Wenn Sie die Befehlszeilenhilfe für den AWS IoT Geräteclient sehen, wurde der AWS IoT Geräteclient erfolgreich erstellt und kann von Ihnen verwendet werden.

Erstellen der in den Tutorials verwendeten Verzeichnisse

Mit diesem Verfahren werden die Verzeichnisse auf dem Raspberry Pi erstellt, in denen die in den Tutorials in diesem Lernpfad verwendeten Dateien gespeichert werden.

So erstellen Sie die in den Tutorials in diesem Lernpfad verwendeten Verzeichnisse:

1. Führen Sie diese Befehle aus, um die erforderlichen Verzeichnisse zu erstellen.

```
mkdir ~/dc-configs
mkdir ~/policies
mkdir ~/messages
mkdir ~/certs/testconn
mkdir ~/certs/pubsub
mkdir ~/certs/jobs
```

2. Führen Sie diese Befehle aus, um die Berechtigungen für die neuen Verzeichnisse festzulegen.

```
chmod 745 ~
chmod 700 ~/certs/testconn
chmod 700 ~/certs/pubsub
chmod 700 ~/certs/jobs
```

Nachdem Sie diese Verzeichnisse erstellt und ihre Berechtigungen festgelegt haben, fahren Sie fort mit the section called “(Optional) Speichern des microSD-Karten-Images”.

(Optional) Speichern des microSD-Karten-Images

Zu diesem Zeitpunkt verfügt die microSD-Karte Ihres Raspberry Pi über ein aktualisiertes Betriebssystem, die grundlegende Anwendungssoftware und den AWS IoT Geräteclient.

Wenn Sie diese Übungen und Tutorials erneut ausprobieren möchten, können Sie die vorherigen Verfahren überspringen, indem Sie das mit diesem Verfahren gespeicherte microSD-Karten-Image auf eine neue microSD-Karte schreiben und mit den Tutorials ab the section called “Stellen Sie Ihren Raspberry Pi bereit” fortfahren.

So speichern Sie das Image der microSD-Karte in einer Datei:

Gehen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, folgendermaßen vor:

1. Vergewissern Sie sich, dass Ihre AWS-Konto Anmeldeinformationen nicht gespeichert wurden.

   a. Führen AWS Sie die Configure-App mit diesem Befehl aus:

```
aws configure
```

b. Wenn Ihre Anmeldeinformationen gespeichert wurden (also in der Eingabeaufforderung angezeigt werden), geben Sie die Zeichenfolge **XYXYXYXYX** ein, wenn Sie dazu aufgefordert werden, wie hier gezeigt. Lassen Sie den Namen der Standardregion und das Standardausgabeformat leer.

```
AWS Access Key ID [****************YXYX]: XYXYXYXYX
AWS Secret Access Key [****************YXYX]: XYXYXYXYX
Default region name:
Default output format:
```

2. Geben Sie diesen Befehl ein, um den Raspberry Pi herunterzufahren.

```
sudo shutdown -h 0
```

3. Nachdem der Raspberry Pi vollständig heruntergefahren ist, trennen Sie ihn von der Stromversorgung.
4. Entfernen Sie die microSD-Karte aus Ihrem Gerät.
5. Auf Ihrem lokalen Host-Computer:

   a. Legen Sie die microSD-Karte ein.
   b. Speichern Sie das Image der microSD-Karte mithilfe des Imaging-Tools für die SD-Karte in eine Datei.
   c. Nachdem das Image der microSD-Karte gespeichert wurde, werfen Sie die Karte aus dem lokalen Host-Computer aus.

Sie können mit dieser microSD-Karte in the section called “Stellen Sie Ihren Raspberry Pi bereit” fortfahren.

## Stellen Sie Ihren Raspberry Pi bereit in AWS IoT

Die Verfahren in diesem Abschnitt beginnen mit dem gespeicherten microSD-Image, auf dem der AWS IoT Geräteclient installiert ist, AWS CLI und erstellen die AWS IoT Ressourcen und Gerätezertifikate, in AWS IoT denen Ihr Raspberry Pi bereitgestellt wird.

Installieren der microSD-Karte in Ihrem Raspberry Pi

Dieses Verfahren installiert die microSD-Karte mit der erforderlichen Software, die auf den Raspberry Pi geladen und konfiguriert ist, und konfiguriert Ihre, AWS-Konto sodass Sie mit den Tutorials in diesem Lernpfad fortfahren können.

Verwenden Sie eine microSD-Karte aus the section called “(Optional) Speichern des microSD-Karten-Images” mit der erforderlichen Software für die Übungen und Tutorials in diesem Lernpfad.

So installieren Sie die microSD-Karte in Ihrem Raspberry Pi:

1. Trennen Sie den Raspberry Pi von der Stromversorgung und legen Sie die microSD-Karte in den Raspberry Pi ein.
2. Schließen Sie den Raspberry Pi an die Stromversorgung an.
3. Starten Sie nach etwa einer Minute auf dem lokalen Host-Computer die Terminalfenstersitzung neu und melden Sie sich beim Raspberry Pi an.
4. Auf Ihrem lokalen Host-Computer, im Terminalfenster und mit den Anmeldeinformationen Zugriffsschlüssel-ID und Geheimer Zugriffsschlüssel für Ihren Raspberry Pi:

   a. Führen Sie die AWS Configure-App mit diesem Befehl aus:

   ```
   aws configure
   ```

   b. Geben Sie Ihre AWS-Konto Anmeldeinformationen und Konfigurationsinformationen ein, wenn Sie dazu aufgefordert werden:

   ```
   AWS Access Key ID [****************YXYX]: your Access Key ID
   AWS Secret Access Key [****************YXYX]: your Secret Access Key
   Default region name [us-west-2]: your AWS-Region code
   Default output format [json]: json
   ```

Nachdem Sie Ihre AWS-Konto Anmeldeinformationen wiederhergestellt haben, können Sie fortfahrenthe section called “Stellen Sie Ihr Gerät bereit in AWS IoT Core”.

Stellen Sie Ihr Gerät bereit in AWS IoT Core

Mit den Verfahren in diesem Abschnitt werden die AWS IoT Ressourcen erstellt, in denen Ihr Raspberry Pi bereitgestellt wird AWS IoT. Bei der Erstellung dieser Ressourcen werden Sie aufgefordert, verschiedene Informationen aufzuzeichnen. Diese Informationen werden von der AWS IoT Geräteclient-Konfiguration im nächsten Verfahren verwendet.

Damit Ihr Raspberry Pi verwendet werden kann AWS IoT, muss er bereitgestellt werden. Bei der Bereitstellung werden die AWS IoT Ressourcen erstellt und konfiguriert, die zur Unterstützung Ihres Raspberry Pi als IoT-Gerät erforderlich sind.

Wenn Ihr Raspberry Pi eingeschaltet ist und neu gestartet wird, verbinden Sie das Terminalfenster auf Ihrem lokalen Host-Computer mit dem Raspberry Pi und führen Sie diese Verfahren durch.

Verfahren in diesem Abschnitt:

- Erstellen und Herunterladen der Gerätezertifikatsdateien
- Ressourcen erstellen AWS IoT

Erstellen und Herunterladen der Gerätezertifikatsdateien

Mit diesem Verfahren werden die Gerätezertifikatsdateien für diese Demo erstellt.

So erstellen Sie die Gerätezertifikatsdateien für Ihren Raspberry Pi und laden sie herunter:

1. Geben Sie im Terminalfenster auf Ihrem lokalen Host-Computer diese Befehle ein, um die Gerätezertifikatsdateien für Ihr Gerät zu erstellen.

   ```
   mkdir ~/certs/testconn
   aws iot create-keys-and-certificate \
   --set-as-active \
   --certificate-pem-outfile "~/certs/testconn/device.pem.crt" \
   --public-key-outfile "~/certs/testconn/public.pem.key" \
   --private-key-outfile "~/certs/testconn/private.pem.key"
   ```

   Die Ausgabe des Befehls ähnelt der folgenden: Notieren Sie sich den *certificateArn*-Wert zur späteren Verwendung.

   ```
   {
       "certificateArn": "arn:aws:iot:us-
   west-2:57EXAMPLE833:cert/76e7e4edb3e52f52334be2f387a06145b2aa4c7fcd810f3aea2d92abc227d269",
       "certificateId":
    "76e7e4edb3e52f5233EXAMPLE7a06145b2aa4c7fcd810f3aea2d92abc227d269",
       "certificatePem": "-----BEGIN CERTIFICATE-----
   \nMIIDWTCCAkGgAwIBAgI_SHORTENED_FOR_EXAMPLE_Lgn4jfgtS\n-----END CERTIFICATE-----
   \n",
       "keyPair": {
           "PublicKey": "-----BEGIN PUBLIC KEY-----
   \nMIIBIjANBgkqhkiG9w0BA_SHORTENED_FOR_EXAMPLE_ImwIDAQAB\n-----END PUBLIC KEY-----
   \n",
           "PrivateKey": "-----BEGIN RSA PRIVATE KEY-----
   \nMIIEowIBAAKCAQE_SHORTENED_FOR_EXAMPLE_T9RoDiukY\n-----END RSA PRIVATE KEY-----\n"
       }
   ```

```
}
```

2. Geben Sie die folgenden Befehle ein, um die Berechtigungen für das Zertifikatsverzeichnis und seine Dateien festzulegen.

```
chmod 745 ~
chmod 700 ~/certs/testconn
chmod 644 ~/certs/testconn/*
chmod 600 ~/certs/testconn/private.pem.key
```

3. Führen Sie diesen Befehl aus, um die Berechtigungen für Ihre Zertifikatsverzeichnisse und -dateien zu überprüfen.

```
ls -l ~/certs/testconn
```

   Der Befehl sollte ähnliche Werte wie die hier angezeigten ausgeben, mit der Ausnahme, dass Datum und Uhrzeit unterschiedlich sein werden.

```
-rw-r--r-- 1 pi pi 1220 Oct 28 13:02 device.pem.crt
-rw------- 1 pi pi 1675 Oct 28 13:02 private.pem.key
-rw-r--r-- 1 pi pi  451 Oct 28 13:02 public.pem.key
```

Sie haben die Gerätezertifikatsdateien bereits auf Ihrem Raspberry Pi installiert und können mit the section called “Ressourcen erstellen AWS IoT” fortfahren.

Ressourcen erstellen AWS IoT

Bei diesem Verfahren wird Ihr Gerät bereitgestellt, AWS IoT indem die Ressourcen erstellt werden, die Ihr Gerät für den Zugriff auf AWS IoT Funktionen und Dienste benötigt.

Um Ihr Gerät bereitzustellen in AWS IoT

1. Geben Sie im Terminalfenster auf Ihrem lokalen Host-Computer den folgenden Befehl ein, um die Adresse des Gerätedatenendpunkts für Ihr AWS-Konto abzurufen.

```
aws iot describe-endpoint --endpoint-type IoT:Data-ATS
```

   Der Befehl aus den vorhergehenden Schritten gibt eine Antwort aus, die der folgenden ähnelt: Notieren Sie sich den *endpointAddress*-Wert zur späteren Verwendung.

```
{
    "endpointAddress": "a3qjEXAMPLEffp-ats.iot.us-west-2.amazonaws.com"
}
```

2. Geben Sie diesen Befehl ein, um eine AWS IoT Ding-Ressource für Ihren Raspberry Pi zu erstellen.

```
aws iot create-thing --thing-name "DevCliTestThing"
```

Wenn Ihre AWS IoT Ding-Ressource erstellt wurde, gibt der Befehl eine Antwort wie diese zurück.

```
{
    "thingName": "DevCliTestThing",
    "thingArn": "arn:aws:iot:us-west-2:57EXAMPLE833:thing/DevCliTestThing",
    "thingId": "8ea78707-32c3-4f8a-9232-14bEXAMPLEfd"
}
```

3. Im Terminalfenster:

   a. Öffnen Sie einen Texteditor, z. B. `nano`.

   b. Kopieren Sie dieses JSON Richtliniendokument und fügen Sie es in Ihren geöffneten Texteditor ein.

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

```
}
```

> **Note**
>
> Dieses Richtliniendokument gewährt allen Ressourcen großzügig die Erlaubnis, Verbindungen herzustellen, zu empfangen, zu veröffentlichen und zu abonnieren. Normalerweise gewähren Richtlinien nur bestimmten Ressourcen die Erlaubnis, bestimmte Aktionen auszuführen. Beim ersten Test der Gerätekonnektivität wird diese zu allgemeine und großzügige Richtlinie jedoch verwendet, um die Wahrscheinlichkeit eines Zugriffsproblems während dieses Tests zu minimieren. In den nachfolgenden Tutorials werden enger abgegrenzte Richtliniendokumente verwendet, um bessere Verfahren für die Richtliniengestaltung zu demonstrieren.

c. Speichern Sie die Datei als **~/policies/dev_cli_test_thing_policy.json** in Ihrem Texteditor.

4. Führen Sie diesen Befehl aus, um das Richtliniendokument aus den vorherigen Schritten zum Erstellen einer AWS IoT Richtlinie zu verwenden.

```
aws iot create-policy \
--policy-name "DevCliTestThingPolicy" \
--policy-document "file://~/policies/dev_cli_test_thing_policy.json"
```

Wenn die Richtlinie erstellt wurde, gibt der Befehl eine Antwort wie die folgende zurück:

```
{
    "policyName": "DevCliTestThingPolicy",
    "policyArn": "arn:aws:iot:us-west-2:57EXAMPLE833:policy/DevCliTestThingPolicy",
    "policyDocument": "{\n    \"Version\": \"2012-10-17\",\n    \"Statement\": [\n
        {\n            \"Effect\": \"Allow\",\n            \"Action\": [\n
           \"iot:Publish\",\n                \"iot:Subscribe\",\n
 \"iot:Receive\",\n                \"iot:Connect\"\n            ],\n
 \"Resource\": [\n                \"*\"\n            ]\n        }\n    ]\n}\n",
    "policyVersionId": "1"
}
```

5. Führen Sie diesen Befehl aus, um die Richtlinie an das Gerätezertifikat anzufügen. Ersetzen Sie *certificateArn* durch den `certificateArn`-Wert, den Sie zuvor gespeichert haben.

```
aws iot attach-policy \
```

```
--policy-name "DevCliTestThingPolicy" \
--target "certificateArn"
```

Bei erfolgreicher Ausführung gibt dieser Befehl nichts zurück.

6. Führen Sie diesen Befehl aus, um das Gerätezertifikat an die AWS IoT Ding-Ressource anzuhängen. Ersetzen Sie *certificateArn* durch den `certificateArn`-Wert, den Sie zuvor gespeichert haben.

```
aws iot attach-thing-principal \
--thing-name "DevCliTestThing" \
--principal "certificateArn"
```

Bei erfolgreicher Ausführung gibt dieser Befehl nichts zurück.

Nachdem Sie Ihr Gerät erfolgreich bereitgestellt haben AWS IoT, können Sie damit fortfahrenthe section called “Konfigurieren Sie den Geräteclient und testen Sie die Konnektivität”.

## Konfigurieren Sie den AWS IoT Geräteclient, um die Konnektivität zu testen

Mit den Verfahren in diesem Abschnitt wird der AWS IoT Device Client so konfiguriert, dass er eine MQTT Nachricht von Ihrem Raspberry Pi veröffentlicht.

Verfahren in diesem Abschnitt:

- Erstellen der Konfigurationsdatei
- Öffnen Sie MQTT den Testclient
- Führen Sie den AWS IoT Geräteclient aus

### Erstellen der Konfigurationsdatei

Dieses Verfahren erstellt die Konfigurationsdatei zum Testen des AWS IoT Geräteclients.

Um die Konfigurationsdatei zum Testen des AWS IoT Geräteclients zu erstellen

- Gehen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, folgendermaßen vor:

  a. Geben Sie diese Befehle ein, um ein Verzeichnis für die Konfigurationsdateien zu erstellen und die Berechtigungen für das Verzeichnis festzulegen:

```
mkdir ~/dc-configs
chmod 745 ~/dc-configs
```

b. Öffnen Sie einen Texteditor, z. B. nano.

c. Kopieren Sie dieses JSON Dokument und fügen Sie es in Ihren geöffneten Texteditor ein.

```
{
  "endpoint": "a3qEXAMPLEaffp-ats.iot.us-west-2.amazonaws.com",
  "cert": "~/certs/testconn/device.pem.crt",
  "key": "~/certs/testconn/private.pem.key",
  "root-ca": "~/certs/AmazonRootCA1.pem",
  "thing-name": "DevCliTestThing",
  "logging": {
    "enable-sdk-logging": true,
    "level": "DEBUG",
    "type": "STDOUT",
    "file": ""
  },
  "jobs": {
    "enabled": false,
    "handler-directory": ""
  },
  "tunneling": {
    "enabled": false
  },
  "device-defender": {
    "enabled": false,
    "interval": 300
  },
  "fleet-provisioning": {
    "enabled": false,
    "template-name": "",
    "template-parameters": "",
    "csr-file": "",
    "device-key": ""
  },
  "samples": {
    "pub-sub": {
      "enabled": true,
      "publish-topic": "test/dc/pubtopic",
      "publish-file": "",
      "subscribe-topic": "test/dc/subtopic",
```

```
      "subscribe-file": ""
    }
  },
  "config-shadow": {
    "enabled": false
  },
  "sample-shadow": {
    "enabled": false,
    "shadow-name": "",
    "shadow-input-file": "",
    "shadow-output-file": ""
  }
}
```

d. Ersetzen Sie das *endpoint* Wert durch den Endpunkt der Gerätedaten für Ihren AWS-Konto , den Sie in gefunden habenthe section called “Stellen Sie Ihr Gerät bereit in AWS IoT Core”.

e. Speichern Sie die Datei als **~/dc-configs/dc-testconn-config.json** in Ihrem Texteditor.

f. Führen Sie diesen Befehl aus, um die Berechtigungen für die neue Konfigurationsdatei festzulegen.

```
chmod 644 ~/dc-configs/dc-testconn-config.json
```

Nachdem Sie die Datei gespeichert haben, können Sie mit the section called “Öffnen Sie MQTT den Testclient” fortfahren.

Öffnen Sie MQTT den Testclient

Dieses Verfahren bereitet den MQTTTestclient in der AWS IoT Konsole darauf vor, die MQTT Nachricht zu abonnieren, die der AWS IoT Geräteclient veröffentlicht, wenn er ausgeführt wird.

Um den MQTTTestclient darauf vorzubereiten, alle MQTT Nachrichten zu abonnieren

1. Wählen Sie auf Ihrem lokalen Host-Computer in der AWS IoT Konsole MQTT Testclient aus.
2. Geben Sie auf der Registerkarte Thema abonnieren im Themenfilter **#** (ein einzelnes Rautenzeichen) ein und wählen Sie Abonnieren aus, um jedes MQTT Thema zu abonnieren.
3. Vergewissern Sie sich, dass Sie unter der Bezeichnung Abonnements **#** (ein einzelnes Pfundzeichen) sehen.

Lassen Sie das Fenster mit dem MQTTTestclient geöffnet, während Sie fortfahrenthe section called “Führen Sie den AWS IoT Geräteclient aus”.

Führen Sie den AWS IoT Geräteclient aus

Bei diesem Verfahren wird der AWS IoT Geräteclient so ausgeführt, dass er eine einzelne MQTT Nachricht veröffentlicht, die der MQTTTestclient empfängt und anzeigt.

Um eine MQTT Nachricht vom AWS IoT Geräteclient aus zu senden

1. Stellen Sie sicher, dass sowohl das Terminalfenster, das mit Ihrem Raspberry Pi verbunden ist, als auch das Fenster mit dem MQTTTestclient sichtbar sind, während Sie dieses Verfahren ausführen.
2. Geben Sie im Terminalfenster diese Befehle ein, um den AWS IoT Geräteclient mithilfe der in erstellten Konfigurationsdatei auszuführenthe section called “Erstellen der Konfigurationsdatei”.

   ```
   cd ~/aws-iot-device-client/build
   ./aws-iot-device-client --config-file ~/dc-configs/dc-testconn-config.json
   ```

   Im Terminalfenster zeigt der AWS IoT Geräteclient Informationsmeldungen und alle Fehler an, die bei der Ausführung auftreten.

   Wenn im Terminalfenster keine Fehler angezeigt werden, überprüfen Sie den MQTTTestclient.
3. Im MQTTTestclient finden Sie im Abonnementfenster Hello World! Nachricht wurde an das `test/dc/pubtopic` Nachrichtenthema gesendet.
4. Wenn der AWS IoT Geräteclient keine Fehler anzeigt und Sie Hello World! sehen an die `test/dc/pubtopic` Nachricht im MQTTTestclient gesendet, haben Sie eine erfolgreiche Verbindung nachgewiesen.
5. Geben Sie im Terminalfenster **^C** (Strg-C) ein, um den AWS IoT Geräteclient zu beenden.

Nachdem Sie nachgewiesen haben, dass der AWS IoT Device Client auf Ihrem Raspberry Pi korrekt läuft und mit ihm kommunizieren kann AWS IoT, können Sie mit dem fortfahren. the section called “Kommunizieren Sie mit dem Geräteclient über MQTT”

# Tutorial: Demonstrieren MQTT Sie die Nachrichtenkommunikation mit dem AWS IoT Device Client

Dieses Tutorial zeigt, wie der AWS IoT Device Client MQTT Nachrichten abonnieren und veröffentlichen kann, die häufig in IoT-Lösungen verwendet werden.

So beginnen Sie dieses Tutorial:

- Sie haben Ihren lokalen Host-Computer und den Raspberry Pi so konfiguriert, wie im vorherigen Abschnitt zu sehen.

  Wenn Sie das microSD-Karten-Image nach der Installation des AWS IoT Device Clients gespeichert haben, können Sie eine microSD-Karte mit diesem Image mit Ihrem Raspberry Pi verwenden.
- Wenn Sie diese Demo schon einmal ausgeführt haben, überprüfen ??? Sie, ob Sie alle AWS IoT Ressourcen löschen sollten, die Sie in früheren Läufen erstellt haben, um doppelte Ressourcenfehler zu vermeiden.

Für dieses Tutorial brauchen Sie ungefähr 45 Minuten.

Wenn Sie mit diesem Thema fertig sind:

- Sie haben verschiedene Möglichkeiten demonstriert, wie Ihr IoT-Gerät MQTT Nachrichten von abonnieren AWS IoT und MQTT Nachrichten an sie veröffentlichen kann AWS IoT.

Erforderliche Ausstattung:

- Ihre lokale Entwicklungs- und Testumgebung aus dem vorherigen Abschnitt
- Der Raspberry Pi, den Sie im vorherigen Abschnitt verwendet haben
- Die microSD-Speicherkarte des Raspberry Pi, die Sie im vorherigen Abschnitt verwendet haben

Verfahren in diesem Tutorial

- Bereiten Sie den Raspberry Pi vor, um die MQTT Nachrichtenkommunikation zu demonstrieren
- Demonstrieren Sie das Veröffentlichen von Nachrichten mit dem AWS IoT Device Client
- Demonstrieren Sie das Abonnieren von Nachrichten mit dem Device Client AWS IoT

## Bereiten Sie den Raspberry Pi vor, um die MQTT Nachrichtenkommunikation zu demonstrieren

Mit diesem Verfahren werden die Ressourcen im AWS IoT und im Raspberry Pi erstellt, um die MQTT Nachrichtenkommunikation mithilfe des AWS IoT Geräteclients zu demonstrieren.

Verfahren in diesem Abschnitt:

- Erstellen Sie die Zertifikatsdateien, um die MQTT Kommunikation zu demonstrieren
- Stellen Sie Ihr Gerät bereit, um die MQTT Kommunikation zu demonstrieren
- Konfigurieren Sie die AWS IoT Device Client-Konfigurationsdatei und MQTT testen Sie den Client, um die MQTT Kommunikation zu demonstrieren

### Erstellen Sie die Zertifikatsdateien, um die MQTT Kommunikation zu demonstrieren

Mit diesem Verfahren werden die Gerätezertifikatsdateien für diese Demo erstellt.

So erstellen Sie die Gerätezertifikatsdateien für Ihren Raspberry Pi und laden sie herunter:

1. Geben Sie im Terminalfenster auf Ihrem lokalen Host-Computer den folgenden Befehl ein, um die Gerätezertifikatsdateien für Ihr Gerät zu erstellen.

   ```
   mkdir ~/certs/pubsub
   aws iot create-keys-and-certificate \
   --set-as-active \
   --certificate-pem-outfile "~/certs/pubsub/device.pem.crt" \
   --public-key-outfile "~/certs/pubsub/public.pem.key" \
   --private-key-outfile "~/certs/pubsub/private.pem.key"
   ```

   Die Ausgabe des Befehls ähnelt der folgenden: Speichern Sie den *certificateArn*-Wert zur späteren Verwendung.

   ```
   {
   "certificateArn": "arn:aws:iot:us-
   west-2:57EXAMPLE833:cert/76e7e4edb3e52f52334be2f387a06145b2aa4c7fcd810f3aea2d92abc227d269",
   "certificateId":
    "76e7e4edb3e52f5233EXAMPLE7a06145b2aa4c7fcd810f3aea2d92abc227d269",
   "certificatePem": "-----BEGIN CERTIFICATE-----
   \nMIIDWTCCAkGgAwIBAgI_SHORTENED_FOR_EXAMPLE_Lgn4jfgtS\n-----END CERTIFICATE-----
   \n",
   ```

```
"keyPair": {
    "PublicKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BA_SHORTENED_FOR_EXAMPLE_ImwIDAQAB\n-----END PUBLIC KEY-----
\n",
    "PrivateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQE_SHORTENED_FOR_EXAMPLE_T9RoDiukY\n-----END RSA PRIVATE KEY-----\n"
}
}
```

2. Geben Sie die folgenden Befehle ein, um die Berechtigungen für das Zertifikatsverzeichnis und seine Dateien festzulegen.

```
chmod 700 ~/certs/pubsub
chmod 644 ~/certs/pubsub/*
chmod 600 ~/certs/pubsub/private.pem.key
```

3. Führen Sie diesen Befehl aus, um die Berechtigungen für Ihre Zertifikatsverzeichnisse und -dateien zu überprüfen.

```
ls -l ~/certs/pubsub
```

   Der Befehl sollte ähnliche Werte wie die hier angezeigten ausgeben, mit der Ausnahme, dass Datum und Uhrzeit unterschiedlich sein werden.

```
-rw-r--r-- 1 pi pi 1220 Oct 28 13:02 device.pem.crt
-rw------- 1 pi pi 1675 Oct 28 13:02 private.pem.key
-rw-r--r-- 1 pi pi  451 Oct 28 13:02 public.pem.key
```

4. Geben Sie diese Befehle ein, um die Verzeichnisse für die Protokolldateien zu erstellen.

```
mkdir ~/.aws-iot-device-client
mkdir ~/.aws-iot-device-client/log
chmod 745 ~/.aws-iot-device-client/log
echo " " > ~/.aws-iot-device-client/log/aws-iot-device-client.log
echo " " > ~/.aws-iot-device-client/log/pubsub_rx_msgs.log
chmod 600 ~/.aws-iot-device-client/log/*
```

Stellen Sie Ihr Gerät bereit, um die MQTT Kommunikation zu demonstrieren

In diesem Abschnitt werden die AWS IoT Ressourcen erstellt, in denen Ihr Raspberry Pi bereitgestellt wird AWS IoT.

So stellen Sie Ihr Gerät in AWS IoT bereit:

1. Geben Sie im Terminalfenster auf Ihrem lokalen Host-Computer den folgenden Befehl ein, um die Adresse des Gerätedatenendpunkts für Ihr AWS-Konto abzurufen.

   ```
   aws iot describe-endpoint --endpoint-type IoT:Data-ATS
   ```

   Der Endpunktwert hat sich seit der letzten Ausführung dieses Befehls im vorhergehenden Tutorial nicht geändert. Wenn Sie den Befehl hier erneut ausführen, können Sie den Datenendpunktwert leicht finden und in die in diesem Tutorial verwendete Konfigurationsdatei einfügen.

   Der Befehl aus den vorhergehenden Schritten gibt eine Antwort aus, die der folgenden ähnelt: Notieren Sie sich den *endpointAddress*-Wert zur späteren Verwendung.

   ```
   {
   "endpointAddress": "a3qjEXAMPLEffp-ats.iot.us-west-2.amazonaws.com"
   }
   ```

2. Geben Sie diesen Befehl ein, um eine neue Ding-Ressource AWS IoT für Ihren Raspberry Pi zu erstellen.

   ```
   aws iot create-thing --thing-name "PubSubTestThing"
   ```

   Da AWS IoT es sich bei einer Ding-Ressource um eine virtuelle Darstellung Ihres Geräts in der Cloud handelt, können wir mehrere Ding-Ressourcen erstellen, AWS IoT um sie für verschiedene Zwecke zu verwenden. Sie können alle von demselben physischen IoT-Gerät verwendet werden, um verschiedene Aspekte des Geräts darzustellen.

   In diesen Tutorials wird jeweils nur eine Objektressource verwendet, um den Raspberry Pi darzustellen. Auf diese Weise stellen sie in diesen Tutorials die verschiedenen Demos dar, sodass Sie, nachdem Sie die AWS IoT Ressourcen für eine Demo erstellt haben, zurückgehen und die Demo mit den Ressourcen wiederholen können, die Sie jeweils speziell erstellt haben.

Wenn Ihre AWS IoT Ding-Ressource erstellt wurde, gibt der Befehl eine Antwort wie diese zurück.

```
{
"thingName": "PubSubTestThing",
"thingArn": "arn:aws:iot:us-west-2:57EXAMPLE833:thing/PubSubTestThing",
"thingId": "8ea78707-32c3-4f8a-9232-14bEXAMPLEfd"
}
```

3. Im Terminalfenster:

   a. Öffnen Sie einen Texteditor, z. B. nano.

   b. Kopieren Sie dieses JSON Dokument und fügen Sie es in Ihren geöffneten Texteditor ein.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Connect"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:client/PubSubTestThing"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/pubtopic"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topicfilter/test/dc/subtopic"
```

```
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/subtopic"
      ]
    }
  ]
}
```

c. Ersetzen Sie im Editor in jedem `Resource` Abschnitt des Richtliniendokuments *us-west-2:57EXAMPLE833* mit Ihrem AWS-Region, einem Doppelpunkt (:) und Ihrer 12-stelligen AWS-Konto Zahl.

d. Speichern Sie die Datei als **~/policies/pubsub_test_thing_policy.json** in Ihrem Texteditor.

4. Führen Sie diesen Befehl aus, um das Richtliniendokument aus den vorherigen Schritten zum Erstellen einer AWS IoT Richtlinie zu verwenden.

```
aws iot create-policy \
--policy-name "PubSubTestThingPolicy" \
--policy-document "file://~/policies/pubsub_test_thing_policy.json"
```

Wenn die Richtlinie erstellt wurde, gibt der Befehl eine Antwort wie die folgende zurück:

```
{
    "policyName": "PubSubTestThingPolicy",
    "policyArn": "arn:aws:iot:us-west-2:57EXAMPLE833:policy/PubSubTestThingPolicy",
    "policyDocument": "{\n\"Version\": \"2012-10-17\",\n\"Statement\": [\n{\n
\"Effect\": \"Allow\",\n\"Action\": [\n\"iot:Connect\"\n],\n\"Resource\":
 [\n\"arn:aws:iot:us-west-2:57EXAMPLE833:client/PubSubTestThing\"\n]\n},\n{\n
\"Effect\": \"Allow\",\n\"Action\": [\n\"iot:Publish\"\n],\n\"Resource\":
 [\n\"arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/pubtopic\"\n]\n},\n{\n
\"Effect\": \"Allow\",\n\"Action\": [\n\"iot:Subscribe\"\n],\n\"Resource\": [\n
\"arn:aws:iot:us-west-2:57EXAMPLE833:topicfilter/test/dc/subtopic\"\n]\n},\n{\n
\"Effect\": \"Allow\",\n\"Action\": [\n\"iot:Receive\"\n],\n\"Resource\": [\n
\"arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/*\"\n]\n}\n]\n}\n",
    "policyVersionId": "1"
```

5. Führen Sie diesen Befehl aus, um die Richtlinie an das Gerätezertifikat anzufügen. Ersetzen Sie *certificateArn* durch den `certificateArn`-Wert, den Sie in diesem Abschnitt bereits gespeichert haben.

   ```
   aws iot attach-policy \
   --policy-name "PubSubTestThingPolicy" \
   --target "certificateArn"
   ```

   Bei erfolgreicher Ausführung gibt dieser Befehl nichts zurück.

6. Führen Sie diesen Befehl aus, um das Gerätezertifikat an die AWS IoT -Objektressource anzuhängen. Ersetzen Sie *certificateArn* durch den `certificateArn`-Wert, den Sie in diesem Abschnitt bereits gespeichert haben.

   ```
   aws iot attach-thing-principal \
   --thing-name "PubSubTestThing" \
   --principal "certificateArn"
   ```

   Bei erfolgreicher Ausführung gibt dieser Befehl nichts zurück.

Nachdem Sie Ihr Gerät erfolgreich bereitgestellt haben AWS IoT, können Sie damit fortfahrenthe section called “Konfigurieren Sie die Konfigurationsdatei und den Client des MQTT Geräteclients”.

Konfigurieren Sie die AWS IoT Device Client-Konfigurationsdatei und MQTT testen Sie den Client, um die MQTT Kommunikation zu demonstrieren

Mit diesem Verfahren wird eine Konfigurationsdatei zum Testen des AWS IoT Geräteclients erstellt.

Um die Konfigurationsdatei zum Testen des AWS IoT Geräteclients zu erstellen

1. Gehen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, folgendermaßen vor:

   a. Öffnen Sie einen Texteditor, z. B. `nano`.

   b. Kopieren Sie dieses JSON Dokument und fügen Sie es in Ihren geöffneten Texteditor ein.

   ```
   {
     "endpoint": "a3qEXAMPLEaffp-ats.iot.us-west-2.amazonaws.com",
     "cert": "~/certs/pubsub/device.pem.crt",
     "key": "~/certs/pubsub/private.pem.key",
   ```

```
"root-ca": "~/certs/AmazonRootCA1.pem",
"thing-name": "PubSubTestThing",
"logging": {
  "enable-sdk-logging": true,
  "level": "DEBUG",
  "type": "STDOUT",
  "file": ""
},
"jobs": {
  "enabled": false,
  "handler-directory": ""
},
"tunneling": {
  "enabled": false
},
"device-defender": {
  "enabled": false,
  "interval": 300
},
"fleet-provisioning": {
  "enabled": false,
  "template-name": "",
  "template-parameters": "",
  "csr-file": "",
  "device-key": ""
},
"samples": {
  "pub-sub": {
    "enabled": true,
    "publish-topic": "test/dc/pubtopic",
    "publish-file": "",
    "subscribe-topic": "test/dc/subtopic",
    "subscribe-file": "~/.aws-iot-device-client/log/pubsub_rx_msgs.log"
  }
},
"config-shadow": {
  "enabled": false
},
"sample-shadow": {
  "enabled": false,
  "shadow-name": "",
  "shadow-input-file": "",
  "shadow-output-file": ""
}
```

```
}
```

c. Ersetzen Sie das *endpoint* Wert durch den Endpunkt der Gerätedaten für Ihren AWS-Konto , den Sie in gefunden habenthe section called “Stellen Sie Ihr Gerät bereit in AWS IoT Core”.

d. Speichern Sie die Datei als **~/dc-configs/dc-pubsub-config.json** in Ihrem Texteditor.

e. Führen Sie diesen Befehl aus, um die Berechtigungen für die neue Konfigurationsdatei festzulegen.

```
chmod 644 ~/dc-configs/dc-pubsub-config.json
```

2. So bereiten Sie den MQTTTestclient darauf vor, alle MQTT Nachrichten zu abonnieren:

a. Wählen Sie auf Ihrem lokalen Host-Computer in der AWS IoT Konsole MQTT Testclient aus.

b. Geben Sie auf der Registerkarte Thema abonnieren unter Themenfilter **#** (ein einzelnes Rautenzeichen) ein und wählen Sie Abonnieren aus.

c. Vergewissern Sie sich, dass Sie unter der Bezeichnung Abonnements **#** (ein einzelnes Pfundzeichen) sehen.

Lassen Sie das Fenster mit dem MQTTTestclient geöffnet, während Sie mit diesem Tutorial fortfahren.

Nachdem Sie die Datei gespeichert und den MQTTTestclient konfiguriert haben, können Sie fortfahrenthe section called “Veröffentlichen Sie Nachrichten mit dem IoT Device Client”.

## Demonstrieren Sie das Veröffentlichen von Nachrichten mit dem AWS IoT Device Client

Die Verfahren in diesem Abschnitt zeigen, wie der AWS IoT Device Client Standard- und benutzerdefinierte MQTT Nachrichten senden kann.

Die Richtlinienanweisungen in der Richtlinie, die Sie im vorherigen Schritt für diese Übungen erstellt haben, geben dem Raspberry Pi die Erlaubnis, die folgenden Aktionen auszuführen:

- **iot:Connect**

Gibt dem genannten Client`PubSubTestThing`, Ihrem Raspberry Pi, auf dem der AWS IoT Geräteclient ausgeführt wird, die Möglichkeit, eine Verbindung herzustellen.

```
{
  "Effect": "Allow",
  "Action": [
    "iot:Connect"
  ],
  "Resource": [
    "arn:aws:iot:us-west-2:57EXAMPLE833:client/PubSubTestThing"
  ]
}
```

- **`iot:Publish`**

  Erteilt dem Raspberry Pi die Erlaubnis, Nachrichten mit dem MQTT Thema zu veröffentlichen`test/dc/pubtopic`.

```
{
  "Effect": "Allow",
  "Action": [
    "iot:Publish"
  ],
  "Resource": [
    "arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/pubtopic"
  ]
}
```

  Die `iot:Publish` Aktion erteilt die Erlaubnis, zu den MQTT Themen zu veröffentlichen, die im Resource-Array aufgeführt sind. Der Inhalt dieser Nachrichten wird nicht durch die Richtlinienanweisung geregelt.

Veröffentlichen der Standardnachricht mithilfe des AWS IoT Device Clients

Bei diesem Verfahren wird der AWS IoT Geräteclient so ausgeführt, dass er eine einzige MQTT Standardnachricht veröffentlicht, die der MQTTTestclient empfängt und anzeigt.

Um die MQTT Standardnachricht vom AWS IoT Geräteclient aus zu senden

1. Stellen Sie sicher, dass sowohl das Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, als auch das Fenster mit dem MQTTTestclient sichtbar sind, während Sie dieses Verfahren ausführen.
2. Geben Sie im Terminalfenster diese Befehle ein, um den AWS IoT Geräteclient mithilfe der in erstellten Konfigurationsdatei auszuführenthe section called “Erstellen der Konfigurationsdatei”.

   ```
   cd ~/aws-iot-device-client/build
   ./aws-iot-device-client --config-file ~/dc-configs/dc-pubsub-config.json
   ```

   Im Terminalfenster zeigt der AWS IoT Geräteclient Informationsmeldungen und alle Fehler an, die bei der Ausführung auftreten.

   Wenn im Terminalfenster keine Fehler angezeigt werden, überprüfen Sie den MQTTTestclient.
3. Im MQTTTestclient finden Sie im Abonnementfenster Hello World! Nachricht wurde an das `test/dc/pubtopic` Nachrichtenthema gesendet.
4. Wenn der AWS IoT Geräteclient keine Fehler anzeigt und Sie Hello World! sehen an die `test/dc/pubtopic` Nachricht im MQTTTestclient gesendet, haben Sie eine erfolgreiche Verbindung nachgewiesen.
5. Geben Sie im Terminalfenster **^C** (Strg-C) ein, um den AWS IoT Geräteclient zu beenden.

Nachdem Sie nachgewiesen haben, dass der AWS IoT Device Client die MQTT Standardnachricht veröffentlicht hat, können Sie mit dem fortfahren. the section called “Veröffentlichen Sie MQTT eine benutzerdefinierte Nachricht”

Veröffentlichen Sie eine benutzerdefinierte Nachricht mit dem AWS IoT Device Client

Die Verfahren in diesem Abschnitt erstellen eine benutzerdefinierte MQTT Nachricht und führen dann den AWS IoT Geräteclient aus, sodass er die benutzerdefinierte MQTT Nachricht einmalig veröffentlicht, damit der MQTTTestclient sie empfangen und anzeigen kann.

Erstellen Sie eine benutzerdefinierte MQTT Nachricht für den AWS IoT Geräteclient

Führen Sie diese Schritte im Terminalfenster auf Ihrem lokalen Host-Computer aus, der mit Ihrem Raspberry Pi verbunden ist.

Um eine benutzerdefinierte Nachricht zu erstellen, die der AWS IoT Device Client veröffentlichen soll

1. Öffnen Sie im Terminalfenster einen Texteditor Ihrer Wahl, z. B. `nano`.
2. Kopieren Sie das folgende JSON Dokument und fügen Sie es in den Texteditor ein. Dies ist die MQTT Nachrichten-Payload, die der AWS IoT Device Client veröffentlicht.

```
{
  "temperature": 28,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

3. Speichern Sie den Inhalt des Texteditors als **`~/messages/sample-ws-message.json`**.
4. Geben Sie den folgenden Befehl ein, um die Berechtigungen der Nachrichtendatei festzulegen, die Sie gerade erstellt haben.

```
chmod 600 ~/messages/*
```

Um eine Konfigurationsdatei für den AWS IoT Geräteclient zu erstellen, die zum Senden der benutzerdefinierten Nachricht verwendet werden soll

1. Öffnen Sie im Terminalfenster in einem Texteditor wie `nano` z. B. die vorhandene AWS IoT Geräteclient-Konfigurationsdatei:**`~/dc-configs/dc-pubsub-config.json`**.
2. Bearbeiten Sie das `samples`-Objekt so, dass es folgendermaßen aussieht. Kein anderer Teil dieser Datei muss geändert werden.

```
  "samples": {
    "pub-sub": {
      "enabled": true,
      "publish-topic": "test/dc/pubtopic",
      "publish-file": "~/messages/sample-ws-message.json",
      "subscribe-topic": "test/dc/subtopic",
      "subscribe-file": "~/.aws-iot-device-client/log/pubsub_rx_msgs.log"
```

3. Speichern Sie den Inhalt des Texteditors als **`~/dc-configs/dc-pubsub-custom-config.json`**.
4. Führen Sie diesen Befehl aus, um die Berechtigungen für die neue Konfigurationsdatei festzulegen.

   ```
   chmod 644 ~/dc-configs/dc-pubsub-custom-config.json
   ```

Veröffentlichen Sie die benutzerdefinierte MQTT Nachricht mithilfe des AWS IoT Geräteclients

Diese Änderung wirkt sich nur auf den Inhalt der MQTT Nachrichten-Payload aus, sodass die aktuelle Richtlinie weiterhin gültig ist. Wenn jedoch das MQTTThema (wie durch den `publish-topic` Wert in definiert`~/dc-configs/dc-pubsub-custom-config.json`) geändert würde, müsste auch die `iot::Publish` Grundsatzerklärung geändert werden, damit der Raspberry Pi unter dem neuen MQTT Thema veröffentlichen kann.

Um die MQTT Nachricht vom AWS IoT Geräteclient aus zu senden

1. Stellen Sie sicher, dass sowohl das Terminalfenster als auch das Fenster mit dem MQTTTestclient sichtbar sind, während Sie dieses Verfahren ausführen. Stellen Sie außerdem sicher, dass Ihr MQTTTestclient weiterhin den #-Themenfilter abonniert hat. Falls nicht, abonnieren Sie den #-Themenfilter erneut.
2. Geben Sie im Terminalfenster diese Befehle ein, um den AWS IoT Device Client mithilfe der in the section called “Erstellen der Konfigurationsdatei” erstellten Konfigurationsdatei auszuführen.

   ```
   cd ~/aws-iot-device-client/build
   ./aws-iot-device-client --config-file ~/dc-configs/dc-pubsub-custom-config.json
   ```

   Im Terminalfenster zeigt der AWS IoT Geräteclient Informationsmeldungen und alle Fehler an, die bei der Ausführung auftreten.

   Wenn im Terminalfenster keine Fehler angezeigt werden, überprüfen Sie den MQTT Testclient.
3. Sehen Sie sich im MQTTTestclient im Abonnementfenster die Nutzdaten für benutzerdefinierte Nachrichten an, die an das `test/dc/pubtopic` Nachrichtenthema gesendet wurden.
4. Wenn der AWS IoT Geräteclient keine Fehler anzeigt und Sie die Payload für benutzerdefinierte Nachrichten sehen, die Sie für die `test/dc/pubtopic` Nachricht im MQTTTestclient veröffentlicht haben, haben Sie eine benutzerdefinierte Nachricht erfolgreich veröffentlicht.

5. Geben Sie im Terminalfenster **^C** (Strg-C) ein, um den AWS IoT Device Client zu beenden.

Nachdem Sie nachgewiesen haben, dass der AWS IoT Device Client eine benutzerdefinierte Nachrichten-Payload veröffentlicht hat, können Sie damit fortfahren. the section called “Abonnieren Sie Nachrichten mit dem IoT Device Client”

## Demonstrieren Sie das Abonnieren von Nachrichten mit dem Device Client AWS IoT

In diesem Abschnitt werden Sie zwei Arten von Nachrichtenabonnements demonstrieren:

- Abonnement für ein einzelnes Thema
- Abonnement für Wildcard-Themen

Die Richtlinienanweisungen in der Richtlinie, die Sie für diese Übungen erstellt haben, geben dem Raspberry Pi die Erlaubnis, die folgenden Aktionen auszuführen:

- **`iot:Receive`**

  Erteilt dem AWS IoT Geräteclient die Berechtigung, MQTT Themen zu empfangen, die den im `Resource` Objekt genannten Themen entsprechen.

  ```
  {
    "Effect": "Allow",
    "Action": [
      "iot:Receive"
    ],
    "Resource": [
      "arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/subtopic"
    ]
  }
  ```

- **`iot:Subscribe`**

  Erteilt dem AWS IoT Geräteclient die Berechtigung, MQTT Themenfilter zu abonnieren, die den im `Resource` Objekt genannten Filtern entsprechen.

  ```
  {
    "Effect": "Allow",
    "Action": [
      "iot:Subscribe"
  ```

```
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topicfilter/test/dc/subtopic"
      ]
    }
```

Abonnieren Sie ein einzelnes MQTT Nachrichtenthema

Dieses Verfahren zeigt, wie der AWS IoT Device Client MQTT Nachrichten abonnieren und protokollieren kann.

Listen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, den Inhalt der Datei von **`~/dc-configs/dc-pubsub-custom-config.json`** auf oder öffnen Sie die Datei in einem Texteditor, um den Inhalt zu überprüfen. Suchen Sie das `samples`-Objekt, das wie folgt aussehen sollte.

```
"samples": {
  "pub-sub": {
    "enabled": true,
    "publish-topic": "test/dc/pubtopic",
    "publish-file": "~/messages/sample-ws-message.json",
    "subscribe-topic": "test/dc/subtopic",
    "subscribe-file": "~/.aws-iot-device-client/log/pubsub_rx_msgs.log"
```

Beachten Sie, dass der `subscribe-topic` Wert das MQTT Thema ist, das der AWS IoT Device Client abonniert, wenn er ausgeführt wird. Der AWS IoT Geräteclient schreibt die Nachrichten-Payloads, die er von diesem Abonnement empfängt, in die im `subscribe-file` Wert angegebene Datei.

Um ein MQTT Nachrichtenthema vom AWS IoT Device Client aus zu abonnieren

1. Stellen Sie sicher, dass sowohl das Terminalfenster als auch das Fenster mit dem MQTT Testclient sichtbar sind, während Sie dieses Verfahren ausführen. Stellen Sie außerdem sicher, dass Ihr MQTTTestclient weiterhin den #-Themenfilter abonniert hat. Falls nicht, abonnieren Sie den #-Themenfilter erneut.
2. Geben Sie im Terminalfenster diese Befehle ein, um den AWS IoT Geräteclient mithilfe der in the section called “Erstellen der Konfigurationsdatei” erstellten Konfigurationsdatei auszuführen.

   ```
   cd ~/aws-iot-device-client/build
   ```

```
./aws-iot-device-client --config-file ~/dc-configs/dc-pubsub-custom-config.json
```

Im Terminalfenster zeigt der AWS IoT Geräteclient Informationsmeldungen und alle Fehler an, die bei der Ausführung auftreten.

Wenn im Terminalfenster keine Fehler angezeigt werden, fahren Sie in der AWS IoT -Konsole fort.

3. Wählen Sie in der AWS IoT Konsole im MQTTTestclient die Registerkarte In einem Thema veröffentlichen aus.
4. Geben Sie in das Feld Name des Themas **`test/dc/subtopic`** ein.
5. Überprüfen Sie unter Nachrichtennutzlast den Nachrichteninhalt.
6. Wählen Sie Veröffentlichen, um die MQTT Nachricht zu veröffentlichen.
7. Achten Sie im Terminalfenster auf den Eintrag „Nachricht erhalten“ vom AWS IoT Geräteclient, der wie folgt aussieht.

```
2021-11-10T16:02:20.890Z [DEBUG] {samples/PubSubFeature.cpp}: Message received on
 subscribe topic, size: 45 bytes
```

8. Wenn Sie den Eintrag „Nachricht empfangen“ sehen, aus dem hervorgeht, dass die Nachricht empfangen wurde, geben Sie **`^C`** (Strg-C) ein, um den AWS IoT Geräteclient zu beenden.
9. Geben Sie diesen Befehl ein, um das Ende der Nachrichtenlogdatei und die Nachricht zu sehen, die Sie vom MQTTTestclient veröffentlicht haben.

```
tail ~/.aws-iot-device-client/log/pubsub_rx_msgs.log
```

Durch das Anzeigen der Nachricht in der Protokolldatei haben Sie nachgewiesen, dass der AWS IoT Device Client die von Ihnen veröffentlichte Nachricht vom MQTT Testclient erhalten hat.

Abonnieren Sie mehrere MQTT Nachrichtenthemen mithilfe von Platzhalterzeichen

Diese Verfahren veranschaulichen, wie der AWS IoT Device Client MQTT Nachrichten mithilfe von Platzhalterzeichen abonnieren und protokollieren kann. Gehen Sie dazu wie folgt vor:

1. Aktualisieren Sie den Themenfilter, den der AWS IoT Device Client zum Abonnieren von MQTT Themen verwendet.
2. Aktualisieren Sie die vom Gerät verwendete Richtlinie, um die neuen Abonnements zuzulassen.

3. Führen Sie den AWS IoT Geräteclient aus und veröffentlichen Sie Nachrichten von der MQTT Testkonsole aus.

Um eine Konfigurationsdatei zum Abonnieren mehrerer MQTT Nachrichtenthemen mithilfe eines Themenfilters mit Platzhaltern MQTT zu erstellen

1. Öffnen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, **`~/dc-configs/dc-pubsub-custom-config.json`**, um das `samples`-Objekt zu finden und zu bearbeiten.
2. Suchen Sie im Texteditor das `samples`-Objekt und aktualisieren Sie den `subscribe-topic`-Wert so, dass er folgendermaßen aussieht:

   ```
   "samples": {
     "pub-sub": {
       "enabled": true,
       "publish-topic": "test/dc/pubtopic",
       "publish-file": "~/messages/sample-ws-message.json",
       "subscribe-topic": "test/dc/#",
       "subscribe-file": "~/.aws-iot-device-client/log/pubsub_rx_msgs.log"
   ```

   Der neue `subscribe-topic` Wert ist ein MQTTThemenfilter mit einem MQTT Platzhalterzeichen am Ende. Dies beschreibt ein Abonnement für alle MQTT Themen, die mit beginnen`test/dc/`. Der AWS IoT Geräteclient schreibt die Nachrichtennutzdaten, die er von diesem Abonnement empfängt, in `subscribe-file` die unter angegebene Datei.
3. Speichern Sie die geänderte Konfigurationsdatei als **`~/dc-configs/dc-pubsub-wild-config.json`** und schließen Sie den Editor.

Um die von Ihrem Raspberry Pi verwendete Richtlinie so zu ändern, dass Sie mehrere MQTT Nachrichtenthemen abonnieren und empfangen können

1. Öffnen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, in Ihrem bevorzugten Texteditor **`~/policies/pubsub_test_thing_policy.json`** zur Bearbeitung und suchen Sie dann die `iot::Subscribe`- und `iot::Receive`-Richtlinienanweisungen in der Datei.
2. Aktualisieren Sie in der `iot::Subscribe`-Richtlinienanweisung die Zeichenfolge im Ressourcenobjekt, indem Sie `subtopic` durch `*` ersetzten, sodass sie wie folgt aussieht:

```
{
  "Effect": "Allow",
  "Action": [
    "iot:Subscribe"
  ],
  "Resource": [
    "arn:aws:iot:us-west-2:57EXAMPLE833:topicfilter/test/dc/*"
  ]
}
```

> **Note**
>
> Die MQTTPlatzhalterzeichen für den Themenfilter sind das + (Pluszeichen) und das # (Rautenzeichen). Eine Abonnementanfrage mit # am Ende abonniert alle Themen, die mit der Zeichenfolge beginnen, die dem #-Zeichen vorausgeht (zum Beispiel `test/dc/` in diesem Fall).
> Für den Ressourcenwert in der Richtlinienanweisung, die dieses Abonnement autorisiert, muss im Themenfilter jedoch ein * (ein Sternchen) anstelle des # (ein Pfundzeichen) verwendet werden. ARN Das liegt daran, dass der Richtlinienprozessor ein anderes Platzhalterzeichen verwendet als MQTT verwendet.
> Weitere Informationen zur Verwendung von Platzhalterzeichen für Themen und Themenfilter in Richtlinien finden Sie unter Verwenden von Platzhalterzeichen in MQTT und AWS IoT Core -Richtlinien.

3. Aktualisieren Sie in der `iot::Receive`-Richtlinienanweisung die Zeichenfolge im Ressourcenobjekt, indem Sie `subtopic` durch * ersetzten, sodass sie wie folgt aussieht:

```
{
  "Effect": "Allow",
  "Action": [
    "iot:Receive"
  ],
  "Resource": [
    "arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/*"
  ]
}
```

4. Speichern Sie das aktualisierte Richtliniendokument unter **`~/policies/pubsub_wild_test_thing_policy.json`** und schließen Sie den Editor.

5. Geben Sie diesen Befehl ein, um die Richtlinie für dieses Tutorial zu aktualisieren und die neuen Ressourcendefinitionen zu verwenden.

```
aws iot create-policy-version \
--set-as-default \
--policy-name "PubSubTestThingPolicy" \
--policy-document "file://~/policies/pubsub_wild_test_thing_policy.json"
```

Bei Erfolg gibt der Befehl ein Ergebnis wie dieses zurück: Beachten Sie, dass `policyVersionId` jetzt 2 ist, was darauf hindeutet, dass es sich um die zweite Version dieser Richtlinie handelt.

Wenn Sie die Richtlinie erfolgreich aktualisiert haben, können Sie mit dem nächsten Verfahren fortfahren.


```
{
    "policyArn": "arn:aws:iot:us-west-2:57EXAMPLE833:policy/PubSubTestThingPolicy",
    "policyDocument": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n
 {\n      \"Effect\": \"Allow\",\n      \"Action\": [\n        \"iot:Connect\"\n
    ],\n      \"Resource\": [\n        \"arn:aws:iot:us-west-2:57EXAMPLE833:client/
PubSubTestThing\"\n      ]\n    },\n    {\n      \"Effect\": \"Allow\",\n
   \"Action\": [\n        \"iot:Publish\"\n      ],\n      \"Resource\": [\n
        \"arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/pubtopic\"\n
  ]\n    },\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": [\n
 \"iot:Subscribe\"\n      ],\n      \"Resource\": [\n        \"arn:aws:iot:us-
west-2:57EXAMPLE833:topicfilter/test/dc/*\"\n      ]\n    },\n    {\n      \"Effect
\": \"Allow\",\n      \"Action\": [\n        \"iot:Receive\"\n      ],\n
 \"Resource\": [\n        \"arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/*\"\n
     ]\n    }\n  ]\n}\n",
    "policyVersionId": "2",
    "isDefaultVersion": true
}
```


Wenn Sie die Fehlermeldung erhalten, dass zu viele Richtlinienversionen vorhanden sind, um eine neue zu speichern, geben Sie diesen Befehl ein, um die aktuellen Versionen der Richtlinie aufzulisten. Suchen Sie in der Liste, die dieser Befehl zurückgibt, nach einer Richtlinienversion, die Sie löschen können.

```
aws iot list-policy-versions --policy-name "PubSubTestThingPolicy"
```

Geben Sie diesen Befehl ein, um eine nicht mehr benötigte Version zu löschen. Beachten Sie, dass Sie die Standardversion der Richtlinie nicht löschen können. Die Standardversion der Richtlinie hat einen `isDefaultVersion`-Wert von `true`.

```
aws iot delete-policy-version \
--policy-name "PubSubTestThingPolicy" \
--policy-version-id policyId
```

Versuchen Sie diesen Schritt erneut, nachdem Sie eine Richtlinienversion gelöscht haben.

Mit der aktualisierten Konfigurationsdatei und Richtlinie sind Sie bereit, Wildcard-Abonnements mit dem AWS IoT Device Client zu demonstrieren.

Um zu demonstrieren, wie der AWS IoT Device Client mehrere MQTT Nachrichtenthemen abonniert und empfängt

1. Überprüfen Sie im MQTTTestclient die Abonnements. Wenn der MQTTTestclient den Filter „Im **#** Thema“ abonniert hat, fahren Sie mit dem nächsten Schritt fort. Falls nicht, geben Sie im MQTTTestclient auf der Registerkarte Thema abonnieren im Themenfilter **#** (ein Rautenzeichen) ein, und wählen Sie dann Abonnieren aus, um ihn zu abonnieren.
2. Gehen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, diese Befehle ein, um den AWS IoT Device Client zu starten.

   ```
   cd ~/aws-iot-device-client/build
   ./aws-iot-device-client --config-file ~/dc-configs/dc-pubsub-wild-config.json
   ```
3. Kehren Sie zum MQTTTestclient zurück, während Sie sich die Ausgabe des AWS IoT Geräteclients im Terminalfenster auf dem lokalen Hostcomputer ansehen. Geben Sie auf der Registerkarte In einem Thema veröffentlichen unter Themenname **`test/dc/subtopic`** ein, und wählen Sie dann Veröffentlichen aus.
4. Vergewissern Sie sich im Terminalfenster, dass die Nachricht empfangen wurde, indem Sie nach einer Nachricht suchen, wie z. B.:

   ```
   2021-11-10T16:34:20.101Z [DEBUG] {samples/PubSubFeature.cpp}: Message received on
    subscribe topic, size: 76 bytes
   ```

5. Kehren Sie zum MQTTTestclient zurück, während Sie sich die Ausgabe des AWS IoT Geräteclients im Terminalfenster des lokalen Host-Computers ansehen. Geben Sie auf der Registerkarte In einem Thema veröffentlichen unter Themenname **`test/dc/subtopic2`** ein, und wählen Sie dann Veröffentlichen aus.
6. Vergewissern Sie sich im Terminalfenster, dass die Nachricht empfangen wurde, indem Sie nach einer Nachricht suchen, wie z. B.:

   ```
   2021-11-10T16:34:32.078Z [DEBUG] {samples/PubSubFeature.cpp}: Message received on
    subscribe topic, size: 77 bytes
   ```
7. Wenn Sie die Meldungen sehen, die bestätigen, dass beide Nachrichten empfangen wurden, drücken Sie **`^C`** (Strg-C), um den AWS IoT Geräteclient zu beenden.
8. Geben Sie diesen Befehl ein, um das Ende der Nachrichtenlogdatei und die Nachricht zu sehen, die Sie vom MQTTTestclient veröffentlicht haben.

   ```
   tail -n 20 ~/.aws-iot-device-client/log/pubsub_rx_msgs.log
   ```

   > **Note**
   >
   > Die Protokolldatei enthält nur Nachrichtennutzlasten. Die Nachrichtenthemen werden nicht in der Protokolldatei für empfangene Nachrichten aufgezeichnet. Möglicherweise sehen Sie die vom AWS IoT Geräteclient veröffentlichte Nachricht auch im empfangenen Protokoll. Das liegt daran, dass der Themenfilter mit Platzhaltern dieses Nachrichtenthema enthält und die Abonnementanforderung manchmal vom Message Broker verarbeitet werden kann, bevor die veröffentlichte Nachricht an Subscriber gesendet wird.

Die Einträge in der Protokolldatei belegen, dass die Nachrichten empfangen wurden. Sie können dieses Verfahren mit anderen Themennamen wiederholen. Alle Nachrichten, deren Themenname mit `test/dc/` beginnt, sollten empfangen und protokolliert werden. Nachrichten mit Themennamen, die mit einem anderen Text beginnen, werden ignoriert.

Nachdem Sie gezeigt haben, wie der AWS IoT Device Client MQTT Nachrichten veröffentlichen und abonnieren kann, fahren Sie fort mitTutorial: Demonstrieren von Remote-Aktionen (Jobs) mit dem AWS IoT Device Client.

# Tutorial: Demonstrieren von Remote-Aktionen (Jobs) mit dem AWS IoT Device Client

In diesen Tutorials konfigurieren und implementieren Sie Jobs auf Ihrem Raspberry Pi, um nachzuweisen, dass Sie Fernoperationen an Ihre IoT-Geräte senden können.

So beginnen Sie dieses Tutorial:

- Lassen Sie Ihren lokalen Host-Computer einen Raspberry Pi konfigurieren, wie im vorherigen Abschnitt zu sehen.
- Wenn Sie das Tutorial im vorherigen Abschnitt noch nicht abgeschlossen haben, können Sie dieses Tutorial ausprobieren, indem Sie den Raspberry Pi mit einer microSD-Karte verwenden, auf der das Bild gespeichert ist, das Sie nach der Installation des AWS IoT Device Clients gespeichert haben. (Optional) Speichern des microSD-Karten-Images
- Wenn Sie diese Demo schon einmal ausgeführt haben, überprüfen ??? Sie, ob Sie alle AWS IoT Ressourcen löschen sollten, die Sie in früheren Läufen erstellt haben, um doppelte Ressourcenfehler zu vermeiden.

Für dieses Tutorial brauchen Sie ungefähr 45 Minuten.

Wenn Sie mit diesem Thema fertig sind:

- Sie haben verschiedene Möglichkeiten demonstriert, wie Ihr IoT-Gerät die verwenden kann AWS IoT Core , um Fernoperationen auszuführen, die von verwaltet werden AWS IoT .

Erforderliche Ausstattung:

- Ihre lokale Entwicklungs- und Testumgebung, die Sie in einem vorherigen Abschnitt getestet haben
- Der Raspberry Pi, den Sie im vorherigen Abschnitt getestet haben
- Die microSD-Speicherkarte des Raspberry Pi, die Sie in einem vorherigen Abschnitt getestet haben

Verfahren in diesem Tutorial

- Bereiten Sie den Raspberry Pi für die Ausführung von Jobs vor
- Erstellen Sie den Job AWS IoT mit dem AWS IoT Geräteclient und führen Sie ihn aus

## Bereiten Sie den Raspberry Pi für die Ausführung von Jobs vor

Die Verfahren in diesem Abschnitt beschreiben, wie Sie Ihren Raspberry Pi für die Ausführung von Jobs mithilfe des AWS IoT Geräteclients vorbereiten.

> **Note**
>
> Diese Verfahren sind gerätespezifisch. Wenn Sie die Verfahren in diesem Abschnitt mit mehr als einem Gerät gleichzeitig durchführen möchten, benötigt jedes Gerät eine eigene Richtlinie und ein eindeutiges, gerätespezifisches Zertifikat sowie einen ebensolchen Objektnamen. Um jedem Gerät seine eigenen Ressourcen zuzuweisen, führen Sie dieses Verfahren einmal für jedes Gerät durch und ändern Sie dabei die gerätespezifischen Elemente, wie in den Verfahren beschrieben.

Verfahren in diesem Tutorial

- Bereitstellen Ihres Raspberry Pi, um Jobs zu demonstrieren
- Konfigurieren Sie den AWS IoT Geräteclient so, dass er den Job-Agent ausführt

### Bereitstellen Ihres Raspberry Pi, um Jobs zu demonstrieren

Die Verfahren in diesem Abschnitt stellen Ihren Raspberry Pi bereit, AWS IoT indem Sie AWS IoT Ressourcen und Gerätezertifikate dafür erstellen.

Themen

- Erstellen Sie Gerätezertifikatsdateien und laden Sie sie herunter, um AWS IoT Jobs zu demonstrieren
- Erstellen Sie AWS IoT Ressourcen, um AWS IoT Jobs zu demonstrieren

#### Erstellen Sie Gerätezertifikatsdateien und laden Sie sie herunter, um AWS IoT Jobs zu demonstrieren

Mit diesem Verfahren werden die Gerätezertifikatsdateien für diese Demo erstellt.

Wenn Sie mehr als ein Gerät vorbereiten, muss dieses Verfahren auf jedem Gerät durchgeführt werden.

So erstellen Sie die Gerätezertifikatsdateien für Ihren Raspberry Pi und laden sie herunter:

Gehen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, folgendermaßen vor:

1. Geben Sie den folgenden Befehl ein, um die Gerätezertifikatsdateien für Ihr Gerät zu erstellen.

   ```
   aws iot create-keys-and-certificate \
   --set-as-active \
   --certificate-pem-outfile "~/certs/jobs/device.pem.crt" \
   --public-key-outfile "~/certs/jobs/public.pem.key" \
   --private-key-outfile "~/certs/jobs/private.pem.key"
   ```

   Die Ausgabe des Befehls ähnelt der Folgenden: Speichern Sie den *certificateArn*-Wert zur späteren Verwendung.

   ```
   {
   "certificateArn": "arn:aws:iot:us-
   west-2:57EXAMPLE833:cert/76e7e4edb3e52f52334be2f387a06145b2aa4c7fcd810f3aea2d92abc227d269",
   "certificateId":
    "76e7e4edb3e52f5233EXAMPLE7a06145b2aa4c7fcd810f3aea2d92abc227d269",
   "certificatePem": "-----BEGIN CERTIFICATE-----
   \nMIIDWTCCAkGgAwIBAgI_SHORTENED_FOR_EXAMPLE_Lgn4jfgtS\n-----END CERTIFICATE-----
   \n",
   "keyPair": {
       "PublicKey": "-----BEGIN PUBLIC KEY-----
   \nMIIBIjANBgkqhkiG9w0BA_SHORTENED_FOR_EXAMPLE_ImwIDAQAB\n-----END PUBLIC KEY-----
   \n",
       "PrivateKey": "-----BEGIN RSA PRIVATE KEY-----
   \nMIIEowIBAAKCAQE_SHORTENED_FOR_EXAMPLE_T9RoDiukY\n-----END RSA PRIVATE KEY-----\n"
   }
   }
   ```

2. Geben Sie die folgenden Befehle ein, um die Berechtigungen für das Zertifikatsverzeichnis und seine Dateien festzulegen.

   ```
   chmod 700 ~/certs/jobs
   chmod 644 ~/certs/jobs/*
   chmod 600 ~/certs/jobs/private.pem.key
   ```

3. Führen Sie diesen Befehl aus, um die Berechtigungen für Ihre Zertifikatsverzeichnisse und -dateien zu überprüfen.

```
ls -l ~/certs/jobs
```

Der Befehl sollte ähnliche Werte wie die hier angezeigten ausgeben, mit der Ausnahme, dass Datum und Uhrzeit unterschiedlich sein werden.

```
-rw-r--r-- 1 pi pi 1220 Oct 28 13:02 device.pem.crt
-rw------- 1 pi pi 1675 Oct 28 13:02 private.pem.key
-rw-r--r-- 1 pi pi  451 Oct 28 13:02 public.pem.key
```

Nachdem Sie die Gerätezertifikatsdateien auf Ihren Raspberry Pi heruntergeladen haben, können Sie mit the section called “Stellen Sie Raspberry Pi für Jobs bereit” fortfahren.

Erstellen Sie AWS IoT Ressourcen, um AWS IoT Jobs zu demonstrieren

Erstellen Sie die AWS IoT Ressourcen für dieses Gerät.

Wenn Sie mehr als ein Gerät vorbereiten, muss dieses Verfahren auf jedem Gerät durchgeführt werden.

So stellen Sie Ihr Gerät in AWS IoT bereit:

Gehen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, folgendermaßen vor:

1. Geben Sie den folgenden Befehl ein, um die Adresse des Gerätedatenendpunkts für Ihr AWS-Konto abzurufen.

   ```
   aws iot describe-endpoint --endpoint-type IoT:Data-ATS
   ```

   Der Endpunktwert hat sich seit der letzten Ausführung dieses Befehls nicht geändert. Wenn Sie den Befehl hier erneut ausführen, können Sie den Datenendpunktwert leicht finden und in die in diesem Tutorial verwendete Konfigurationsdatei einfügen.

   Die Ausgabe des describe-endpoint-Befehls ähnelt der folgenden: Notieren Sie sich den *endpointAddress*-Wert zur späteren Verwendung.

   ```
   {
   "endpointAddress": "a3qjEXAMPLEffp-ats.iot.us-west-2.amazonaws.com"
   ```

```
}
```

2. Ersetzen *uniqueThingName* mit einem eindeutigen Namen für Ihr Gerät. Wenn Sie dieses Tutorial mit mehreren Geräten durchführen möchten, geben Sie jedem Gerät einen eigenen Namen. Beispiele: **TestDevice01**, **TestDevice02** usw.

   Geben Sie diesen Befehl ein, um eine neue Ding-Ressource AWS IoT für Ihren Raspberry Pi zu erstellen.

   ```
   aws iot create-thing --thing-name "uniqueThingName"
   ```

   Da AWS IoT es sich bei einer Ding-Ressource um eine virtuelle Darstellung Ihres Geräts in der Cloud handelt, können wir mehrere Ding-Ressourcen erstellen, AWS IoT um sie für verschiedene Zwecke zu verwenden. Sie können alle von demselben physischen IoT-Gerät verwendet werden, um verschiedene Aspekte des Geräts darzustellen.

   > **Note**
   >
   > Wenn Sie die Richtlinie für mehrere Geräte sichern möchten, können Sie `${iot:Thing.ThingName}` anstelle des statischen Objektnamens verwenden, *uniqueThingName*.

   In diesen Tutorials wird jeweils nur eine Objektressource pro Gerät verwendet. Auf diese Weise stellen sie in diesen Tutorials die verschiedenen Demos dar, sodass Sie, nachdem Sie die AWS IoT Ressourcen für eine Demo erstellt haben, zurückgehen und die Demos wiederholen können, indem Sie die Ressourcen verwenden, die Sie jeweils speziell erstellt haben.

   Wenn Ihre AWS IoT Ding-Ressource erstellt wurde, gibt der Befehl eine Antwort wie diese zurück. Notieren Sie sich den *thingArn*-Wert, damit er später verwendet werden kann, wenn Sie den Job für die Ausführung auf diesem Gerät erstellen.

   ```
   {
   "thingName": "uniqueThingName",
   "thingArn": "arn:aws:iot:us-west-2:57EXAMPLE833:thing/uniqueThingName",
   "thingId": "8ea78707-32c3-4f8a-9232-14bEXAMPLEfd"
   }
   ```

3. Im Terminalfenster:

a. Öffnen Sie einen Texteditor, z. B. nano.

b. Kopieren Sie dieses JSON Dokument und fügen Sie es in Ihren geöffneten Texteditor ein.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Connect"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:client/uniqueThingName"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/pubtopic",
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/events/job/*",
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/events/jobExecution/*",
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/things/uniqueThingName/
jobs/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topicfilter/test/dc/subtopic",
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/events/jobExecution/*",
        "arn:aws:iot:us-west-2:57EXAMPLE833:topicfilter/$aws/
things/uniqueThingName/jobs/*"
      ]
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/subtopic",
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/things/uniqueThingName/
jobs/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:DescribeJobExecution",
        "iot:GetPendingJobExecutions",
        "iot:StartNextPendingJobExecution",
        "iot:UpdateJobExecution"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/things/uniqueThingName"
      ]
    }
  ]
}
```

c. Ersetzen Sie im Editor im `Resource` Abschnitt jeder Grundsatzerklärung *us-west-2:57EXAMPLE833* mit Ihrem AWS-Region, einem Doppelpunkt (:) und Ihrer 12-stelligen AWS-Konto Zahl.

d. Ersetzen Sie im Editor in jeder Grundsatzerklärung *uniqueThingName* mit dem Namen, den du diesem Ding als Ressource gegeben hast.

e. Speichern Sie die Datei als **~/policies/jobs_test_thing_policy.json** in Ihrem Texteditor.

   Wenn Sie dieses Verfahren für mehrere Geräte ausführen, speichern Sie die Datei auf jedem Gerät unter diesem Dateinamen.

4. Ersetzen *uniqueThingName* mit dem Ding-Namen für das Gerät, und führen Sie dann diesen Befehl aus, um eine AWS IoT Richtlinie zu erstellen, die auf dieses Gerät zugeschnitten ist.

```
aws iot create-policy \
--policy-name "JobTestPolicyForuniqueThingName" \
--policy-document "file://~/policies/jobs_test_thing_policy.json"
```

Wenn die Richtlinie erstellt wurde, gibt der Befehl eine Antwort wie die folgende zurück:

```
{
    "policyName": "JobTestPolicyFor<uniqueThingName>",
    "policyArn": "arn:aws:iot:us-west-2:57EXAMPLE833:policy/
JobTestPolicyFor<uniqueThingName>",
    "policyDocument": "{\n\"Version\": \"2012-10-17\",\n\"Statement\": [\n{\n
\"Effect\": \"Allow\",\n\"Action\": [\n\"iot:Connect\"\n],\n\"Resource\":
 [\n\"arn:aws:iot:us-west-2:57EXAMPLE833:client/PubSubTestThing\"\n]\n},\n{\n
\"Effect\": \"Allow\",\n\"Action\": [\n\"iot:Publish\"\n],\n\"Resource\":
 [\n\"arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/pubtopic\"\n]\n},\n{\n
\"Effect\": \"Allow\",\n\"Action\": [\n\"iot:Subscribe\"\n],\n\"Resource\": [\n
\"arn:aws:iot:us-west-2:57EXAMPLE833:topicfilter/test/dc/subtopic\"\n]\n},\n{\n
\"Effect\": \"Allow\",\n\"Action\": [\n\"iot:Receive\"\n],\n\"Resource\": [\n
\"arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/*\"\n]\n}\n]\n}\n",
    "policyVersionId": "1"
```

5. Ersetzen *uniqueThingName* mit dem Ding-Namen für das Gerät und *certificateArn* mit dem `certificateArn` Wert, den Sie weiter oben in diesem Abschnitt für dieses Gerät gespeichert haben, und führen Sie dann diesen Befehl aus, um die Richtlinie an das Gerätezertifikat anzuhängen.

   ```
   aws iot attach-policy \
   --policy-name "JobTestPolicyFor<uniqueThingName>" \
   --target "<certificateArn>"
   ```

   Bei erfolgreicher Ausführung gibt dieser Befehl nichts zurück.

6. Ersetzen *uniqueThingName* durch den Ding-Namen für das Gerät *certificateArn* ersetzen Sie ihn durch den `certificateArn` Wert, den Sie weiter oben in diesem Abschnitt gespeichert haben, und führen Sie dann diesen Befehl aus, um das Gerätezertifikat an die AWS IoT Ding-Ressource anzuhängen.

   ```
   aws iot attach-thing-principal \
   --thing-name "<uniqueThingName>" \
   --principal "<certificateArn>"
   ```

   Bei erfolgreicher Ausführung gibt dieser Befehl nichts zurück.

Nachdem Sie Ihren Raspberry Pi erfolgreich bereitgestellt haben, können Sie diesen Abschnitt für einen anderen Raspberry Pi in Ihrem Test wiederholen oder, falls alle Geräte bereitgestellt wurden, mit the section called “Konfigurieren Sie den Geräteclient für die Ausführung von Jobs” fortfahren.

Konfigurieren Sie den AWS IoT Geräteclient so, dass er den Job-Agent ausführt

Mit diesem Verfahren wird eine Konfigurationsdatei für den AWS IoT Geräteclient erstellt, um den Job-Agenten auszuführen:.

Hinweis: Wenn Sie mehr als ein Gerät vorbereiten, muss dieses Verfahren auf jedem Gerät durchgeführt werden.

So erstellen Sie die Konfigurationsdatei zum Testen des AWS IoT Geräteclients:

1. Gehen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, folgendermaßen vor:

   a. Öffnen Sie einen Texteditor, z. B. `nano`.

   b. Kopieren Sie dieses JSON Dokument und fügen Sie es in Ihren geöffneten Texteditor ein.

```
{
  "endpoint": "a3qEXAMPLEaffp-ats.iot.us-west-2.amazonaws.com",
  "cert": "~/certs/jobs/device.pem.crt",
  "key": "~/certs/jobs/private.pem.key",
  "root-ca": "~/certs/AmazonRootCA1.pem",
  "thing-name": "uniqueThingName",
  "logging": {
    "enable-sdk-logging": true,
    "level": "DEBUG",
    "type": "STDOUT",
    "file": ""
  },
  "jobs": {
    "enabled": true,
    "handler-directory": ""
  },
  "tunneling": {
    "enabled": false
  },
  "device-defender": {
    "enabled": false,
    "interval": 300
```

```
  },
  "fleet-provisioning": {
    "enabled": false,
    "template-name": "",
    "template-parameters": "",
    "csr-file": "",
    "device-key": ""
  },
  "samples": {
    "pub-sub": {
      "enabled": false,
      "publish-topic": "",
      "publish-file": "",
      "subscribe-topic": "",
      "subscribe-file": ""
    }
  },
  "config-shadow": {
    "enabled": false
  },
  "sample-shadow": {
    "enabled": false,
    "shadow-name": "",
    "shadow-input-file": "",
    "shadow-output-file": ""
  }
}
```

c. Ersetzen Sie das *endpoint* Wert durch den Endpunktwert der Gerätedaten für Ihren AWS-Konto , den Sie in gefunden habenthe section called “Stellen Sie Ihr Gerät bereit in AWS IoT Core”.

d. Ersetzen *uniqueThingName* mit dem Dingnamen, den Sie für dieses Gerät verwendet haben.

e. Speichern Sie die Datei als **~/dc-configs/dc-jobs-config.json** in Ihrem Texteditor.

2. Führen Sie diesen Befehl aus, um die Dateiberechtigungen der neuen Konfigurationsdatei festzulegen.

```
chmod 644 ~/dc-configs/dc-jobs-config.json
```

Sie werden den MQTTTestclient für diesen Test nicht verwenden. Das Gerät tauscht zwar auftragsbezogene MQTT Nachrichten mit AWS IoT, Nachrichten über den Auftragsfortschritt werden jedoch nur mit dem Gerät ausgetauscht, auf dem der Job ausgeführt wird. Da Nachrichten über den Auftragsstatus nur mit dem Gerät ausgetauscht werden, auf dem der Job ausgeführt wird, können Sie sie nicht von einem anderen Gerät aus abonnieren, z. B. von der AWS IoT Konsole aus.

Nachdem Sie die Konfigurationsdatei gespeichert haben, können Sie mit the section called “IoT-Job erstellen und ausführen” fortfahren.

## Erstellen Sie den Job AWS IoT mit dem AWS IoT Geräteclient und führen Sie ihn aus

Mit den Verfahren in diesem Abschnitt werden ein Jobdokument und eine AWS IoT Jobressource erstellt. Nachdem Sie die Auftragsressource erstellt haben, wird das Auftragsdokument an die angegebenen Auftragsziele AWS IoT gesendet, auf die ein Job-Agent das Auftragsdokument auf das Gerät oder den Client überträgt.

Verfahren in diesem Abschnitt

- Erstellen und speichern Sie das Jobdokument für den IoT-Job
- Führen Sie einen Job AWS IoT für ein IoT-Gerät aus

### Erstellen und speichern Sie das Jobdokument für den IoT-Job

Mit diesem Verfahren wird ein einfaches Auftragsdokument erstellt, das in eine AWS IoT Auftragsressource aufgenommen werden kann. In diesem Jobdokument wird „Hallo Welt!“ auf dem Jobziel angezeigt.

So erstellen und speichern Sie ein Jobdokument:

1. Wählen Sie den Amazon-S3-Bucket aus, in dem Sie Ihr Jobdokument speichern möchten. Wenn Sie nicht über einen vorhandenen Amazon-S3-Bucket verfügen, den Sie verwenden können, müssen Sie einen erstellen. Weitere Informationen zum Erstellen von Amazon-S3-Buckets finden Sie unterErste Schritte mit Amazon S3.
2. Erstellen und Speichern des Jobdokuments für diesen Job

   a. Öffnen Sie auf Ihrem lokalen Host-Computer einen Texteditor.

   b. Kopieren Sie den folgenden Text und fügen Sie ihn in den Editor ein.

```
{
```

```
    "operation": "echo",
    "args": ["Hello world!"]
}
```

c. Speichern Sie auf dem lokalen Host-Computer den Inhalt des Editors in einer Datei mit dem Namen **`hello-world-job.json`**.

d. Vergewissern Sie sich, dass die Datei korrekt gespeichert wurde. Einige Texteditoren fügen `.txt` beim Speichern einer Textdatei automatisch an den Dateinamen an. Wenn Ihr Editor `.txt` an den Dateinamen angehängt hat, korrigieren Sie den Dateinamen, bevor Sie fortfahren.

3. Ersetzen Sie das *`path_to_file`* durch den Pfad zu**`hello-world-job.json`**, falls er sich nicht in Ihrem aktuellen Verzeichnis befindet, ersetzen Sie *`s3_bucket_name`* mit dem Amazon S3 S3-Bucket-Pfad zu dem von Ihnen ausgewählten Bucket und führen Sie dann diesen Befehl aus, um Ihr Jobdokument in den Amazon S3 S3-Bucket einzufügen.

```
aws s3api put-object \
--key hello-world-job.json \
--body path_to_file/hello-world-job.json --bucket s3_bucket_name
```

Das Job-DokumentURL, das das Job-Dokument identifiziert, das Sie in Amazon S3 gespeichert haben, wird bestimmt, indem Sie das *`s3_bucket_name`* and *`AWS_region`* im FolgendenURL. Notieren Sie das ErgebnisURL, um es später als *`job_document_path`*

```
https://s3_bucket_name.s3.AWS_Region.amazonaws.com/hello-world-job.json
```

> **Note**
>
> AWS Die Sicherheit verhindert, dass Sie dies URL außerhalb Ihres Computers öffnen können AWS-Konto, z. B. mithilfe eines Browsers. Das URL wird standardmäßig von der AWS IoT Job-Engine verwendet, die Zugriff auf die Datei hat. In einer Produktionsumgebung müssen Sie sicherstellen, dass Ihre AWS IoT -Services berechtigt sind, auf die in Amazon S3 gespeicherten Jobdokumente zuzugreifen.

Nachdem Sie die Auftragsdokumente gespeichert habenURL, fahren Sie fort mitthe section called “Job für ein einzelnes Gerät ausführen”.

Führen Sie einen Job AWS IoT für ein IoT-Gerät aus

Die Verfahren in diesem Abschnitt starten den AWS IoT Geräteclient auf Ihrem Raspberry Pi, um den Job-Agenten auf dem Gerät auszuführen und auf die Ausführung von Jobs zu warten. Außerdem wird eine Jobressource in erstellt AWS IoT, die den Job an Ihr IoT-Gerät sendet und dort ausgeführt wird.

> **Note**
>
> Dieses Verfahren führt einen Job nur auf einem einzigen Gerät aus.

So starten Sie den Job-Agenten auf Ihrem Raspberry Pi:

1. Führen Sie im Terminalfenster auf Ihrem lokalen Host-Computer, der mit Ihrem Raspberry Pi verbunden ist, diesen Befehl aus, um den AWS IoT Geräteclient zu starten.

   ```
   cd ~/aws-iot-device-client/build
   ./aws-iot-device-client --config-file ~/dc-configs/dc-jobs-config.json
   ```

2. Bestätigen Sie im Terminalfenster, dass der AWS IoT Geräteclient diese Meldungen anzeigt

   ```
   2021-11-15T18:45:56.708Z [INFO]  {Main.cpp}: Jobs is enabled
                          .
                          .
                          .
   2021-11-15T18:45:56.708Z [INFO]  {Main.cpp}: Client base has been notified that
    Jobs has started
   2021-11-15T18:45:56.708Z [INFO]  {JobsFeature.cpp}: Running Jobs!
   2021-11-15T18:45:56.708Z [DEBUG] {JobsFeature.cpp}: Attempting to subscribe to
    startNextPendingJobExecution accepted and rejected
   2021-11-15T18:45:56.708Z [DEBUG] {JobsFeature.cpp}: Attempting to subscribe to
    nextJobChanged events
   2021-11-15T18:45:56.708Z [DEBUG] {JobsFeature.cpp}: Attempting to subscribe to
    updateJobExecutionStatusAccepted for jobId +
   2021-11-15T18:45:56.738Z [DEBUG] {JobsFeature.cpp}: Ack received for
    SubscribeToUpdateJobExecutionAccepted with code {0}
   2021-11-15T18:45:56.739Z [DEBUG] {JobsFeature.cpp}: Attempting to subscribe to
    updateJobExecutionStatusRejected for jobId +
   2021-11-15T18:45:56.753Z [DEBUG] {JobsFeature.cpp}: Ack received for
    SubscribeToNextJobChanged with code {0}
   2021-11-15T18:45:56.760Z [DEBUG] {JobsFeature.cpp}: Ack received for
    SubscribeToStartNextJobRejected with code {0}
   ```

```
2021-11-15T18:45:56.776Z [DEBUG] {JobsFeature.cpp}: Ack received for
 SubscribeToStartNextJobAccepted with code {0}
2021-11-15T18:45:56.776Z [DEBUG] {JobsFeature.cpp}: Ack received for
 SubscribeToUpdateJobExecutionRejected with code {0}
2021-11-15T18:45:56.777Z [DEBUG] {JobsFeature.cpp}: Publishing
 startNextPendingJobExecutionRequest
2021-11-15T18:45:56.785Z [DEBUG] {JobsFeature.cpp}: Ack received for
 StartNextPendingJobPub with code {0}
2021-11-15T18:45:56.785Z [INFO]  {JobsFeature.cpp}: No pending jobs are scheduled,
 waiting for the next incoming job
```

3. Wenn Sie im Terminalfenster diese Meldung sehen, fahren Sie mit dem nächsten Verfahren fort und erstellen Sie die Jobressource. Beachten Sie, dass dies möglicherweise nicht der letzte Eintrag in der Liste ist.

```
2021-11-15T18:45:56.785Z [INFO]  {JobsFeature.cpp}: No pending jobs are scheduled,
 waiting for the next incoming job
```

Um eine AWS IoT Jobressource zu erstellen

1. Auf Ihrem lokalen Host-Computer:

   a. Ersetzen *job_document_url* mit dem Jobdokument URL vonthe section called “Jobdokument erstellen und speichern”.

   b. Ersetzen *thing_arn* mit ARN der Thing-Ressource, die Sie für Ihr Gerät erstellt haben, und führen Sie dann diesen Befehl aus.

   ```
   aws iot create-job \
   --job-id hello-world-job-1 \
   --document-source "job_document_url" \
   --targets "thing_arn" \
   --target-selection SNAPSHOT
   ```

   Bei Erfolg gibt der Befehl ein Ergebnis wie dieses zurück:

   ```
   {
     "jobArn": "arn:aws:iot:us-west-2:57EXAMPLE833:job/hello-world-job-1",
     "jobId": "hello-world-job-1"
   }
   ```

2. Im Terminalfenster sollten Sie eine Ausgabe vom AWS IoT Geräteclient wie folgt sehen.

```
2021-11-15T18:02:26.688Z [INFO]  {JobsFeature.cpp}: No pending jobs are scheduled,
 waiting for the next incoming job
2021-11-15T18:10:24.890Z [DEBUG] {JobsFeature.cpp}: Job ids differ
2021-11-15T18:10:24.890Z [INFO]  {JobsFeature.cpp}: Executing job: hello-world-
job-1
2021-11-15T18:10:24.890Z [DEBUG] {JobsFeature.cpp}: Attempting to update job
 execution status!
2021-11-15T18:10:24.890Z [DEBUG] {JobsFeature.cpp}: Not including stdout with the
 status details
2021-11-15T18:10:24.890Z [DEBUG] {JobsFeature.cpp}: Not including stderr with the
 status details
2021-11-15T18:10:24.890Z [DEBUG] {JobsFeature.cpp}: Assuming executable is in PATH
2021-11-15T18:10:24.890Z [INFO]  {JobsFeature.cpp}: About to execute: echo Hello
 world!
2021-11-15T18:10:24.890Z [DEBUG] {Retry.cpp}: Retryable function starting, it will
 retry until success
2021-11-15T18:10:24.890Z [DEBUG] {JobsFeature.cpp}: Created EphermalPromise for
 ClientToken 3TEWba9Xj6 in the updateJobExecution promises map
2021-11-15T18:10:24.890Z [DEBUG] {JobEngine.cpp}: Child process now running
2021-11-15T18:10:24.890Z [DEBUG] {JobEngine.cpp}: Child process about to call
 execvp
2021-11-15T18:10:24.890Z [DEBUG] {JobEngine.cpp}: Parent process now running, child
 PID is 16737
2021-11-15T18:10:24.891Z [DEBUG] {16737}: Hello world!
2021-11-15T18:10:24.891Z [DEBUG] {JobEngine.cpp}: JobEngine finished waiting for
 child process, returning 0
2021-11-15T18:10:24.891Z [INFO]  {JobsFeature.cpp}: Job exited with status: 0
2021-11-15T18:10:24.891Z [INFO]  {JobsFeature.cpp}: Job executed successfully!
2021-11-15T18:10:24.891Z [DEBUG] {JobsFeature.cpp}: Attempting to update job
 execution status!
2021-11-15T18:10:24.891Z [DEBUG] {JobsFeature.cpp}: Not including stdout with the
 status details
2021-11-15T18:10:24.891Z [DEBUG] {JobsFeature.cpp}: Not including stderr with the
 status details
2021-11-15T18:10:24.892Z [DEBUG] {Retry.cpp}: Retryable function starting, it will
 retry until success
2021-11-15T18:10:24.892Z [DEBUG] {JobsFeature.cpp}: Created EphermalPromise for
 ClientToken GmQ0HTzWGg in the updateJobExecution promises map
2021-11-15T18:10:24.905Z [DEBUG] {JobsFeature.cpp}: Ack received for
 PublishUpdateJobExecutionStatus with code {0}
```

```
2021-11-15T18:10:24.905Z [DEBUG] {JobsFeature.cpp}: Removing ClientToken 3TEWba9Xj6
 from the updateJobExecution promises map
2021-11-15T18:10:24.905Z [DEBUG] {JobsFeature.cpp}: Success response after
 UpdateJobExecution for job hello-world-job-1
2021-11-15T18:10:24.917Z [DEBUG] {JobsFeature.cpp}: Ack received for
 PublishUpdateJobExecutionStatus with code {0}
2021-11-15T18:10:24.918Z [DEBUG] {JobsFeature.cpp}: Removing ClientToken GmQ0HTzWGg
 from the updateJobExecution promises map
2021-11-15T18:10:24.918Z [DEBUG] {JobsFeature.cpp}: Success response after
 UpdateJobExecution for job hello-world-job-1
2021-11-15T18:10:25.861Z [INFO]  {JobsFeature.cpp}: No pending jobs are scheduled,
 waiting for the next incoming job
```

3. Während der AWS IoT Geräteclient läuft und auf einen Job wartet, können Sie einen anderen Job einreichen, indem Sie den `job-id` Wert ändern und den create-job aus Schritt 1 stammenden Vorgang erneut ausführen.

Wenn Sie mit der Ausführung der Jobs fertig sind, geben Sie im Terminalfenster ^C (Strg-C) ein, um den AWS IoT Device Client zu beenden.

## Tutorial: Aufräumen nach dem Ausführen der AWS IoT Device Client-Tutorials

Die Verfahren in diesem Tutorial führen Sie durch das Entfernen der Dateien und Ressourcen, die Sie beim Abschluss der Tutorials in diesem Lernpfad erstellt haben.

Verfahren in diesem Tutorial

- Schritt 1: Aufräumen Ihrer Geräte nach dem Erstellen von Demos mit dem AWS IoT Device Client
- Schritt 2: Aufräumen Ihrer Demos AWS-Konto nach dem Erstellen mit dem AWS IoT Device Client

### Schritt 1: Aufräumen Ihrer Geräte nach dem Erstellen von Demos mit dem AWS IoT Device Client

In diesem Tutorial werden zwei Optionen beschrieben, wie Sie die microSD-Karte bereinigen können, nachdem Sie die Demos in diesem Lernpfad erstellt haben. Wählen Sie die Option, die das Sicherheitsniveau bietet, das Sie benötigen.

Beachten Sie, dass durch das Reinigen der microSD-Karte des Geräts keine AWS IoT Ressourcen entfernt werden, die Sie erstellt haben. Um die AWS IoT Ressourcen zu bereinigen, nachdem Sie

die microSD-Karte des Geräts gereinigt haben, sollten Sie das Tutorial unter the section called “Aufräumen nach dem Erstellen von Demos mit dem AWS IoT Device Client” lesen.

Option 1: Aufräumen durch Neuschreiben der microSD-Karte

Die einfachste und gründlichste Methode, die microSD-Karte nach Abschluss der Tutorials in diesem Lernpfad zu reinigen, besteht darin, die microSD-Karte mit einer gespeicherten Bilddatei zu überschreiben, die Sie bei der ersten Vorbereitung Ihres Geräts erstellt haben.

Bei diesem Verfahren wird der lokale Host-Computer verwendet, um ein gespeichertes microSD-Karten-Image auf eine microSD-Karte zu schreiben.

> **Note**
>
> Wenn Ihr Gerät keinen Wechseldatenträger für sein Betriebssystem verwendet, lesen Sie das Verfahren für dieses Gerät.

Um ein neues Bild auf die microSD-Karte zu schreiben

1. Suchen Sie auf Ihrem lokalen Host-Computer nach dem gespeicherten microSD-Karten-Image, das Sie auf Ihre microSD-Karte schreiben möchten.
2. Stecken Sie Ihre microSD-Karte in den lokalen Host-Computer.
3. Schreiben Sie die ausgewählte Bilddatei mit einem SD-Karten-Imaging-Tool auf die microSD-Karte.
4. Nachdem Sie das Raspberry Pi OS-Image auf die microSD-Karte geschrieben haben, werfen Sie die microSD-Karte aus und entfernen Sie sie sicher vom lokalen Host-Computer.

Ihre microSD-Karte ist einsatzbereit.

Option 2: Aufräumen durch Löschen von Benutzerverzeichnissen

Um die microSD-Karte nach Abschluss der Tutorials zu reinigen, ohne das microSD-Karten-Image neu zu schreiben, können Sie die Benutzerverzeichnisse einzeln löschen. Dies ist nicht so gründlich wie das Neuschreiben der microSD-Karte aus einem gespeicherten Image, da dabei keine möglicherweise installierten Systemdateien entfernt werden.

Wenn das Entfernen der Benutzerverzeichnisse für Ihre Bedürfnisse ausreichend ist, können Sie wie folgt vorgehen.

So löschen Sie die Benutzerverzeichnisse dieses Lernpfads von Ihrem Gerät

1. Führen Sie diese Befehle aus, um die Benutzerverzeichnisse, Unterverzeichnisse und alle zugehörigen Dateien, die in diesem Lernpfad erstellt wurden, in dem mit Ihrem Gerät verbundenen Terminalfenster zu löschen.

   > **Note**
   >
   > Nachdem Sie diese Verzeichnisse und Dateien gelöscht haben, können Sie die Demos nicht ausführen, ohne die Tutorials erneut abgeschlossen zu haben.

   ```
   rm -Rf ~/dc-configs
   rm -Rf ~/policies
   rm -Rf ~/messages
   rm -Rf ~/certs
   rm -Rf ~/.aws-iot-device-client
   ```

2. Führen Sie diese Befehle aus, um die Quellverzeichnisse und Dateien der Anwendung in dem mit Ihrem Gerät verbundenen Terminalfenster zu löschen.

   > **Note**
   >
   > Mit diesen Befehlen werden keine Programme deinstalliert. Sie entfernen nur die Quelldateien, die zum Erstellen und Installieren verwendet wurden. Nachdem Sie diese Dateien gelöscht haben, funktionieren der AWS CLI und der AWS IoT Device Client möglicherweise nicht.

   ```
   rm -Rf ~/aws-cli
   rm -Rf ~/aws
   rm -Rf ~/aws-iot-device-client
   ```

## Schritt 2: Aufräumen Ihrer Demos AWS-Konto nach dem Erstellen mit dem AWS IoT Device Client

Diese Verfahren helfen Ihnen dabei, die AWS Ressourcen zu identifizieren und zu entfernen, die Sie beim Abschluss der Tutorials in diesem Lernpfad erstellt haben.

## AWS IoTRessourcen bereinigen

Dieses Verfahren hilft Ihnen dabei, die AWS IoT Ressourcen zu identifizieren und zu entfernen, die Sie beim Abschluss der Tutorials in diesem Lernpfad erstellt haben.

AWS IoTRessourcen, die in diesem Lernpfad erstellt wurden

| Tutorial | Ressource für Dinge | Politische Ressource |
|---|---|---|
| the section called “Installation und Konfiguration des IoT-Geräteclients” | DevCliTestThing | DevCliTestThingPolicy |
| the section called “Kommunizieren Sie mit dem Geräteclient über MQTT” | PubSubTestThing | PubSubTestThingPolicy |
| the section called “Führen Sie IoT-Jobs mit dem Device Client aus” | benutzerdefiniert (es könnte mehrere geben) | benutzerdefiniert (es könnte mehrere geben) |

Um die AWS IoT Ressourcen zu löschen, gehen Sie für jede von Ihnen erstellte Dingressource wie folgt vor:

1. Ersetzen Sie es *thing_name* durch den Namen der Dingressource, die Sie löschen möchten, und führen Sie dann diesen Befehl aus, um die an die Dingressource angehängten Zertifikate vom lokalen Hostcomputer aus aufzulisten.

   ```
   aws iot list-thing-principals --thing-name thing_name
   ```

   Dieser Befehl gibt eine Antwort wie diese zurück, die die angehängten Zertifikate auflistet*thing_name*. In den meisten Fällen wird die Liste nur ein Zertifikat enthalten.

   ```
   {
       "principals": [
           "arn:aws:iot:us-
   west-2:57EXAMPLE833:cert/23853eea3cf0edc7f8a69c74abeafa27b2b52823cab5b3e156295e94b26ae8ac"
       ]
   }
   ```

2. Gehen Sie für jedes Zertifikat, das im vorherigen Befehl aufgeführt wurde, wie folgt vor:

   a. Ersetzen Sie *certificate_ID* durch die Zertifikats-ID aus dem vorherigen Befehl. Die Zertifikat-ID besteht aus den alphanumerischen Zeichen, die `cert/` in dem vom vorherigen Befehl zurückgegebenen ARN folgen. Führen Sie dann diesen Befehl aus, um das Zertifikat zu inaktivieren.

   ```
   aws iot update-certificate --new-status INACTIVE --certificate-
   id certificate_ID
   ```

   Bei Erfolg gibt dieser Befehl nichts zurück.

   b. Ersetzen Sie es *certificate_ARN* durch den Zertifikat-ARN aus der Liste der zuvor zurückgegebenen Zertifikate, und führen Sie dann diesen Befehl aus, um die an dieses Zertifikat angehängten Richtlinien aufzulisten.

   ```
   aws iot list-attached-policies --target certificate_ARN
   ```

   Dieser Befehl gibt eine Antwort wie diese zurück, in der die an das Zertifikat angehängten Richtlinien aufgeführt sind. In den meisten Fällen wird die Liste nur eine Richtlinie enthalten.

   ```
   {
       "policies": [
           {
               "policyName": "DevCliTestThingPolicy",
               "policyArn": "arn:aws:iot:us-west-2:57EXAMPLE833:policy/
   DevCliTestThingPolicy"
           }
       ]
   }
   ```

   c. Gehen Sie für jede dem Zertifikat beigefügte Richtlinie wie folgt vor:

      i. Ersetzen Sie *policy_name* durch den `policyName` Wert aus dem vorherigen Befehl, *certificate_ARN* ersetzen Sie ihn durch den ARN des Zertifikats, und führen Sie dann diesen Befehl aus, um die Richtlinie vom Zertifikat zu trennen.

      ```
      aws iot detach-policy --policy-name policy_name --target certificate_ARN
      ```

      Bei Erfolg gibt dieser Befehl nichts zurück.

ii. Ersetzen Sie *policy_name* durch den `policyName` Wert, und führen Sie dann diesen Befehl aus, um festzustellen, ob die Richtlinie an weitere Zertifikate angehängt ist.

```
aws iot list-targets-for-policy --policy-name policy_name
```

Wenn der Befehl eine leere Liste wie diese zurückgibt, ist die Richtlinie an kein Zertifikat angehängt und Sie führen weiterhin die Richtlinienversionen auf. Wenn der Richtlinie noch Zertifikate beigefügt sind, fahren Sie mit dem detach-thing-principal Schritt fort.

```
{
    "targets": []
}
```

iii. Ersetzen Sie ihn *policy_name* durch den `policyName` Wert, und führen Sie dann diesen Befehl aus, um nach Richtlinienversionen zu suchen. Um die Richtlinie zu löschen, darf sie nur über eine Version verfügen.

```
aws iot list-policy-versions --policy-name policy_name
```

Wenn die Richtlinie nur eine Version hat, wie in diesem Beispiel, können Sie mit dem delete-policy Schritt fortfahren und die Richtlinie jetzt löschen.

```
{
    "policyVersions": [
        {
            "versionId": "1",
            "isDefaultVersion": true,
            "createDate": "2021-11-18T01:02:46.778000+00:00"
        }
    ]
}
```

Wenn die Richtlinie mehr als eine Version hat, wie in diesem Beispiel, `false` müssen die Richtlinienversionen mit einem `isDefaultVersion` Wert von gelöscht werden, bevor die Richtlinie gelöscht werden kann.

```
{
    "policyVersions": [
        {
```

```
            "versionId": "2",
            "isDefaultVersion": true,
            "createDate": "2021-11-18T01:52:04.423000+00:00"
        },
        {
            "versionId": "1",
            "isDefaultVersion": false,
            "createDate": "2021-11-18T01:30:18.083000+00:00"
        }
    ]
}
```

Wenn Sie eine Richtlinienversion löschen müssen, ersetzen *policy_name* Sie sie durch den `policyName` Wert, *version_ID* ersetzen Sie sie durch den `versionId` Wert aus dem vorherigen Befehl und führen Sie dann diesen Befehl aus, um eine Richtlinienversion zu löschen.

```
aws iot delete-policy-version --policy-name policy_name --policy-version-
id version_ID
```

Bei Erfolg gibt dieser Befehl nichts zurück.

Nachdem Sie eine Richtlinienversion gelöscht haben, wiederholen Sie diesen Schritt, bis die Richtlinie nur noch eine Richtlinienversion enthält.

iv. Ersetzen Sie *policy_name* durch den `policyName` Wert, und führen Sie dann diesen Befehl aus, um die Richtlinie zu löschen.

```
aws iot delete-policy --policy-name policy_name
```

d. *thing_name*Ersetzen Sie es durch den Namen des Dings, *certificate_ARN* ersetzen Sie es durch den ARN des Zertifikats und führen Sie dann diesen Befehl aus, um das Zertifikat von der Dingressource zu trennen.

```
aws iot detach-thing-principal --thing-name thing_name --
principal certificate_ARN
```

Bei Erfolg gibt dieser Befehl nichts zurück.

e. Ersetzen Sie *certificate_ID* durch die Zertifikats-ID aus dem vorherigen Befehl. Die Zertifikat-ID besteht aus den alphanumerischen Zeichen, die `cert/` in dem vom

vorherigen Befehl zurückgegebenen ARN folgen. Führen Sie dann diesen Befehl aus, um die Zertifikatsressource zu löschen.

```
aws iot delete-certificate --certificate-id certificate_ID
```

Bei Erfolg gibt dieser Befehl nichts zurück.

3. Ersetzen Sie es *thing_name* durch den Namen des Dings und führen Sie dann diesen Befehl aus, um das Ding zu löschen.

```
aws iot delete-thing --thing-name thing_name
```

Bei Erfolg gibt dieser Befehl nichts zurück.

AWSRessourcen bereinigen

Dieses Verfahren hilft Ihnen dabei, andere AWS Ressourcen zu identifizieren und zu entfernen, die Sie beim Abschluss der Tutorials in diesem Lernpfad erstellt haben.

Andere AWS Ressourcen, die in diesem Lernpfad erstellt wurden

| Tutorial | Ressourcentyp | Name oder ID der Ressource |
|---|---|---|
| the section called “Führen Sie IoT-Jobs mit dem Device Client aus” | Amazon S3-Objekt | hello-world-job.json |
| the section called “Führen Sie IoT-Jobs mit dem Device Client aus” | AWS IoTRessourcen für Jobs | benutzerdefiniert |

Um die in diesem Lernpfad erstellten AWS Ressourcen zu löschen

1. Um die in diesem Lernpfad geschaffenen Jobs zu löschen

   a. Führen Sie diesen Befehl aus, um die Jobs in Ihrem aufzulistenAWS-Konto.

```
aws iot list-jobs
```

Der Befehl gibt eine Liste der AWS IoT Jobs in Ihrem zurück AWS-Konto und AWS-Region das sieht so aus.

```
{
    "jobs": [
        {
            "jobArn": "arn:aws:iot:us-west-2:57EXAMPLE833:job/hello-world-
job-2",
            "jobId": "hello-world-job-2",
            "targetSelection": "SNAPSHOT",
            "status": "COMPLETED",
            "createdAt": "2021-11-16T23:40:36.825000+00:00",
            "lastUpdatedAt": "2021-11-16T23:40:41.375000+00:00",
            "completedAt": "2021-11-16T23:40:41.375000+00:00"
        },
        {
            "jobArn": "arn:aws:iot:us-west-2:57EXAMPLE833:job/hello-world-
job-1",
            "jobId": "hello-world-job-1",
            "targetSelection": "SNAPSHOT",
            "status": "COMPLETED",
            "createdAt": "2021-11-16T23:35:26.381000+00:00",
            "lastUpdatedAt": "2021-11-16T23:35:29.239000+00:00",
            "completedAt": "2021-11-16T23:35:29.239000+00:00"
        }
    ]
}
```

b. Ersetzen Sie für jeden Job, den Sie in der Liste als einen Job erkennen, den Sie in diesem Lernpfad erstellt haben, *`jobId`* durch den `jobId` Wert des zu löschenden Jobs, und führen Sie dann diesen Befehl aus, um einen AWS IoT Job zu löschen.

```
aws iot delete-job --job-id jobId
```

Wenn der Befehl erfolgreich ist, gibt er nichts zurück.

2. Um die Jobdokumente zu löschen, die Sie in einem Amazon S3-Bucket in diesem Lernpfad gespeichert haben.

a. Ersetzen Sie es *bucket* durch den Namen des Buckets, das Sie verwendet haben, und führen Sie dann diesen Befehl aus, um die Objekte im Amazon S3-Bucket aufzulisten, die Sie verwendet haben.

```
aws s3api list-objects --bucket bucket
```

Der Befehl gibt eine Liste der Amazon S3-Objekte im Bucket zurück, die wie folgt aussieht.

```
{
    "Contents": [
        {
            "Key": "hello-world-job.json",
            "LastModified": "2021-11-18T03:02:12+00:00",
            "ETag": "\"868c8bc3f56b5787964764d4b18ed5ef\"",
            "Size": 54,
            "StorageClass": "STANDARD",
            "Owner": {
                "DisplayName": "EXAMPLE",
                "ID":
 "e9e3d6ec1EXAMPLEf5bfb5e6bd0a2b6ed03884d1ed392a82ad011c144736a4ee"
            }
        },
        {
            "Key": "iot_job_firmware_update.json",
            "LastModified": "2021-04-13T21:57:07+00:00",
            "ETag": "\"7c68c591949391791ecf625253658c61\"",
            "Size": 66,
            "StorageClass": "STANDARD",
            "Owner": {
                "DisplayName": "EXAMPLE",
                "ID":
 "e9e3d6ec1EXAMPLEf5bfb5e6bd0a2b6ed03884d1ed392a82ad011c144736a4ee"
            }
        },
        {
            "Key": "order66.json",
            "LastModified": "2021-04-13T21:57:07+00:00",
            "ETag": "\"bca60d5380b88e1a70cc27d321caba72\"",
            "Size": 29,
            "StorageClass": "STANDARD",
            "Owner": {
```

```
                "DisplayName": "EXAMPLE",
                "ID":
 "e9e3d6ec1EXAMPLEf5bfb5e6bd0a2b6ed03884d1ed392a82ad011c144736a4ee"
            }
        }
    ]
}
```

b. Ersetzen Sie für jedes Objekt, das Sie aus der Liste als Objekt erkennen, das Sie in diesem Lernpfad erstellt haben, *bucket* durch den Bucket-Namen und *key* durch den Schlüsselwert des zu löschenden Objekts, und führen Sie dann diesen Befehl aus, um ein Amazon S3-Objekt zu löschen.

```
aws s3api delete-object --bucket bucket --key key
```

Wenn der Befehl erfolgreich ist, gibt er nichts zurück.

Nachdem Sie alle AWS Ressourcen und Objekte gelöscht haben, die Sie während des Abschlusses dieses Lernpfads erstellt haben, können Sie von vorne beginnen und die Tutorials wiederholen.

# Mit dem AWS IoT Gerät Lösungen entwickeln SDKs

Die Tutorials in diesem Abschnitt führen Sie durch die Schritte zur Entwicklung einer IoT-Lösung, die mithilfe von in einer Produktionsumgebung eingesetzt werden kann AWS IoT.

Diese Tutorials können mehr Zeit in Anspruch nehmen als die Anleitungen im Abschnitt über, the section called “Demos mit dem AWS IoT Device Client erstellen” da sie das AWS IoT Gerät verwenden SDKs und die angewandten Konzepte ausführlicher erläutern, um Ihnen bei der Entwicklung sicherer und zuverlässiger Lösungen zu helfen.

## Fangen Sie an, Lösungen mit dem AWS IoT Gerät zu entwickeln SDKs

Diese Tutorials führen Sie durch verschiedene AWS IoT Szenarien. Gegebenenfalls verwenden die Tutorials das AWS IoT Gerät SDKs.

Themen

- Tutorial: Ein Gerät mit AWS IoT Core dem AWS IoT Gerät verbinden SDK
- AWS IoT Regeln erstellen, um Gerätedaten an andere Dienste weiterzuleiten
- Beibehalten des Gerätestatus mit Geräteschatten, während das Gerät offline ist

- Tutorial: Erstellen eines benutzerdefinierten Autorisierers für AWS IoT Core
- Tutorial: Überwachung der Bodenfeuchte mit einem AWS IoT Raspberry Pi

# Tutorial: Ein Gerät mit AWS IoT Core dem AWS IoT Gerät verbinden SDK

In diesem Tutorial wird gezeigt, wie Sie ein Gerät anschließen, AWS IoT Core damit es Daten an und von dort senden und empfangen kann AWS IoT. Nachdem Sie dieses Tutorial abgeschlossen haben, wird Ihr Gerät so konfiguriert, dass es eine Verbindung herstellt, AWS IoT Core und Sie werden verstehen, wie Geräte miteinander kommunizieren AWS IoT.

Themen

- Voraussetzungen
- Bereiten Sie Ihr Gerät vor für AWS IoT
- Überprüfen Sie das MQTT Protokoll
- Sehen Sie sich die SDK Gerätebeispiel-App pubsub.py an
- Connect dein Gerät und kommuniziere mit AWS IoT Core
- Überprüfen Sie die Ergebnisse.
- Tutorial: Verwenden des AWS IoT Device SDK for Embedded C

## Voraussetzungen

Stellen Sie vor Beginn dieses Tutorials sicher, dass Sie über Folgendes verfügen:

- Erste Schritte mit AWS IoT Core Tutorials abgeschlossen haben.

  Wählen Sie im Abschnitt des besagten Tutorials, in dem Sie the section called “Konfigurieren Ihres Geräts” müssen, die Option the section called “Verbinden eines Raspberry Pi oder eines anderes Gerätes” für Ihr Gerät und verwenden Sie die Python-Sprachoptionen, um Ihr Gerät zu konfigurieren.

  > **Note**
  >
  > Lassen Sie das im besagten Tutorial verwendete Terminalfenster geöffnet, da Sie es auch in diesem Tutorial verwenden.

- Ein Gerät, auf dem AWS IoT Device SDK v2 für Python ausgeführt werden kann.

Dieses Tutorial zeigt anhand AWS IoT Core von Python-Codebeispielen, für die ein relativ leistungsfähiges Gerät erforderlich ist, wie Sie ein Gerät mit einem Gerät verbinden. Wenn Sie mit ressourcenbeschränkten Geräten arbeiten, funktionieren diese Codebeispiele möglicherweise nicht. In diesem Fall haben Sie möglicherweise mehr Erfolg mit dem the section called “Mit dem AWS IoT Device SDK for Embedded C” Tutorial.

- Sie haben die erforderlichen Informationen erhalten, um eine Verbindung mit dem Gerät herzustellen

  Um Ihr Gerät zu verbinden AWS IoT, benötigen Sie Informationen zum Namen des Objekts, zum Hostnamen und zur Portnummer.

  > **Note**
  >
  > Sie können auch eine benutzerdefinierte Authentifizierung verwenden, um Geräte mit zu verbinden AWS IoT Core. Die Verbindungsdaten, die Sie an Ihre Autorisierungs-Lambda-Funktion übergeben, hängen vom verwendeten Protokoll ab.

  - Name der Sache: Der Name der AWS IoT Sache, zu der Sie eine Verbindung herstellen möchten. Sie müssen sich als Ihr Gerät als AWS IoT Ding registriert haben. Weitere Informationen finden Sie unter Geräte verwalten mit AWS IoT.
  - Hostname: Der Hostname für den kontospezifischen IoT-Endpunkt.
  - Portnummer: Die Portnummer, zu der eine Verbindung hergestellt werden soll.

  Sie können die `configureEndpoint` Methode in AWS IoT Python verwendenSDK, um den Hostnamen und die Portnummer zu konfigurieren.

  ```
  myAWSIoTMQTTClient.configureEndpoint("random.iot.region.amazonaws.com", 8883)
  ```

## Bereiten Sie Ihr Gerät vor für AWS IoT

In Erste Schritte mit AWS IoT Core Tutorials haben Sie Ihr Gerät und Ihr AWS -Konto vorbereitet, sodass sie kommunizieren können. In diesem Abschnitt werden die Aspekte dieser Vorbereitung beschrieben, die für jede Geräteverbindung mit gelten AWS IoT Core.

Damit ein Gerät sich mit AWS IoT Core verbinden kann:

1. Benötigen Sie ein AWS-Konto.

   Das Verfahren unter Einrichten AWS-Konto beschreibt, wie Sie eine erstellen, AWS-Konto falls Sie noch keine haben.

2. In diesem Konto müssen Sie die folgenden AWS IoT Ressourcen für das Gerät in Ihrer Region AWS-Konto und Ihrer Region definiert haben.

   Das Verfahren unter AWS IoT Ressourcen erstellen beschreibt, wie Sie diese Ressourcen für das Gerät in Ihrem AWS-Konto und Ihrer Region erstellen.

   - Ein Gerätezertifikat, das bei AWS IoT registriert und zur Authentifizierung des Geräts aktiviert wurde.

     Das Zertifikat wird häufig mit einem AWS IoT -Objekt erstellt und an dieses angehängt. Ein Dingobjekt ist zwar nicht erforderlich, damit ein Gerät eine Verbindung herstellen kann AWS IoT, es stellt dem Gerät jedoch zusätzliche AWS IoT Funktionen zur Verfügung.

   - Eine dem Gerätezertifikat beigefügte Richtlinie, die es autorisiert, eine Verbindung herzustellen AWS IoT Core und alle gewünschten Aktionen auszuführen.

3. Eine Internetverbindung, die auf die Endpunkte des Geräts Ihres AWS-Konto s zugreifen kann.

   Die Geräteendpunkte werden unter beschrieben AWS IoT Gerätedaten und Dienstendpunkte und können auf der Einstellungsseite der AWS IoT Konsole eingesehen werden.

4. Kommunikationssoftware, wie sie vom AWS IoT Gerät SDKs bereitgestellt wird. Dieses Tutorial verwendet das AWS IoT Device SDK v2 für Python.

## Überprüfen Sie das MQTT Protokoll

Bevor wir über die Beispiel-App sprechen, ist es hilfreich, das MQTT Protokoll zu verstehen. Das MQTT Protokoll bietet einige Vorteile gegenüber anderen Netzwerkkommunikationsprotokollen, z. B. HTTP was es zu einer beliebten Wahl für IoT-Geräte macht. In diesem Abschnitt werden die wichtigsten Aspekte beschriebenMQTT, die für dieses Tutorial gelten. Informationen zum MQTT Vergleich mit finden Sie HTTP unterWählen Sie ein Anwendungsprotokoll für die Kommunikation mit Ihrem Gerät.

MQTTverwendet ein Kommunikationsmodell zum Veröffentlichen und Abonnieren

Das MQTT Protokoll verwendet ein publish/subscribe communication model with its host. This model differs from the request/response Modell, das verwendet. HTTP Mit MQTT bauen Geräte eine Sitzung

mit dem Host auf, der durch eine eindeutige Client-ID identifiziert wird. Zum Senden von Daten veröffentlichen die Geräte durch Themen identifizierte Nachrichten an einen Message Broker auf dem Host. Zum Empfangen von Nachrichten vom Message Broker abonnieren Geräte Themen, indem sie Themenfilter in Subscriber-Anfragen an den Message Broker senden.

MQTTunterstützt persistente Sitzungen

Der Message Broker empfängt Nachrichten von Geräten und veröffentlicht Nachrichten an Geräte, die diese abonniert haben. Mit persistenten Sitzungen – Sitzungen, die auch dann aktiv bleiben, wenn das initiierende Gerät getrennt ist – können Geräte Nachrichten abrufen, die während der Unterbrechung der Verbindung veröffentlicht wurden. Auf der Geräteseite werden Quality of Service Levels (QoS) MQTT unterstützt, die sicherstellen, dass der Host vom Gerät gesendete Nachrichten empfängt.

## Sehen Sie sich die SDK Gerätebeispiel-App pubsub.py an

In diesem Abschnitt wird die `pubsub.py` Beispiel-App von AWS IoT Device SDK v2 für Python beschrieben, die in diesem Tutorial verwendet wurde. Hier werden wir uns ansehen, wie es eine Verbindung AWS IoT Core zum Veröffentlichen und Abonnieren von MQTT Nachrichten herstellt. Im nächsten Abschnitt finden Sie einige Übungen, anhand derer Sie herausfinden können, wie ein Gerät eine Verbindung herstellt und mit AWS IoT Core ihm kommuniziert.

Die pubsub.py Beispiel-App veranschaulicht die folgenden Aspekte einer MQTT Verbindung mit AWS IoT Core:

- Kommunikationsprotokolle
- Persistente Sitzungen
- Quality of Service (Servicequalität)
- Nachrichten veröffentlichen
- Nachrichten abonnieren
- Trennen und erneutes Anschließen des Geräts

Kommunikationsprotokolle

Das `pubsub.py` Beispiel zeigt eine MQTT Verbindung unter Verwendung der WSS Protokolle MQTT und MQTT über. Die AWS Common Runtime (AWS CRT) -Bibliothek bietet Unterstützung für Low-Level-Kommunikationsprotokolle und ist in AWS IoT Device SDK v2 für Python enthalten.

MQTT

Das `pubsub.py` Beispiel ruft `mtls_from_path` (hier gezeigt) auf `mqtt_connection_builder`, um AWS IoT Core mithilfe des MQTT Protokolls eine Verbindung herzustellen. `mtls_from_path`verwendet X.509-Zertifikate und Version TLS 1.2, um das Gerät zu authentifizieren. Die AWS CRT Bibliothek verarbeitet die Details dieser Verbindung auf niedrigerer Ebene.

```
mqtt_connection = mqtt_connection_builder.mtls_from_path(
    endpoint=args.endpoint,
    cert_filepath=args.cert,
    pri_key_filepath=args.key,
    ca_filepath=args.ca_file,
    client_bootstrap=client_bootstrap,
    on_connection_interrupted=on_connection_interrupted,
    on_connection_resumed=on_connection_resumed,
    client_id=args.client_id,
    clean_session=False,
    keep_alive_secs=6
)
```

`endpoint`

Ihr AWS-Konto IoT-Geräte-Endpunkt

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

`cert_filepath`

Der Pfad zur Zertifikatsdatei des Geräts

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

`pri_key_filepath`

Der Pfad zur privaten Schlüsseldatei des Geräts, die mit der zugehörigen Zertifikatsdatei erstellt wurde

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

`ca_filepath`

Der Pfad zur Root-CA-Datei Nur erforderlich, wenn der MQTT Server ein Zertifikat verwendet, das sich noch nicht in Ihrem Trust Store befindet.

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

`client_bootstrap`

Das Common-Runtime-Objekt, das Socket-Kommunikationsaktivitäten verarbeitet

In der Beispiel-App wird dieses Objekt vor dem Aufruf zum `mqtt_connection_builder.mtls_from_path` instanziiert.

`on_connection_interrupted`, `on_connection_resumed`

Die Callback-Funktionen, die aufgerufen werden, wenn die Verbindung des Geräts unterbrochen und wieder aufgenommen wird

`client_id`

Die ID, die dieses Gerät eindeutig in der AWS-Region identifiziert

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

`clean_session`

Wahl der Option, eine neue persistente Sitzung zu starten oder, falls vorhanden, eine Verbindung zu einer bestehenden Sitzung wiederherzustellen

`keep_alive_secs`

Der Keep-Alive-Wert in Sekunden, der in der `CONNECT`-Anfrage gesendet werden soll. In diesem Intervall wird automatisch ein Ping gesendet. Wenn der Server nach dem 1,5-fachen dieses Werts keinen Ping empfängt, wird davon ausgegangen, dass die Verbindung unterbrochen wurde.

### MQTTüber WSS

Das `pubsub.py` Beispiel ruft `websockets_with_default_aws_signing` (hier gezeigt) auf `mqtt_connection_builder`, um eine Verbindung herzustellen, AWS IoT Core indem das MQTT Protokoll über verwendet wirdWSS. `websockets_with_default_aws_signing`stellt WSS mithilfe von Signature V4 eine MQTT Verbindung her, um das Gerät zu authentifizieren.

```
mqtt_connection = mqtt_connection_builder.websockets_with_default_aws_signing(
    endpoint=args.endpoint,
    client_bootstrap=client_bootstrap,
    region=args.signing_region,
    credentials_provider=credentials_provider,
    websocket_proxy_options=proxy_options,
    ca_filepath=args.ca_file,
```

```
    on_connection_interrupted=on_connection_interrupted,
    on_connection_resumed=on_connection_resumed,
    client_id=args.client_id,
    clean_session=False,
    keep_alive_secs=6
)
```

`endpoint`

Ihr AWS-Konto IoT-Geräte-Endpunkt

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

`client_bootstrap`

Das Common-Runtime-Objekt, das Socket-Kommunikationsaktivitäten verarbeitet

In der Beispiel-App wird dieses Objekt vor dem Aufruf zum `mqtt_connection_builder.websockets_with_default_aws_signing` instanziiert.

`region`

Die AWS Signaturregion, die von der Signature V4-Authentifizierung verwendet wird. In `pubsub.py` übergibt sie den in der Befehlszeile eingegebenen Parameter.

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

`credentials_provider`

Die zur Authentifizierung bereitgestellten AWS Anmeldeinformationen

In der Beispiel-App wird dieses Objekt vor dem Aufruf zu `mqtt_connection_builder.websockets_with_default_aws_signing` instanziiert.

`websocket_proxy_options`

HTTPProxy-Optionen, wenn Sie einen Proxy-Host verwenden

In der Beispiel-App wird dieser Wert vor dem Aufruf zu `mqtt_connection_builder.websockets_with_default_aws_signing` initialisiert.

`ca_filepath`

Der Pfad zur Root-CA-Datei Nur erforderlich, wenn der MQTT Server ein Zertifikat verwendet, das sich noch nicht in Ihrem Trust Store befindet.

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

`on_connection_interrupted`, `on_connection_resumed`

Die Callback-Funktionen, die aufgerufen werden, wenn die Verbindung des Geräts unterbrochen und wieder aufgenommen wird

`client_id`

Die ID, die dieses Gerät eindeutig in der AWS-Region identifiziert.

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

`clean_session`

Wahl der Option, eine neue persistente Sitzung zu starten oder, falls vorhanden, eine Verbindung zu einer bestehenden Sitzung wiederherzustellen

`keep_alive_secs`

Der Keep-Alive-Wert in Sekunden, der in der `CONNECT`-Anfrage gesendet werden soll. In diesem Intervall wird automatisch ein Ping gesendet. Wenn der Server nach dem 1,5-fachen dieses Werts keinen Ping empfängt, wird davon ausgegangen, dass die Verbindung unterbrochen wurde.

### HTTPS

WorüberHTTPS? AWS IoT Core unterstützt Geräte, die HTTPS Anfragen veröffentlichen. Aus Sicht der Programmierung senden Geräte HTTPS Anfragen an AWS IoT Core wie jede andere Anwendung. Ein Beispiel für ein Python-Programm, das eine HTTP Nachricht von einem Gerät sendet, finden Sie im HTTPSCodebeispiel, das die `requests` Python-Bibliothek verwendet. In diesem Beispiel wird eine Nachricht an AWS IoT Core einen HTTPS Benutzer gesendet, der sie als MQTT Nachricht AWS IoT Core interpretiert.

AWS IoT Core Unterstützt zwar HTTPS Anfragen von Geräten, aber überprüfen Sie unbedingt die Informationen darüber, Wählen Sie ein Anwendungsprotokoll für die Kommunikation mit Ihrem Gerät damit Sie eine fundierte Entscheidung darüber treffen können, welches Protokoll Sie für Ihre Gerätekommunikation verwenden möchten.

### Persistente Sitzungen

In der Beispiel-App bedeutet die Einstellung des `clean_session`-Parameters auf `False`, dass die Verbindung dauerhaft sein soll. In der Praxis bedeutet dies, dass die durch diesen Aufruf geöffnete Verbindung erneut eine Verbindung zu einer bestehenden persistenten Sitzung herstellt, sofern eine besteht. Andernfalls wird eine neue persistente Sitzung erstellt und eine Verbindung zu ihr hergestellt.

Bei einer persistenten Sitzung werden Nachrichten, die an das Gerät gesendet werden, vom Message Broker gespeichert, solange das Gerät nicht verbunden ist. Wenn ein Gerät die Verbindung zu einer persistenten Sitzung wieder aufnimmt, sendet der Message Broker alle von dem Gerät abonnierten gespeicherten Nachrichten an das Gerät.

Ohne eine persistente Sitzung empfängt das Gerät keine Nachrichten, die gesendet werden, während das Gerät nicht verbunden ist. Welche Option Sie verwenden, hängt von Ihrer App ab und davon, ob Nachrichten, die auftreten, während ein Gerät nicht angeschlossen ist, übermittelt werden müssen. Weitere Informationen finden Sie unter Persistente MQTT-Sitzungen.

Quality of Service (Servicequalität)

Wenn das Gerät Nachrichten veröffentlicht und abonniert, kann die bevorzugte Dienstqualität (QoS) festgelegt werden. AWS IoT unterstützt die QoS-Stufen 0 und 1 für Veröffentlichungs- und Abonnementvorgänge. Weitere Informationen zu QoS-Stufen finden Sie AWS IoT unterMQTT QoS-(Quality of Service)-Optionen.

Die AWS CRT Laufzeit für Python definiert diese Konstanten für die QoS-Stufen, die sie unterstützt:

Servicequalitätsstufen von Python

| MQTTQoS-Stufe | Symbolischer Python-Wert, verwendet von SDK | Beschreibung |
|---|---|---|
| QoS Stufe 0 | `mqtt.QoS.AT_MOST_ONCE` | Es wird nur ein Versuch zum Senden der Nachricht unternommen, unabhängig davon, ob sie empfangen wird oder nicht. Die Nachricht wird möglicherweise überhaupt nicht gesendet, z. B. wenn das Gerät nicht angeschlossen ist oder ein Netzwerkfehler vorliegt. |
| QoS-Stufe 1 | `mqtt.QoS.AT_LEAST_ONCE` | Die Nachricht wird wiederholt gesendet, bis eine PUBACK-Bestätigung eingeht. |

In der Beispiel-App werden die Veröffentlichungs- und Abonnementanfragen mit einer QoS-Stufe von 1 (`mqtt.QoS.AT_LEAST_ONCE`) gestellt.

- QoS beim Veröffentlichen

  Wenn ein Gerät eine Nachricht mit QoS Stufe 1 veröffentlicht, sendet es die Nachricht wiederholt, bis es eine PUBACK-Antwort vom Message Broker erhält. Wenn das Gerät nicht verbunden ist, wird die Nachricht in die Warteschlange gestellt, damit sie nach dem erneuten Herstellen der Verbindung gesendet werden kann.
- QoS beim Abonnieren

  Wenn ein Gerät eine Nachricht mit QoS Stufe 1 abonniert, speichert der Message Broker die Nachrichten, die das Gerät abonniert hat, bis sie an das Gerät gesendet werden können. Der Message Broker sendet die Nachrichten so oft, bis er eine PUBACK-Antwort vom Gerät erhält.

Nachrichten veröffentlichen

Nach dem erfolgreichen Herstellen einer Verbindung zu AWS IoT Core können Geräte Nachrichten veröffentlichen. Das `pubsub.py`-Beispiel tut dies, indem es die `publish`-Operation des `mqtt_connection`-Objekts aufruft.

```
mqtt_connection.publish(
    topic=args.topic,
    payload=message,
    qos=mqtt.QoS.AT_LEAST_ONCE
)
```

`topic`

Der Themenname der Nachricht, der die Nachricht identifiziert

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

`payload`

Die als Zeichenfolge formatierte Nutzdaten der Nachricht (z. B. ein JSON Dokument)

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

Ein JSON Dokument ist ein gängiges Nutzdatenformat, das auch von anderen AWS IoT Diensten erkannt wird. Das Datenformat der Nachrichtennutzdaten kann jedoch ein beliebiges Datenformat

sein, auf das sich Herausgeber und Abonnenten einigen. Andere AWS IoT Dienste erkennen die meisten Vorgänge jedoch nur JSONCBOR, und in einigen Fällen sogar für sie.

`qos`

Die QoS-Stufe für diese Nachricht

### Nachrichten abonnieren

Um Nachrichten von AWS IoT und anderen Diensten und Geräten zu empfangen, abonnieren Geräte diese Nachrichten anhand ihres Themennamens. Geräte können einzelne Nachrichten abonnieren, indem sie einen Themennamen angeben, und eine Gruppe von Nachrichten, indem sie einen Themenfilter angeben, der Platzhalterzeichen enthalten kann. Das `pubsub.py`-Beispiel verwendet den hier gezeigten Code, um Nachrichten zu abonnieren und die Callback-Funktionen zu registrieren, um die Nachricht nach dem Empfang zu verarbeiten.

```
subscribe_future, packet_id = mqtt_connection.subscribe(
    topic=args.topic,
    qos=mqtt.QoS.AT_LEAST_ONCE,
    callback=on_message_received
)
subscribe_result = subscribe_future.result()
```

`topic`

Das zu abonnierende Thema. Dies kann ein Themenname oder ein Themenfilter sein.

In der Beispiel-App wird dieser Wert von der Befehlszeile aus übergeben.

`qos`

Ob der Message Broker diese Nachrichten speichern soll, während das Gerät nicht angeschlossen ist.

Ein Wert von `mqtt.QoS.AT_LEAST_ONCE` (QoS Stufe 1) erfordert die Angabe einer persistenten Sitzung (`clean_session=False`), wenn die Verbindung hergestellt wird.

`callback`

Die Funktion, die aufgerufen werden soll, um die abonnierte Nachricht zu verarbeiten.

Die `mqtt_connection.subscribe`-Funktion gibt eine Future- und eine Paket-ID zurück. Wenn die Anfrage nach einem Abonnement erfolgreich initiiert wurde, ist die zurückgegebene Paket-ID größer als 0. Um sicherzustellen, dass das Abonnement vom Message Broker empfangen und registriert wurde, müssen Sie warten, bis das Ergebnis des asynchronen Vorgangs zurückgegeben wird, wie im Codebeispiel gezeigt.

Die Callback-Funktion

Der Callback im `pubsub.py`-Beispiel verarbeitet die abonnierten Nachrichten so, wie das Gerät sie empfängt.

```
def on_message_received(topic, payload, **kwargs):
    print("Received message from topic '{}': {}".format(topic, payload))
    global received_count
    received_count += 1
    if received_count == args.count:
        received_all_event.set()
```

`topic`

Das Thema der Nachricht

Dies ist der spezifische Themenname der empfangenen Nachricht, auch wenn Sie einen Themenfilter abonniert haben.

`payload`

Die Nutzdaten der Nachricht

Das Format dafür ist anwendungsspezifisch.

`kwargs`

Mögliche zusätzliche Argumente, wie unter `mqtt.Connection.subscribe` beschrieben.

Im `pubsub.py`-Beispiel zeigt nur `on_message_received` das Thema und seine Payload an. Außerdem werden die eingegangenen Nachrichten gezählt, um das Programm zu beenden, nachdem das Limit erreicht wurde.

Ihre App würde das Thema und die Payload auswerten, um zu bestimmen, welche Aktionen ausgeführt werden sollen.

Trennen und erneutes Anschließen des Geräts

Das `pubsub.py`-Beispiel enthält Callback-Funktionen, die aufgerufen werden, wenn das Gerät getrennt wird und wenn die Verbindung wiederhergestellt wird. Welche Aktionen Ihr Gerät bei diesen Ereignissen ausführt, ist anwendungsspezifisch.

Wenn ein Gerät zum ersten Mal eine Verbindung herstellt, muss es Themen abonnieren, um empfangen zu können. Wenn die Sitzung eines Geräts beim erneuten Herstellen der Verbindung vorhanden ist, werden seine Abonnements wiederhergestellt, und alle gespeicherten Nachrichten aus diesen Abonnements werden nach dem erneuten Herstellen der Verbindung an das Gerät gesendet.

Wenn die Sitzung eines Geräts beim erneuten Herstellen der Verbindung nicht mehr besteht, muss das Gerät seine Abonnements erneut abonnieren. Persistente Sitzungen haben eine begrenzte Lebensdauer und können ablaufen, wenn das Gerät zu lange keine Verbindung hat.

## Connect dein Gerät und kommuniziere mit AWS IoT Core

In diesem Abschnitt finden Sie einige Übungen, mit denen Sie die verschiedenen Aspekte der Verbindung Ihres Geräts mit AWS IoT Core kennenlernen können. Für diese Übungen verwenden Sie den MQTTTestclient in der AWS IoT Konsole, um zu sehen, was Ihr Gerät veröffentlicht, und um Nachrichten auf Ihrem Gerät zu veröffentlichen. Diese Übungen verwenden das `pubsub.py`Beispiel von AWS IoT Device SDK v2 für Python und bauen auf Ihren Erfahrungen mit Erste-Schritte-Tutorials Tutorials auf.

In diesem Abschnitt führen Sie folgende Schritte aus:

- Abonnieren von Themenfiltern mit Platzhaltern
- Abonnements mit Themenfiltern verarbeiten
- Veröffentlichen von Nachrichten vom Gerät.

Für diese Übungen beginnen Sie mit dem `pubsub.py`-Beispielprogramm.

> **Note**
>
> Bei diesen Übungen wird davon ausgegangen, dass Sie die Erste-Schritte-Tutorials-Tutorials abgeschlossen haben und das Terminalfenster für das Gerät aus diesem Tutorial verwenden.

### Abonnieren von Themenfiltern mit Platzhaltern

In dieser Übung ändern Sie die Befehlszeile, die verwendet wird, um `pubsub.py` zum Abonnieren eines Themenfilters mit Platzhaltern aufzurufen, und verarbeiten die empfangenen Nachrichten auf der Grundlage des Themas der Nachricht.

#### Ablauf der Übung

Stellen Sie sich für diese Übung vor, dass das Gerät über eine Temperatursteuerung und eine Lichtsteuerung verfügt. Es verwendet diese Themennamen, um die Nachrichten zu diesen Themen zu identifizieren.

1. Bevor Sie mit der Übung beginnen, versuchen Sie, diesen Befehl aus den Erste-Schritte-Tutorials-Tutorials auf dem Gerät auszuführen, um sicherzustellen, dass alles für die Übung bereit ist.

   ```
   cd ~/aws-iot-device-sdk-python-v2/samples
   python3 pubsub.py --topic topic_1 --ca_file ~/certs/Amazon-root-CA-1.pem --cert ~/
   certs/device.pem.crt --key ~/certs/private.pem.key --endpoint your-iot-endpoint
   ```

   Sie sollten dieselbe Ausgabe wie im Tutorial Erste Schritte sehen.

2. Ändern Sie für diese Übung diese Befehlszeilen-Parameter.

| Aktion | Befehlszeilen-Parameter | Auswirkung |
|---|---|---|
| hinzufügen | --message "" | Konfigurieren Sie `pubsub.py` so, dass nur zugehört wird. |
| hinzufügen | --count 2 | Beenden Sie das Programm, nachdem Sie zwei Nachricht en erhalten haben |
| ändern | --topic `device/+/details` | Definieren Sie den Themenfil ter, den Sie abonnieren möchten |

Wenn Sie diese Änderungen an der ersten Befehlszeile vornehmen, wird diese Befehlszeile angezeigt. Geben Sie diesen Befehl in das Terminalfenster Ihres Geräts ein.

```
python3 pubsub.py --message "" --count 2 --topic device/+/details --ca_file
 ~/certs/Amazon-root-CA-1.pem --cert ~/certs/device.pem.crt --key ~/certs/
private.pem.key --endpoint your-iot-endpoint
```

Das Programm sollte wie folgt aussehen:

```
Connecting to a3qexamplesffp-ats.iot.us-west-2.amazonaws.com with client ID
 'test-24d7cdcc-cc01-458c-8488-2d05849691e1'...
Connected!
Subscribing to topic 'device/+/details'...
Subscribed with QoS.AT_LEAST_ONCE
Waiting for all messages to be received...
```

Wenn Sie so etwas auf Ihrem Terminal sehen, ist Ihr Gerät bereit und wartet auf Nachrichten, bei denen die Themennamen mit `device` beginnen und mit `/detail` enden. Lassen Sie uns das also testen.

3. Hier sind ein paar Nachrichten, die Ihr Gerät möglicherweise empfängt.

| Themenname | Nachrichten-Payload |
| --- | --- |
| `device/temp/details` | `{ "desiredTemp": 20, "currentT emp": 15 }` |
| `device/light/details` | `{ "desiredLight": 100, "currentL ight": 50 }` |

4. Senden Sie mithilfe des MQTT Testclients in der AWS IoT Konsole die im vorherigen Schritt beschriebenen Nachrichten an Ihr Gerät.

   a. Öffnen Sie den MQTTTestclient in der AWS IoT Konsole.

   b. Geben Sie unter Abonnieren eines Themas im Feld Abonnementthema den Themenfilter **`device/+/details`** ein und wählen Sie anschließend Thema Abonnieren aus.

   c. Wählen Sie in der Spalte Abonnements des MQTT Testclients die Option device/+/details aus.

d. Gehen Sie für jedes der Themen in der vorherigen Tabelle im Testclient wie folgt vor: MQTT

1. Geben Sie unter Veröffentlichen den Wert aus der Spalte Themenname in der Tabelle ein.
2. Geben Sie in das Feld Nachrichten-Payload unter dem Themennamen den Wert aus der Spalte Nachrichten-Payload in der Tabelle ein.
3. Beobachten Sie das Terminalfenster, in dem ausgeführt `pubsub.py` wird, und wählen Sie im MQTT Testclient die Option Als Thema veröffentlichen aus.

Sie sollten im Terminalfenster sehen, dass die Nachricht von `pubsub.py` empfangen wurde.

Ergebnis der Übung

Damit hat `pubsub.py` die Nachrichten mithilfe eines Themenfilters mit Platzhaltern abonniert, sie empfangen und im Terminalfenster angezeigt. Beachten Sie, dass Sie einen einzelnen Themenfilter abonniert haben und die Callback-Funktion aufgerufen wurde, um Nachrichten mit zwei unterschiedlichen Themen zu verarbeiten.

Abonnements mit Themenfiltern verarbeiten

Aufbauend auf der vorherigen Übung ändern Sie die `pubsub.py` Beispiel-App, um die Nachrichtenthemen auszuwerten und die abonnierten Nachrichten auf der Grundlage des Themas zu verarbeiten.

Ablauf der Übung

Um das Thema der Nachricht zu bewerten,

1. Kopieren Sie `pubsub.py` in `pubsub2.py`.
2. Öffnen Sie `pubsub2.py` in Ihrem bevorzugten Texteditor oderIDE.
3. Suchen Sie in `pubsub2.py` nach der `on_message_received`-Funktion.
4. Fügen Sie in `on_message_received` den folgenden Code nach der Zeile ein, die mit `print("Received message` beginnt, und vor der Zeile, die mit `global received_count` beginnt.

```
    topic_parsed = False
```

```
    if "/" in topic:
        parsed_topic = topic.split("/")
        if len(parsed_topic) == 3:
            # this topic has the correct format
            if (parsed_topic[0] == 'device') and (parsed_topic[2] == 'details'):
                # this is a topic we care about, so check the 2nd element
                if (parsed_topic[1] == 'temp'):
                    print("Received temperature request: {}".format(payload))
                    topic_parsed = True
                if (parsed_topic[1] == 'light'):
                    print("Received light request: {}".format(payload))
                    topic_parsed = True
    if not topic_parsed:
        print("Unrecognized message topic.")
```

5. Speichern Sie Ihre Änderungen und führen Sie das geänderte Programm mithilfe dieser Befehlszeile aus.

```
python3 pubsub2.py --message "" --count 2 --topic device/+/details --ca_file
 ~/certs/Amazon-root-CA-1.pem --cert ~/certs/device.pem.crt --key ~/certs/
private.pem.key --endpoint your-iot-endpoint
```

6. Öffnen Sie in der AWS IoT Konsole den MQTTTestclient.
7. Geben Sie unter Abonnieren eines Themas im Feld Abonnementthema den Themenfilter **`device/+/details`** ein und wählen Sie anschließend Thema Abonnieren aus.
8. Wählen Sie in der Spalte Abonnements des MQTT Testclients die Option device/+/details aus.
9. Gehen Sie für jedes der Themen in dieser Tabelle im Testclient wie folgt vor: MQTT

| Themenname | Nachrichten-Payload |
|---|---|
| `device/temp/details` | `{ "desiredTemp": 20, "currentTemp": 15 }` |
| `device/light/details` | `{ "desiredLight": 100, "currentLight": 50 }` |

1. Geben Sie unter Veröffentlichen den Wert aus der Spalte Themenname in der Tabelle ein.
2. Geben Sie in das Feld Nachrichten-Payload unter dem Themennamen den Wert aus der Spalte Nachrichten-Payload in der Tabelle ein.

3. Beobachten Sie das Terminalfenster, in dem ausgeführt `pubsub.py` wird, und wählen Sie im MQTT Testclient die Option Als Thema veröffentlichen aus.

   Sie sollten im Terminalfenster sehen, dass die Nachricht von `pubsub.py` empfangen wurde.

Sie sollten in Ihrem Terminalfenster etwas Ähnliches sehen.

```
Connecting to a3qexamplesffp-ats.iot.us-west-2.amazonaws.com with client ID 'test-
af794be0-7542-45a0-b0af-0b0ea7474517'...
Connected!
Subscribing to topic 'device/+/details'...
Subscribed with QoS.AT_LEAST_ONCE
Waiting for all messages to be received...
Received message from topic 'device/light/details': b'{ "desiredLight": 100,
 "currentLight": 50 }'
Received light request: b'{ "desiredLight": 100, "currentLight": 50 }'
Received message from topic 'device/temp/details': b'{ "desiredTemp": 20,
 "currentTemp": 15 }'
Received temperature request: b'{ "desiredTemp": 20, "currentTemp": 15 }'
2 message(s) received.
Disconnecting...
Disconnected!
```

Ergebnis der Übung

In dieser Übung haben Sie Code hinzugefügt, damit die Beispiel-App mehrere Nachrichten in der Callback-Funktion erkennt und verarbeitet. Damit könnte Ihr Gerät Nachrichten empfangen und darauf reagieren.

Ihr Gerät kann auch mehrere Nachrichten empfangen und verarbeiten, indem es verschiedene Nachrichten separat abonniert und jedem Abonnement eine eigene Callback-Funktion zuweist.

Veröffentlichen von Nachrichten vom Gerät.

Sie können die Beispiel-App pubsub.py verwenden, um Nachrichten von Ihrem Gerät aus zu veröffentlichen. Nachrichten werden zwar so veröffentlicht, wie sie sind, aber sie können nicht als JSON Dokumente gelesen werden. In dieser Übung wird die Beispiel-App so modifiziert, dass sie JSON Dokumente in der Nachrichten-Payload veröffentlichen kann, die dann gelesen werden können. AWS IoT Core

### Ablauf der Übung

In dieser Übung wird die folgende Nachricht zusammen mit dem `device/data`-Thema gesendet.

```
{
    "timestamp": 1601048303,
    "sensorId": 28,
    "sensorData": [
        {
        "sensorName": "Wind speed",
        "sensorValue": 34.2211224
        }
    ]
}
```

Um Ihren MQTT Testclient darauf vorzubereiten, die Nachrichten aus dieser Übung zu überwachen

1. Geben Sie unter Abonnieren eines Themas im Feld Abonnementthema den Themenfilter **`device/data`** ein und wählen Sie anschließend Thema Abonnieren aus.
2. Wählen Sie in der Spalte Abonnements des MQTT Testclients die Option Gerät/Daten aus.
3. Lassen Sie das Fenster des MQTT Testclients geöffnet, um auf Nachrichten von Ihrem Gerät zu warten.

Um JSON Dokumente mit der Beispiel-App pubsub.py zu versenden

1. Kopieren Sie auf dem Gerät `pubsub.py` nach `pubsub3.py`.
2. Bearbeiten Sie `pubsub3.py`, um die Formatierung der zu veröffentlichenden Nachrichten zu ändern.

   a. Öffnen Sie `pubsub3.py` in einem Texteditor.

   b. Suchen Sie diese Codezeile:

   ```
   message = "{} [{}]".format(message_string, publish_count)
   ```

   c. Ändern Sie sie in:

   ```
   message = "{}".format(message_string)
   ```

   d. Suchen Sie diese Codezeile:

   ```
   message_json = json.dumps(message)
   ```

e. Ändern Sie sie in:

```
message = "{}".json.dumps(json.loads(message))
```

f. Speichern Sie Ihre Änderungen.

3. Führen Sie auf dem Gerät diesen Befehl aus, um die Nachricht zweimal zu senden.

```
python3 pubsub3.py  --ca_file ~/certs/Amazon-root-CA-1.pem  --cert ~/certs/
device.pem.crt  --key ~/certs/private.pem.key  --topic device/data  --count 2 --
message '{"timestamp":1601048303,"sensorId":28,"sensorData":[{"sensorName":"Wind
 speed","sensorValue":34.2211224}]}'  --endpoint your-iot-endpoint
```

4. Prüfen Sie im MQTT Testclient, ob das JSON Dokument in der Nachrichtennutzlast interpretiert und formatiert wurde, z. B. wie folgt:

`pubsub3.py` abonniert standardmäßig auch die Nachrichten, die es sendet. Sie sollten sehen können, dass es die Nachrichten im Ausgabefenster der App empfangen hat. Das Terminalfenster sollte etwa folgendermaßen aussehen.

```
Connecting to a3qEXAMPLEsffp-ats.iot.us-west-2.amazonaws.com with client ID
 'test-5cff18ae-1e92-4c38-a9d4-7b9771afc52f'...
Connected!
Subscribing to topic 'device/data'...
Subscribed with QoS.AT_LEAST_ONCE
Sending 2 message(s)
Publishing message to topic 'device/data':
 {"timestamp":1601048303,"sensorId":28,"sensorData":[{"sensorName":"Wind
 speed","sensorValue":34.2211224}]}
```

```
Received message from topic 'device/data':
 b'{"timestamp":1601048303,"sensorId":28,"sensorData":[{"sensorName":"Wind
 speed","sensorValue":34.2211224}]}'
Publishing message to topic 'device/data':
 {"timestamp":1601048303,"sensorId":28,"sensorData":[{"sensorName":"Wind
 speed","sensorValue":34.2211224}]}
Received message from topic 'device/data':
 b'{"timestamp":1601048303,"sensorId":28,"sensorData":[{"sensorName":"Wind
 speed","sensorValue":34.2211224}]}'
2 message(s) received.
Disconnecting...
Disconnected!
```

Ergebnis der Übung

Auf diese Weise kann Ihr Gerät Nachrichten generieren, an die Sie senden können, AWS IoT Core um die grundlegende Konnektivität zu testen, und Gerätemeldungen AWS IoT Core zur Verarbeitung bereitstellen. Sie könnten diese App beispielsweise verwenden, um Testdaten von Ihrem Gerät zu senden, um AWS IoT Regelaktionen zu testen.

### Überprüfen Sie die Ergebnisse.

Die Beispiele in diesem Tutorial haben Ihnen praktische Erfahrungen mit den Grundlagen der Kommunikation zwischen Geräten vermittelt AWS IoT Core— ein wesentlicher Bestandteil Ihrer AWS IoT Lösung. Wenn Ihre Geräte in der Lage sind AWS IoT Core, mit ihnen zu kommunizieren, können sie Nachrichten an AWS Dienste und andere Geräte weiterleiten, auf denen sie reagieren können. Ebenso können AWS Dienste und andere Geräte Informationen verarbeiten, die dazu führen, dass Nachrichten an Ihre Geräte zurückgesendet werden.

Wenn Sie bereit sind, AWS IoT Core weiter zu forschen, probieren Sie diese Tutorials aus:

- the section called “Senden einer SNS Amazon-Benachrichtigung”
- the section called “Speichern von Gerätedaten in einer DynamoDB-Tabelle”
- the section called “Formatieren einer Benachrichtigung mithilfe einer Funktion AWS Lambda ”

## Tutorial: Verwenden des AWS IoT Device SDK for Embedded C

In diesem Abschnitt wird beschrieben, wie Sie den ausführen AWS IoT Device SDK for Embedded C.

Verfahren in diesem Abschnitt

- Schritt 1: Installieren Sie das AWS IoT Device SDK for Embedded C
- Schritt 2: Konfigurieren der Beispielanwendung
- Schritt 3: So laden Sie die Beispielanwendung herunter und führen sie aus


## Schritt 1: Installieren Sie das AWS IoT Device SDK for Embedded C

Das AWS IoT Device SDK for Embedded C richtet sich im Allgemeinen an Geräte mit eingeschränkten Ressourcen, die eine optimierte Laufzeit in C-Sprache benötigen. Sie können das SDK auf jedem Betriebssystem verwenden und es auf jedem Prozessortyp hosten (z. B. MCUs undMPUs). Wenn Sie mehr Speicher- und Verarbeitungsressourcen zur Verfügung haben, empfehlen wir, dass Sie eines der AWS IoT Geräte- und Mobilgeräte der höheren Ordnung verwenden SDKs (z. B. C++ JavaScript, Java und Python).

Im Allgemeinen AWS IoT Device SDK for Embedded C ist das für Systeme vorgesehen, die eingebettete Betriebssysteme verwenden MCUs oder MPUs Low-End-Betriebssysteme verwenden. Für das Programmierbeispiel in diesem Abschnitt gehen wir davon aus, dass Ihr Gerät Linux verwendet.

Example

1. Laden Sie das von AWS IoT Device SDK for Embedded C GitHubauf Ihr Gerät herunter.

   ```
   git clone https://github.com/aws/aws-iot-device-sdk-embedded-c.git --recurse-
   submodules
   ```

   Dadurch wird ein Verzeichnis mit dem Namen `aws-iot-device-sdk-embedded-c` im aktuellen Verzeichnis erstellt.

2. Navigieren Sie zu diesem Verzeichnis und machen Sie sich mit der neuesten Version vertraut. Das neueste Release-Tag finden Sie unter github.com/aws/ aws-iot-device-sdk -embedded-c/ tags.

   ```
   cd aws-iot-device-sdk-embedded-c
   git checkout latest-release-tag
   ```

3. SSLInstallieren Sie Open Version 1.1.0 oder höher. Die SSL Open-Entwicklungsbibliotheken werden normalerweise „libssl-dev“ oder „openssl-devel“ genannt, wenn sie über einen Paketmanager installiert werden.

```
sudo apt-get install libssl-dev
```

### Schritt 2: Konfigurieren der Beispielanwendung

Das AWS IoT Device SDK for Embedded C beinhaltet Beispielanwendungen, die Sie ausprobieren können. Der Einfachheit halber wird in diesem Tutorial die `mqtt_demo_mutual_auth` Anwendung verwendet, die veranschaulicht, wie Sie eine Verbindung zum AWS IoT Core Message Broker herstellen und MQTT Themen abonnieren und veröffentlichen.

1. Kopieren Sie das Zertifikat und den privaten Schlüssel, den Sie in Erste Schritte mit AWS IoT Core Tutorials erstellt haben, in das Verzeichnis `build/bin/certificates`.

   > **Note**
   >
   > Geräte- und CA-Stammzertifikate laufen ab oder können widerrufen werden. Wenn diese Zertifikate ablaufen oder widerrufen werden, müssen Sie ein neues CA-Zertifikat oder einen privaten Schlüssel und ein Gerätezertifikat auf Ihr Gerät kopieren.

2. Sie müssen das Beispiel mit Ihrem persönlichen AWS IoT Core Endpunkt, Ihrem privaten Schlüssel, Ihrem Zertifikat und Ihrem Root-CA-Zertifikat konfigurieren. Navigieren Sie zum `aws-iot-device-sdk-embedded-c/demos/mqtt/mqtt_demo_mutual_auth` Verzeichnis .

   Wenn Sie das AWS CLI installiert haben, können Sie diesen Befehl verwenden, um den Endpunkt Ihres Kontos zu findenURL.

   ```
   aws iot describe-endpoint --endpoint-type iot:Data-ATS
   ```

   Wenn Sie den nicht AWS CLI installiert haben, öffnen Sie Ihre AWS IoT Konsole. Wählen Sie im Navigationsbereich Verwalten und dann Objekte aus. Wählen Sie das IoT-Objekt für Ihr Gerät und dann Interagieren aus. Ihr Endpunkt wird im HTTPSAbschnitt der Seite mit den Ding-Details angezeigt.

3. Öffnen Sie die Datei `demo_config.h` und aktualisieren Sie die Werte für Folgendes:

   AWS_IOT_ENDPOINT

   Ihr persönlicher Endpunkt.

CLIENT_CERT_PATH

Der Dateipfad Ihres Zertifikats, zum Beispiel `certificates/device.pem.crt"`.

CLIENT_PRIVATE_KEY_PATH

Der Dateiname Ihres privaten Schlüssels, zum Beispiel `certificates/private.pem.key`.

Beispielsweise:

```
// Get from demo_config.h
// ================================================
#define AWS_IOT_ENDPOINT                "my-endpoint-ats.iot.us-
east-1.amazonaws.com"
#define AWS_MQTT_PORT                   8883
#define CLIENT_IDENTIFIER               "testclient"
#define ROOT_CA_CERT_PATH               "certificates/AmazonRootCA1.crt"
#define CLIENT_CERT_PATH                "certificates/my-device-cert.pem.crt"
#define CLIENT_PRIVATE_KEY_PATH         "certificates/my-device-private-key.pem.key"
// ================================================
```

4. Prüfen Sie mit diesem Befehl, ob Sie es auf Ihrem Gerät CMake installiert haben.

```
cmake --version
```

Wenn die Versionsinformationen für den Compiler angezeigt werden, können Sie mit dem nächsten Abschnitt fortfahren.

Wenn Sie eine Fehlermeldung erhalten oder keine Informationen angezeigt werden, müssen Sie das CMake-Paket mit diesem Befehl installieren.

```
sudo apt-get install cmake
```

Führen Sie den cmake --version Befehl erneut aus und vergewissern Sie CMake sich, dass er installiert wurde und dass Sie bereit sind, fortzufahren.

5. Überprüfen Sie mithilfe dieses Befehls, ob die Entwicklungstools auf Ihrem Gerät installiert sind.

```
gcc --version
```

Wenn die Versionsinformationen für den Compiler angezeigt werden, können Sie mit dem nächsten Abschnitt fortfahren.

Wenn Sie eine Fehlermeldung erhalten oder keine Compilerinformationen angezeigt werden, müssen Sie das Paket `build-essential` mit diesem Befehl installieren.

```
sudo apt-get install build-essential
```

Führen Sie den Befehl gcc --version erneut aus und vergewissern Sie sich, dass die Build-Tools installiert wurden und Sie fortfahren können.

### Schritt 3: So laden Sie die Beispielanwendung herunter und führen sie aus

In diesem Verfahren wird erklärt, wie Sie die `mqtt_demo_mutual_auth` Anwendung auf Ihrem Gerät generieren und sie mithilfe von mit der AWS IoT Konsole verbinden. AWS IoT Device SDK for Embedded C

Um die Beispielanwendungen auszuführen AWS IoT Device SDK for Embedded C

1. Navigieren Sie zu `aws-iot-device-sdk-embedded-c` und erstellen Sie ein Build-Verzeichnis.

   ```
   mkdir build && cd build
   ```

2. Geben Sie den folgenden CMake Befehl ein, um die zum Erstellen benötigten Makefiles zu generieren.

   ```
   cmake ..
   ```

3. Geben Sie den folgenden Befehl ein, um die ausführbare App-Datei zu erstellen:

   ```
   make
   ```

4. Führen Sie die App `mqtt_demo_mutual_auth` mit diesem Befehl aus.

   ```
   cd bin
   ./mqtt_demo_mutual_auth
   ```

   Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
[INFO] [DEMO] [mqtt_demo_mutual_auth.c:584] Establishing a TLS session to a2zk5tjv9x07ct-ats.iot.us-west-2.amazonaws.com:8883.
[INFO] [DEMO] [mqtt_demo_mutual_auth.c:1264] Creating an MQTT connection to a2zk5tjv9x07ct-ats.iot.us-west-2.amazonaws.com.
[INFO] [MQTT] [core_mqtt.c:855] Packet received. ReceivedBytes=2.
[INFO] [MQTT] [core_mqtt_serializer.c:970] CONNACK session present bit not set.
[INFO] [MQTT] [core_mqtt_serializer.c:912] Connection accepted.
[INFO] [MQTT] [core_mqtt.c:1526] Received MQTT CONNACK successfully from broker.
[INFO] [MQTT] [core_mqtt.c:1792] MQTT connection established with the broker.
[INFO] [DEMO] [mqtt_demo_mutual_auth.c:1033] MQTT connection successfully established with broker.


[INFO] [DEMO] [mqtt_demo_mutual_auth.c:1296] A clean MQTT connection is established. Cleaning up all the stored outgoing publishes.


[INFO] [DEMO] [mqtt_demo_mutual_auth.c:1314] Subscribing to the MQTT topic testclient/example/topic.
[INFO] [DEMO] [mqtt_demo_mutual_auth.c:1097] SUBSCRIBE sent for topic testclient/example/topic to broker.


[INFO] [MQTT] [core_mqtt.c:855] Packet received. ReceivedBytes=3.
[INFO] [DEMO] [mqtt_demo_mutual_auth.c:921] Subscribed to the topic testclient/example/topic. with maximum QoS 1.


[INFO] [DEMO] [mqtt_demo_mutual_auth.c:1358] Sending Publish to the MQTT topic testclient/example/topic.
[INFO] [DEMO] [mqtt_demo_mutual_auth.c:1195] PUBLISH sent for topic testclient/example/topic to broker with packet ID 2.


[INFO] [MQTT] [core_mqtt.c:855] Packet received. ReceivedBytes=2.
[INFO] [MQTT] [core_mqtt.c:1126] Ack packet deserialized with result: MQTTSuccess.
[INFO] [MQTT] [core_mqtt.c:1139] State record updated. New state=MQTTPublishDone.
[INFO] [DEMO] [mqtt_demo_mutual_auth.c:946] PUBACK received for packet id 2.


[INFO] [DEMO] [mqtt_demo_mutual_auth.c:672] Cleaned up outgoing publish packet with packet id 2.


[INFO] [MQTT] [core_mqtt.c:855] Packet received. ReceivedBytes=40.
[INFO] [MQTT] [core_mqtt.c:1015] De-serialized incoming PUBLISH packet: DeserializerResult=MQTTSuccess.
```

Ihr Gerät ist jetzt AWS IoT mit dem verbunden AWS IoT Device SDK for Embedded C.

Sie können die AWS IoT Konsole auch verwenden, um die MQTT Nachrichten anzuzeigen, die die Beispiel-App veröffentlicht. Informationen zur Verwendung des MQTT Clients in der AWS IoT Konsole finden Sie unterthe section called “MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen”.

## AWS IoT Regeln erstellen, um Gerätedaten an andere Dienste weiterzuleiten

In diesen Tutorials erfahren Sie, wie Sie AWS IoT Regeln mithilfe einiger der gängigsten Regelaktionen erstellen und testen.

AWS IoT Regeln senden Daten von Ihren Geräten an andere AWS Dienste. Sie warten auf bestimmte MQTT Nachrichten, formatieren die Daten in den Nachrichtennutzdaten und senden das Ergebnis an andere AWS Dienste.

Wir empfehlen Ihnen, diese in der Reihenfolge auszuprobieren, in der sie hier angezeigt werden, auch wenn Sie eine Regel erstellen möchten, die eine Lambda-Funktion oder etwas komplexeres

verwendet. Die Tutorials werden in der Reihenfolge von einfach bis komplex präsentiert. Sie stellen schrittweise neue Konzepte vor, damit Sie sich mit den Konzepten vertraut machen können, die Sie zum Erstellen von Regelaktionen verwenden können, für die es kein spezielles Tutorial gibt.

> **Note**
>
> AWS IoT Regeln helfen Ihnen dabei, die Daten von Ihren IoT-Geräten an andere AWS Dienste zu senden. Um dies erfolgreich zu tun, benötigen Sie jedoch Grundkenntnisse der anderen Dienste, an die Sie Daten senden möchten. Diese Tutorials enthalten zwar die notwendigen Informationen, um die Aufgaben zu erledigen, aber es könnte hilfreich sein, mehr über die Dienste zu erfahren, an die Sie Daten senden möchten, bevor Sie sie in Ihrer Lösung verwenden. Eine ausführliche Erläuterung der anderen AWS Dienste würde den Rahmen dieser Tutorials sprengen.

### Überblick über Tutorial-Szenarien

Das Szenario für diese Tutorials ist das eines Wettersensorgeräts, das seine Daten regelmäßig veröffentlicht. In diesem imaginären System gibt es viele solcher Sensorgeräte. Die Tutorials in diesem Abschnitt konzentrieren sich jedoch auf ein einzelnes Gerät und zeigen, wie Sie mehrere Sensoren unterbringen können.

Die Tutorials in diesem Abschnitt zeigen Ihnen, wie Sie AWS IoT Regeln verwenden, um die folgenden Aufgaben mit diesem imaginären System von Wettersensorgeräten zu erledigen.

- Tutorial: Eine Nachricht erneut veröffentlichen MQTT

  In diesem Tutorial wird gezeigt, wie Sie eine von den Wettersensoren empfangene MQTT Nachricht als Nachricht erneut veröffentlichen, die nur die Sensor-ID und den Temperaturwert enthält. Es verwendet nur AWS IoT Core Dienste und demonstriert eine einfache SQL Abfrage sowie die Verwendung des MQTT Clients zum Testen Ihrer Regel.

- Tutorial: Eine SNS Amazon-Benachrichtigung senden

  Dieses Tutorial zeigt, wie Sie eine SNS Nachricht senden, wenn ein Wert von einem Wettersensorgerät einen bestimmten Wert überschreitet. Es baut auf den Konzepten auf, die im vorherigen Tutorial vorgestellt wurden, und fügt hinzu, wie Sie mit einem anderen AWS Service, dem Amazon Simple Notification Service (AmazonSNS), arbeiten können.

Wenn Sie neu bei Amazon sindSNS, lesen Sie sich die Übungen Erste Schritte durch, bevor Sie mit diesem Tutorial beginnen.

- Tutorial: Gerätedaten in einer DynamoDB-Tabelle speichern

  Dieses Tutorial zeigt, wie Sie die Daten der Wettersensorgeräte in einer Datenbanktabelle speichern. Es verwendet die Regelabfrageanweisung und die Ersatzvorlagen, um die Nachrichtendaten für den Zieldienst Amazon DynamoDB zu formatieren.

  Wenn Sie mit DynamoDB noch nicht vertraut sind, lesen Sie sich die Übungen Erste Schritte durch, bevor Sie mit diesem Tutorial beginnen.

- Tutorial: Formatieren einer Benachrichtigung mithilfe einer AWS Lambda Funktion

  Dieses Tutorial zeigt, wie Sie eine Lambda-Funktion aufrufen, um die Gerätedaten neu zu formatieren und sie dann als Textnachricht zu senden. Es fügt ein Python-Skript und AWS SDK Funktionen in einer AWS LambdaFunktion hinzu, um mit den Nachrichtennutzdaten der Wettersensorgeräte zu formatieren und eine Textnachricht zu senden.

  Wenn Sie Lambda noch nicht kennen, lesen Sie sich die Übungen Erste Schritte durch, bevor Sie mit diesem Tutorial beginnen.

## AWS IoT Überblick über die Regeln

In all diesen Tutorials werden AWS IoT Regeln erstellt.

Damit eine AWS IoT Regel die Daten von einem Gerät an einen anderen AWS Dienst sendet, verwendet sie:

- Eine Anweisung zur Regelabfrage, die aus folgenden Elementen besteht:
  - Eine SQL SELECT Klausel, die die Daten aus der Nachrichtennutzlast auswählt und formatiert
  - Ein Themenfilter (das FROM Objekt in der Regelabfrageanweisung), der die zu verwendenden Nachrichten identifiziert
  - Eine optionale bedingte Anweisung (eine SQL WHERE Klausel), die bestimmte Bedingungen festlegt, auf die reagiert werden soll
- Mindestens eine Regelaktion

Geräte veröffentlichen Nachrichten zu MQTT Themen. Der Themenfilter in der SQL SELECT Anweisung identifiziert die MQTT Themen, auf die die Regel angewendet werden soll. Die in der SQL SELECT Anweisung angegebenen Felder formatieren die Daten aus der Payload für eingehende MQTT Nachrichten, sodass sie von den Aktionen der Regel verwendet werden können. Eine vollständige Liste der Regelaktionen finden Sie unter AWS IoT Regelaktionen.

Tutorials in diesem Abschnitt

- Tutorial: Eine Nachricht erneut veröffentlichen MQTT
- Tutorial: Eine SNS Amazon-Benachrichtigung senden
- Tutorial: Gerätedaten in einer DynamoDB-Tabelle speichern
- Tutorial: Formatieren einer Benachrichtigung mithilfe einer AWS Lambda Funktion

## Tutorial: Eine Nachricht erneut veröffentlichen MQTT

In diesem Tutorial wird gezeigt, wie Sie eine AWS IoT Regel erstellen, die eine MQTT Nachricht veröffentlicht, wenn eine bestimmte MQTT Nachricht empfangen wird. Die Nutzlast für eingehende Nachrichten kann durch die Regel geändert werden, bevor sie veröffentlicht wird. Auf diese Weise können Sie Nachrichten erstellen, die auf bestimmte Anwendungen zugeschnitten sind, ohne dass Sie Ihr Gerät oder dessen Firmware ändern müssen. Sie können auch den Filteraspekt einer Regel verwenden, um Nachrichten nur zu veröffentlichen, wenn eine bestimmte Bedingung erfüllt ist.

Die durch eine Regel erneut veröffentlichten Nachrichten verhalten sich wie Nachrichten, die von einem anderen AWS IoT Gerät oder Client gesendet wurden. Geräte können die erneut veröffentlichten Nachrichten genauso abonnieren, wie sie jedes andere MQTT Nachrichtenthema abonnieren können.

Was Sie in diesem Tutorial lernen werden:

- Wie verwendet man einfache SQL Abfragen und Funktionen in einer Regelabfrageanweisung
- Wie benutzt man den MQTT Client, um eine AWS IoT Regel zu testen

Für dieses Tutorial brauchen Sie ungefähr 30 Minuten.

In diesem Tutorial führen Sie die folgenden Aktivitäten durch:

- Lesen Sie die MQTT Themen und AWS IoT Regeln
- Schritt 1: Erstellen Sie eine AWS IoT Regel, um eine MQTT Nachricht erneut zu veröffentlichen

- Schritt 2: Testen Ihrer neuen Regel
- Schritt 3: Überprüfen Sie die Ergebnisse und die nächsten Schritte

Stellen Sie vor Beginn dieses Tutorials sicher, dass Sie über Folgendes verfügen:

- Einrichten AWS-Konto

  Sie benötigen Ihre AWS-Konto AWS IoT Handkonsole, um dieses Tutorial abzuschließen.
- Überprüft MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen

  Stellen Sie sicher, dass Sie den MQTT Client verwenden können, um ein Thema zu abonnieren und zu veröffentlichen. In diesem Verfahren verwenden Sie den MQTT Client, um Ihre neue Regel zu testen.

### Lesen Sie die MQTT Themen und AWS IoT Regeln

Bevor wir über AWS IoT Regeln sprechen, ist es hilfreich, das MQTT Protokoll zu verstehen. Bei IoT-Lösungen bietet das MQTT Protokoll einige Vorteile gegenüber anderen Netzwerkkommunikationsprotokollen, z. B. HTTP was es zu einer beliebten Wahl für die Verwendung durch IoT-Geräte macht. In diesem Abschnitt werden die wichtigsten Aspekte MQTT beschrieben, die für dieses Tutorial relevant sind. Informationen zum MQTT Vergleich mit finden Sie HTTP unterWählen Sie ein Anwendungsprotokoll für die Kommunikation mit Ihrem Gerät.

#### MQTTProtokoll

Das MQTT Protokoll verwendet ein Veröffentlichungs-/Abonnement-Kommunikationsmodell mit seinem Host. Um Daten zu senden, veröffentlichen Geräte Nachrichten, die anhand von Themen identifiziert sind, an den AWS IoT Message Broker. Um Nachrichten vom Message Broker zu empfangen, abonnieren Geräte die Themen, die sie erhalten, indem sie Themenfilter in Abonnementanfragen an den Message Broker senden. Die AWS IoT Regel-Engine empfängt MQTT Nachrichten vom Message Broker.

#### AWS IoT Regeln

AWS IoT Regeln bestehen aus einer Regelabfrageanweisung und einer oder mehreren Regelaktionen. Wenn die AWS IoT Regel-Engine eine MQTT Nachricht empfängt, wirken sich diese Elemente wie folgt auf die Nachricht aus.

- Anweisung zur Regelabfrage

Die Abfrageanweisung der Regel beschreibt die zu verwendenden MQTT Themen, interpretiert die Daten aus der Nachrichtennutzlast und formatiert die Daten wie in einer SQL Anweisung beschrieben, die den Anweisungen in gängigen SQL Datenbanken ähnelt. Das Ergebnis der Abfrageanweisung sind die Daten, die an die Aktionen der Regel gesendet werden.

- Regelaktion

  Jede Regelaktion in einer Regel wirkt sich auf die Daten aus, die sich aus der Abfrageanweisung der Regel ergeben. AWS IoT unterstützt viele Regelaktionen. In diesem Tutorial konzentrieren Sie sich jedoch auf die Wiederveröffentlichen Regelaktion, bei der das Ergebnis der Abfrageanweisung als MQTT Nachricht mit einem bestimmten Thema veröffentlicht wird.

### Schritt 1: Erstellen Sie eine AWS IoT Regel, um eine MQTT Nachricht erneut zu veröffentlichen

Die AWS IoT Regel, die Sie in diesem Tutorial erstellen, bezieht sich auf die folgenden Themen `device/`*`device_id`*`/data` MQTT *`device_id`* ist die ID des Geräts, das die Nachricht gesendet hat. Diese Themen werden durch einen Themenfilter als `device/+/data` beschrieben, wobei es sich bei + um ein Platzhalterzeichen handelt, das einer beliebigen Zeichenfolge zwischen den beiden Schrägstrichen entspricht.

Wenn die Regel eine Nachricht von einem passenden Thema empfängt, veröffentlicht sie die `temperature` Werte `device_id` und und erneut als neue MQTT Nachricht mit dem `device/data/temp` Thema.

Die Payload einer MQTT Nachricht mit dem `device/22/data` Thema sieht beispielsweise wie folgt aus:

```
{
  "temperature": 28,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

Die Regel verwendet den `temperature` Wert aus der Nachrichtennutzlast und den Wert `device_id` aus dem Thema und veröffentlicht sie erneut als MQTT Nachricht mit dem `device/data/temp` Thema und einer Nachrichtennutzlast, die wie folgt aussieht:

```
{
  "device_id": "22",
  "temperature": 28
}
```

Mit dieser Regel abonnieren Geräte, die nur die Geräte-ID und die Temperaturdaten benötigen, das `device/data/temp` Thema, um nur diese Informationen zu erhalten.

Um eine Regel zu erstellen, die eine Nachricht erneut veröffentlicht MQTT

1. Öffnen Sie den Regel-Hub der AWS IoT Konsole.
2. Wählen Sie unter Regeln die Option Erstellen aus und beginnen Sie mit der Erstellung Ihrer neuen Regel.
3. Gehen Sie im oberen Teil von Regel erstellen wie folgt vor:

   a. Geben Sie im Feld Name den Namen der Regel ein. Für dieses Tutorial nennen Sie es **`republish_temp`**.

      Denken Sie daran, dass ein Regelname innerhalb Ihres Kontos und Ihrer Region eindeutig sein muss und keine Leerzeichen enthalten darf. Wir haben in diesem Namen einen Unterstrich verwendet, um die beiden Wörter im Namen der Regel voneinander zu trennen.

   b. Beschreiben Sie die Regel im Feld Beschreibung.

      Eine aussagekräftige Beschreibung hilft Ihnen dabei, sich daran zu erinnern, was diese Regel bewirkt und warum Sie sie erstellt haben. Die Beschreibung kann so lang wie nötig sein, also seien Sie so detailliert wie möglich.

4. In der Regelabfrageanweisung von Regel erstellen:

   a. Wählen Sie unter SQL Version verwenden die Option aus**`2016-03-23`**.

   b. Geben Sie im Bearbeitungsfeld Regelabfrageanweisung die folgende Anweisung ein:

      ```
      SELECT topic(2) as device_id, temperature FROM 'device/+/data'
      ```

      Diese Aussage:

      - Hört auf MQTT Nachrichten mit einem Thema, das dem `device/+/data` Themenfilter entspricht.

- Wählt das zweite Element aus der Themenzeichenfolge aus und weist es dem `device_id` Feld zu.
- Wählt das Wert `temperature` Feld aus der Nachrichtennutzlast aus und weist es dem `temperature` Feld zu.

5. Gehen Sie im Feld Eine oder mehrere Aktionen festlegen wie folgt vor:

   a. Um die Liste der Regelaktionen für diese Regel zu öffnen, wählen Sie Aktion hinzufügen.

   b. Wählen Sie unter Aktion auswählen die Option Nachricht erneut zu einem AWS IoT Thema veröffentlichen aus.

   c. Wählen Sie unten in der Aktionsliste die Option Aktion konfigurieren aus, um die Konfigurationsseite der ausgewählten Aktion zu öffnen.

6. Gehen Sie in Aktion konfigurieren wie folgt vor:

   a. Geben Sie im Feld Thema **`device/data/temp`** ein. Dies ist das MQTT Thema der Nachricht, die diese Regel veröffentlichen wird.

   b. Wählen Sie unter Qualität der Dienstleistung die Option 0 aus. Die Nachricht wird null oder mehrere Mal zugestellt.

   c. Gehen Sie unter Rolle auswählen oder erstellen, um AWS IoT Zugriff auf diese Aktion zu gewähren, wie folgt vor:

      i. Wählen Sie Create Role aus. Das Dialogfeld Eine neue Rolle erstellen wird geöffnet.

      ii. Geben Sie einen Namen ein, der die neue Rolle beschreibt. Verwenden Sie in diesem Tutorial **`republish_role`**.

      Wenn Sie eine neue Rolle erstellen, werden die richtigen Richtlinien für die Ausführung der Regelaktion erstellt und der neuen Rolle zugeordnet. Wenn Sie das Thema dieser Regelaktion ändern oder diese Rolle in einer anderen Regelaktion verwenden, müssen Sie die Richtlinie für diese Rolle aktualisieren, um das neue Thema oder die neue Aktion zu autorisieren. Um eine bestehende Rolle zu aktualisieren, wählen Sie in diesem Abschnitt die Option Rolle aktualisieren aus.

      iii. Wählen Sie Rolle erstellen aus, um die Rolle zu erstellen und das Dialogfeld zu schließen.

   d. Wählen Sie Aktion hinzufügen, um die Aktion zur Regel hinzuzufügen und zur Seite Regel erstellen zurückzukehren.

7. Die Aktion Eine Nachricht in einem AWS IoT Thema erneut veröffentlichen ist jetzt unter Eine oder mehrere Aktionen festlegen aufgeführt.

   In der Kachel der neuen Aktion unter Nachricht zu einem AWS IoT Thema erneut veröffentlichen können Sie das Thema sehen, in dem die neue Aktion veröffentlicht wird.

   Dies ist die einzige Regelaktion, die Sie zu dieser Regel hinzufügen werden.
8. Scrollen Sie in Regel erstellen ganz nach unten und wählen Sie Regel erstellen aus, um die Regel zu erstellen und diesen Schritt abzuschließen.

### Schritt 2: Testen Ihrer neuen Regel

Um Ihre neue Regel zu testen, verwenden Sie den MQTT Client, um die von dieser Regel verwendeten MQTT Nachrichten zu veröffentlichen und zu abonnieren.

Öffnen Sie den MQTTClient in der AWS IoT Konsole in einem neuen Fenster. Auf diese Weise können Sie die Regel bearbeiten, ohne die Konfiguration Ihres MQTT Clients zu verlieren. Der MQTT Client speichert keine Abonnements oder Nachrichtenprotokolle, wenn Sie ihn verlassen, um zu einer anderen Seite in der Konsole zu wechseln.

Um den MQTT Client zum Testen Ihrer Regel zu verwenden

1. Abonnieren Sie im MQTT Client in der AWS IoT Konsole die Eingabethemen, in diesem Fall`device/+/data`.

   a. Wählen Sie im MQTT Client unter Abonnements die Option Thema abonnieren aus.

   b. Geben Sie im Abonnementthema das Thema des Eingabethemenfilters **`device/+/data`** ein.

   c. Belassen Sie die übrigen Felder auf ihren Standardeinstellungen.

   d. Wählen Sie Thema abonnieren aus.

      In der Spalte Abonnements wird **`device/+/data`** unter In einem Thema veröffentlichen angezeigt.
2. Abonnieren Sie das Thema, das Ihre Regel veröffentlichen wird: `device/data/temp`.

   a. Wählen Sie unter Abonnements erneut die Option Thema abonnieren aus, und geben Sie unter Abonnementthema das Thema der erneut veröffentlichten Nachricht **`device/data/temp`** ein.

b. Belassen Sie die übrigen Felder auf ihren Standardeinstellungen.

c. Wählen Sie Thema abonnieren aus.

In der Spalte Abonnements wird **`device/data/temp`** unter Geräte/+/Daten angezeigt.

3. Veröffentlichen Sie eine Nachricht zum Eingabethema mit einer bestimmten Geräte-ID, **`device/22/data`**. Sie können nicht zu MQTT Themen veröffentlichen, die Platzhalterzeichen enthalten.

a. Wählen Sie im MQTT Client unter Abonnements die Option Als Thema veröffentlichen aus.

b. Geben Sie im Feld Veröffentlichen den Namen des Eingabethemas **`device/22/data`** ein.

c. Kopieren Sie die hier gezeigten Beispieldaten und fügen Sie die Beispieldaten in das Bearbeitungsfeld unter dem Themennamen ein.

```
{
  "temperature": 28,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

d. Um Ihre MQTT Nachricht zu senden, wählen Sie Im Thema veröffentlichen.

4. Überprüfen Sie die gesendeten Nachrichten.

a. Im MQTT Client befindet sich unter Abonnements ein grüner Punkt neben den beiden Themen, die Sie zuvor abonniert haben.

Die grünen Punkte zeigen an, dass eine oder mehrere neue Nachrichten eingegangen sind, seit Sie sie das letzte Mal angesehen haben.

b. Wählen Sie unter Abonnements die Option Gerät/+/Daten aus, um zu überprüfen, ob die Nutzlast der Nachricht mit dem übereinstimmt, was Sie gerade veröffentlicht haben, und wie folgt aussieht:

```
{
  "temperature": 28,
  "humidity": 80,
  "barometer": 1013,
```

```
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

c. Wählen Sie unter Abonnements die Option Gerät/Daten/Temp aus, um zu überprüfen, ob Ihre neu veröffentlichte Nachrichtennutzlast wie folgt aussieht:

```
{
  "device_id": "22",
  "temperature": 28
}
```

Beachten Sie, dass es sich bei dem `device_id` Wert um eine Zeichenfolge in Anführungszeichen handelt und der Wert `temperature` numerisch ist. Das liegt daran, dass die `topic()` Funktion die Zeichenfolge aus dem Themennamen der Eingabenachricht extrahiert hat, während der `temperature` Wert den numerischen Wert aus der Nutzlast der Eingabenachricht verwendet.

Wenn Sie den Wert zu einem numerischen `device_id` Wert machen möchten, ersetzen Sie `topic(2)` in der Anweisung zur Regelabfrage durch:

```
cast(topic(2) AS DECIMAL)
```

Beachten Sie, dass die Umwandlung des `topic(2)` Werts in einen numerischen Wert nur funktioniert, wenn dieser Teil des Themas nur numerische Zeichen enthält.

5. Wenn Sie sehen, dass die richtige Nachricht im Thema Gerät/Daten/Temp veröffentlicht wurde, hat Ihre Regel funktioniert. Weitere Informationen zur Aktion „Regel erneut veröffentlichen“ finden Sie im nächsten Abschnitt.

   Wenn Sie nicht sehen, dass die richtige Nachricht in den Themen Gerät/+/Daten oder Gerät/Daten/Temp veröffentlicht wurde, lesen Sie die Tipps zur Fehlerbehebung.

Problembehebung bei der Regel „Nachricht erneut veröffentlichen“

Hier sind einige Dinge, die Sie überprüfen sollten, falls Sie nicht die erwarteten Ergebnisse sehen.

- Sie haben ein Fehlerbanner

Wenn bei der Veröffentlichung der Eingabemeldung ein Fehler aufgetreten ist, korrigieren Sie diesen Fehler zuerst. Die folgenden Schritte können Ihnen helfen, diesen Fehler zu korrigieren.

- Die Eingabemeldung wird im Client nicht angezeigt MQTT

  Jedes Mal, wenn Sie Ihre Eingabenachricht zu dem `device/22/data` Thema veröffentlichen, sollte diese Nachricht im MQTT Client erscheinen, sofern Sie den `device/+/data` Themenfilter wie im Verfahren beschrieben abonniert haben.

  Zu überprüfende Dinge

  - Überprüfen Sie den Themenfilter, den Sie abonniert haben

    Wenn Sie das Thema der Eingabenachricht wie im Verfahren beschrieben abonniert haben, sollte Ihnen bei jeder Veröffentlichung eine Kopie der Eingabenachricht angezeigt werden.

    Wenn Sie die Nachricht nicht sehen, überprüfen Sie den Themennamen, den Sie abonniert haben, und vergleichen Sie ihn mit dem Thema, zu dem Sie sie veröffentlicht haben. Bei Themennamen wird Groß- und Kleinschreibung beachtet, und das Thema, das Sie abonniert haben, muss mit dem Thema identisch sein, zu dem Sie die Nachrichtennutzlast veröffentlicht haben.

  - Überprüfen Sie die Funktion zum Veröffentlichen von Nachrichten

    Wählen Sie im MQTT Client unter Abonnements die Option device/+/data aus, überprüfen Sie das Thema der Veröffentlichungsnachricht und wählen Sie dann Als Thema veröffentlichen aus. Sie sollten sehen, dass die Nutzlast der Nachricht aus dem Bearbeitungsfeld unter dem Thema in der Nachrichtenliste erscheinen.

- Ihre erneut veröffentlichte Nachricht wird im Client nicht angezeigt MQTT

  Damit Ihre Regel funktioniert, muss sie über die richtige Richtlinie verfügen, die sie autorisiert, eine Nachricht zu empfangen und erneut zu veröffentlichen, und sie muss die Nachricht empfangen.

  Zu überprüfende Dinge

  - Überprüfen Sie die AWS-Region Daten Ihres MQTT Kunden und die Regel, die Sie erstellt haben

    Die Konsole, in der Sie den MQTT Client ausführen, muss sich in derselben AWS Region befinden wie die von Ihnen erstellte Regel.

  - Überprüfen Sie das Thema der Eingabemeldung in der Regelabfrageanweisung

Damit die Regel funktioniert, muss sie eine Nachricht mit dem Themennamen erhalten, der dem Themenfilter in der FROM Klausel der Regelabfrageanweisung entspricht.

Überprüfen Sie die Schreibweise des Themenfilters in der Regelabfrageanweisung mit der Schreibweise des Themas im MQTT Client. Bei Themennamen wird Groß- und Kleinschreibung beachtet, und das Thema der Nachricht muss mit dem Themenfilter in der Regelabfrageanweisung übereinstimmen.

- Überprüfen Sie den Inhalt der Nutzlast der Input-Nachricht

  Damit die Regel funktioniert, muss sie das Datenfeld in der Nachrichtennutzlast finden, das in der SELECT Anweisung deklariert ist.

  Überprüfen Sie die Schreibweise des `temperature` Felds in der Regelabfrageanweisung mit der Schreibweise der Nachrichtennutzdaten im MQTT Client. Bei Feldnamen wird zwischen Groß- und Kleinschreibung unterschieden, und das `temperature` Feld in der Regelabfrageanweisung muss mit dem `temperature` Feld in der Nachrichtennutzlast identisch sein.

  Stellen Sie sicher, dass das JSON Dokument in der Nachrichten-Payload korrekt formatiert ist. Wenn das Fehler JSON enthält, z. B. ein fehlendes Komma, kann die Regel es nicht lesen.

- Überprüfen Sie das Thema der erneut veröffentlichten Nachricht in der Regelaktion

  Das Thema, zu dem die Regelaktion „Erneut veröffentlichen“ die neue Nachricht veröffentlicht, muss mit dem Thema übereinstimmen, das Sie im Client abonniert haben. MQTT

  Öffnen Sie die Regel, die Sie in der Konsole erstellt haben, und überprüfen Sie das Thema, zu dem die Regelaktion die Nachricht erneut veröffentlicht.

- Überprüfen Sie die Rolle, die von der Regel verwendet wird

  Die Regelaktion muss berechtigt sein, das ursprüngliche Thema zu empfangen und das neue Thema zu veröffentlichen.

  Die Richtlinien, mit denen die Regel autorisiert wird, Nachrichtendaten zu empfangen und erneut zu veröffentlichen, sind spezifisch für die verwendeten Themen. Wenn Sie das Thema ändern, das für die erneute Veröffentlichung der Nachrichtendaten verwendet wird, müssen Sie die Rolle der Regelaktion aktualisieren, damit ihre Richtlinie dem aktuellen Thema entspricht.

Wenn Sie vermuten, dass dies das Problem ist, bearbeiten Sie die Aktion Regel erneut veröffentlichen und erstellen Sie eine neue Rolle. Neue Rollen, die durch die Regelaktion erstellt wurden, erhalten die erforderlichen Autorisierungen, um diese Aktionen auszuführen.

Schritt 3: Überprüfen Sie die Ergebnisse und die nächsten Schritte

In diesem Tutorial

- Sie haben eine einfache SQL Abfrage und einige Funktionen in einer Regelabfrageanweisung verwendet, um eine neue MQTT Nachricht zu erstellen.
- Sie haben eine Regel erstellt, die diese neue Nachricht erneut veröffentlicht hat.
- Sie haben den MQTT Client verwendet, um Ihre AWS IoT Regel zu testen.

Nächste Schritte

Nachdem Sie einige Nachrichten mit dieser Regel erneut veröffentlicht haben, probieren Sie sie aus, um zu sehen, wie sich Änderungen einiger Aspekte des Tutorials auf die erneut veröffentlichte Nachricht auswirken. Hier sind einige Ideen, die Ihnen den Einstieg erleichtern sollen.

- Ändern Sie die *`device_id`* klicken Sie auf das Thema der eingegebenen Nachricht und beobachten Sie die Auswirkungen auf die Payload der neu veröffentlichten Nachricht.
- Ändern Sie die in der Regelabfrageanweisung ausgewählten Felder und beobachten Sie die Auswirkungen auf die Nutzlast der erneut veröffentlichten Nachricht.
- Probieren Sie das nächste Tutorial in dieser Serie und lernen Sie, wie man Tutorial: Eine SNS Amazon-Benachrichtigung senden.

Die in diesem Tutorial verwendete Aktion Regel erneut veröffentlichen kann Ihnen auch beim Debuggen von Regelabfrageanweisungen helfen. Sie können diese Aktion beispielsweise einer Regel hinzufügen, um zu sehen, wie ihre Regelabfrageanweisung die von ihren Regelaktionen verwendeten Daten formatiert.

## Tutorial: Eine SNS Amazon-Benachrichtigung senden

Dieses Tutorial zeigt, wie Sie eine AWS IoT Regel erstellen, die MQTT Nachrichtendaten an ein SNS Amazon-Thema sendet, sodass sie als SMS Textnachricht gesendet werden können.

In diesem Tutorial erstellen Sie eine Regel, die Nachrichtendaten von einem Wettersensor an alle Abonnenten eines SNS Amazon-Themas sendet, wenn die Temperatur den in der Regel festgelegten Wert überschreitet. Die Regel erkennt, wenn die gemeldete Temperatur den in der Regel festgelegten Wert überschreitet, und erstellt dann eine neue Nachrichtennutzlast, die nur die Geräte-ID, die gemeldete Temperatur und den Temperaturgrenzwert, der überschritten wurde, enthält. Die Regel sendet die neue Nachrichten-Payload als JSON Dokument an ein SNS Thema, wodurch alle Abonnenten des SNS Themas benachrichtigt werden.

Was Sie in diesem Tutorial lernen werden:

- So erstellen und testen Sie eine SNS Amazon-Benachrichtigung
- So rufen Sie eine SNS Amazon-Benachrichtigung von einer AWS IoT Regel aus auf
- Wie verwendet man einfache SQL Abfragen und Funktionen in einer Regelabfrageanweisung
- Wie benutzt man den MQTT Client, um eine AWS IoT Regel zu testen

Für dieses Tutorial brauchen Sie ungefähr 30 Minuten.

In diesem Tutorial führen Sie die folgenden Aktivitäten durch:

- Schritt 1: Erstellen Sie ein SNS Amazon-Thema, das eine SMS Textnachricht sendet
- Schritt 2: Erstellen Sie eine AWS IoT Regel zum Senden der Textnachricht
- Schritt 3: Testen Sie die AWS IoT Regel und die SNS Amazon-Benachrichtigung
- Schritt 4: Überprüfen Sie die Ergebnisse und die nächsten Schritte

Stellen Sie vor Beginn dieses Tutorials sicher, dass Sie über Folgendes verfügen:

- Einrichten AWS-Konto

  Sie benötigen Ihre AWS-Konto AWS IoT Handkonsole, um dieses Tutorial abzuschließen.
- Überprüft MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen

  Stellen Sie sicher, dass Sie den MQTT Client verwenden können, um ein Thema zu abonnieren und zu veröffentlichen. In diesem Verfahren verwenden Sie den MQTT Client, um Ihre neue Regel zu testen.
- Der Amazon Amazon Simple Notification Service wurde überprüft

Wenn Sie Amazon SNS noch nicht verwendet haben, lesen Sie den Artikel Zugriff für Amazon einrichten SNS. Wenn Sie bereits andere AWS IoT Tutorials abgeschlossen haben, AWS-Konto sollten Sie bereits korrekt konfiguriert sein.

### Schritt 1: Erstellen Sie ein SNS Amazon-Thema, das eine SMS Textnachricht sendet

In diesem Verfahren wird erklärt, wie Sie das SNS Amazon-Thema erstellen, an das Ihr Wettersensor Nachrichtendaten senden kann. Das SNS Amazon-Thema benachrichtigt dann alle Abonnenten per SMS Textnachricht über die Überschreitung der Temperaturgrenze.

Um ein SNS Amazon-Thema zu erstellen, das eine SMS Textnachricht sendet

1. Erstellen Sie ein SNS Amazon-Thema.

   a. Melden Sie sich bei der SNSAmazon-Konsole an.

   b. Wählen Sie im linken Navigationsbereich Topics (Themen).

   c. Wählen Sie auf der Seite Topics (Themen) Create New Topic (Neues Thema erstellen) aus.

   d. Wählen Sie unter Details den Standardtyp aus. Standardmäßig erstellt die Konsole ein FIFO Thema.

   e. Geben Sie im Feld Name den Namen des SNS Themas ein. Geben Sie für dieses Tutorial **`high_temp_notice`** ein.

   f. Scrollen Sie zum Ende der Seite und wählen Sie Create topic (Erstellen eines Themas) aus.

      In der Konsole wird die Seite Details geöffnet.

2. Erstellen Sie ein SNS Amazon-Abonnement.

   > **Note**
   >
   > Für die Telefonnummer, die Sie in diesem Abonnement verwenden, können Gebühren für Textnachrichten aufgrund der Nachrichten anfallen, die Sie in diesem Tutorial versenden.

   a. Wählen Sie auf der Detailseite des Themas high_temp_notice die Option Abonnement erstellen.

b. Wählen Sie unter Abonnement erstellen im Abschnitt Details in der Protokollliste die Option aus SMS.

c. Geben Sie im Feld Endpunkt die Nummer eines Telefons ein, das Textnachrichten empfangen kann. Achten Sie darauf, dass Sie es so eingeben, dass es mit einem + beginnt, die Landes- und Ortsvorwahl enthält und keine anderen Satzzeichen enthält.

d. Wählen Sie Create subscription (Abonnement erstellen) aus.

3. Testen Sie die SNS Amazon-Benachrichtigung.

a. Wählen Sie in der SNSAmazon-Konsole im linken Navigationsbereich Themen aus.

b. Um die Detailseite des Themas zu öffnen, wählen Sie unter Themen in der Liste der Themen den Eintrag high_temp_notice aus.

c. Um die Seite Nachricht im Thema veröffentlichen zu öffnen, wählen Sie auf der Detailseite von high_temp_notice die Option Nachricht veröffentlichen aus.

d. Geben Sie unter Nachricht zum Thema veröffentlichen im Abschnitt Nachrichtentext im Feld Nachrichtentext, der an den Endpunkt gesendet werden soll, eine Kurznachricht ein.

e. Scrollen Sie auf der Seite nach unten und wählen Sie Nachricht veröffentlichen.

f. Vergewissern Sie sich auf dem Telefon mit der Nummer, die Sie zuvor bei der Erstellung des Abonnements verwendet haben, dass die Nachricht empfangen wurde.

Wenn Sie die Testnachricht nicht erhalten haben, überprüfen Sie die Telefonnummer und die Einstellungen Ihres Telefons.

Stellen Sie sicher, dass Sie Testnachrichten von der SNSAmazon-Konsole aus veröffentlichen können, bevor Sie mit dem Tutorial fortfahren.

### Schritt 2: Erstellen Sie eine AWS IoT Regel zum Senden der Textnachricht

Die AWS IoT Regel, die Sie in diesem Tutorial erstellen, abonniert die `device/`*`device_id`*`/data` MQTT Themen, in denen die ID des Geräts angegeben *`device_id`* ist, das die Nachricht gesendet hat. Diese Themen werden in einem Themenfilter als `device/+/data` beschrieben, wobei es sich bei + um ein Platzhalterzeichen handelt, das einer beliebigen Zeichenfolge zwischen den beiden Schrägstrichen entspricht. Diese Regel testet auch den Wert des `temperature` Felds in der Nachrichtennutzlast.

Wenn die Regel eine Nachricht von einem passenden Thema empfängt, verwendet sie den *`device_id`* Themennamen, den `temperature` Wert aus der Nachrichtennutzlast, fügt einen

konstanten Wert für das zu testende Limit hinzu und sendet diese Werte als JSON Dokument an ein SNS Amazon-Benachrichtigungsthema.

Eine MQTT Nachricht vom Wettersensorgerät Nummer 32 verwendet beispielsweise das `device/32/data` Thema und hat eine Nachrichten-Payload, die wie folgt aussieht:

```
{
  "temperature": 38,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

Die Regelabfrageanweisung der Regel nimmt den `temperature` Wert aus der Nachrichtennutzlast, den *`device_id`* aus dem Themennamen und fügt den konstanten `max_temperature` Wert hinzu, um eine Nachrichtennutzlast zu senden, die wie folgt aussieht, zum SNS Amazon-Thema:

```
{
  "device_id": "32",
  "reported_temperature": 38,
  "max_temperature": 30
}
```

Um eine AWS IoT Regel zur Erkennung einer Temperaturüberschreitung zu erstellen und die Daten zu erstellen, die an das SNS Amazon-Thema gesendet werden sollen

1. Öffnen Sie den Regel-Hub der AWS IoT Konsole.
2. Wenn dies Ihre erste Regel ist, wählen Sie Erstellen oder Regel erstellen.
3. In Erstellen einer Regel:

   a. Geben Sie unter Name **`temp_limit_notify`** ein.

      Denken Sie daran, dass ein Regelname in Ihrer Region AWS-Konto und in Ihrer Region eindeutig sein muss und keine Leerzeichen enthalten darf. Wir haben in diesem Namen einen Unterstrich verwendet, um die Wörter im Namen der Regel voneinander zu trennen.

   b. Beschreiben Sie die Regel im Feld Beschreibung.

Eine aussagekräftige Beschreibung macht es einfacher, sich daran zu erinnern, was diese Regel bewirkt und warum Sie sie erstellt haben. Die Beschreibung kann so lang wie nötig sein, also seien Sie so detailliert wie möglich.

4. In der Regelabfrageanweisung von Regel erstellen:

   a. Wählen Sie unter SQL Version verwenden die Option 2016-03-23 aus.

   b. Geben Sie im Bearbeitungsfeld Regelabfrageanweisung die folgende Anweisung ein:

```
SELECT topic(2) as device_id,
    temperature as reported_temperature,
    30 as max_temperature
  FROM 'device/+/data'
  WHERE temperature > 30
```

   Diese Aussage:

   - Sucht nach MQTT Nachrichten mit einem Thema, das dem `device/+/data` Themenfilter entspricht und deren `temperature` Wert größer als 30 ist.
   - Wählt das zweite Element aus der Themenzeichenfolge aus und weist es dem `device_id` Feld zu.
   - Wählt das Wert `temperature` Feld aus der Nachrichtennutzlast aus und weist es dem `reported_temperature` Feld zu.
   - Erstellt einen konstanten Wert `30`, der den Grenzwert darstellt, und weist ihn dem `max_temperature` Feld zu.

5. Um die Liste der Regelaktionen für diese Regel zu öffnen, wählen Sie unter Eine oder mehrere Aktionen festlegen die Option Aktion hinzufügen aus.

6. Wählen Sie unter Aktion auswählen die Option Nachricht als SNS Push-Benachrichtigung senden aus.

7. Um die Konfigurationsseite der ausgewählten Aktion zu öffnen, wählen Sie unten in der Aktionsliste die Option Aktion konfigurieren aus.

8. Gehen Sie in Aktion konfigurieren wie folgt vor:

   a. Wählen Sie in SNSTarget die Option Select aus, suchen Sie Ihr SNS Thema mit dem Namen high_temp_notice und wählen Sie Select aus.

   b. Wählen Sie unter Nachrichtenformat die Option. RAW

c. Wählen Sie unter Rolle auswählen oder erstellen, um AWS IoT Zugriff auf diese Aktion zu gewähren, die Option Rolle erstellen aus.

d. Geben Sie unter Neue Rolle erstellen im Feld Name einen eindeutigen Namen für die neue Rolle ein. Verwenden Sie für dieses Tutorial **`sns_rule_role`**.

e. Wählen Sie Rolle erstellen.

Wenn Sie dieses Tutorial wiederholen oder eine bestehende Rolle wiederverwenden, wählen Sie Rolle aktualisieren, bevor Sie fortfahren. Dadurch wird das Richtliniendokument der Rolle aktualisiert, sodass es mit dem SNS Ziel funktioniert.

9. Wählen Sie Aktion hinzufügen und kehren Sie zur Seite Regel erstellen zurück.

   In der Kachel der neuen Aktion unter Eine Nachricht als SNS Push-Benachrichtigung senden finden Sie das SNS Thema, das in Ihrer Regel aufgerufen wird.

   Dies ist die einzige Regelaktion, die Sie zu dieser Regel hinzufügen werden.

10. Um die Regel zu erstellen und diesen Schritt abzuschließen, scrollen Sie unter Regel erstellen nach unten und wählen Sie Regel erstellen aus.

### Schritt 3: Testen Sie die AWS IoT Regel und die SNS Amazon-Benachrichtigung

Um Ihre neue Regel zu testen, verwenden Sie den MQTT Client, um die von dieser Regel verwendeten MQTT Nachrichten zu veröffentlichen und zu abonnieren.

Öffnen Sie den MQTTClient in der AWS IoT Konsole in einem neuen Fenster. Auf diese Weise können Sie die Regel bearbeiten, ohne die Konfiguration Ihres MQTT Clients zu verlieren. Wenn Sie den MQTT Client verlassen, um zu einer anderen Seite in der Konsole zu wechseln, werden keine Abonnements oder Nachrichtenprotokolle gespeichert.

Um den MQTT Client zum Testen Ihrer Regel zu verwenden

1. Abonnieren Sie im MQTT Client in der AWS IoT Konsole die Eingabethemen, in diesem Fall`device/+/data`.

   a. Wählen Sie im MQTT Client unter Abonnements die Option Thema abonnieren aus.

   b. Geben Sie im Abonnementthema das Thema des Eingabethemenfilters **`device/+/data`** ein.

   c. Belassen Sie die übrigen Felder auf ihren Standardeinstellungen.

d. Wählen Sie Thema abonnieren aus.

   In der Spalte Abonnements wird **`device/+/data`** unter In einem Thema veröffentlichen angezeigt.

2. Veröffentlichen Sie eine Nachricht zum Eingabethema mit einer bestimmten Geräte-ID, **`device/32/data`**. Sie können nicht zu MQTT Themen veröffentlichen, die Platzhalterzeichen enthalten.

   a. Wählen Sie im MQTT Client unter Abonnements die Option Als Thema veröffentlichen aus.

   b. Geben Sie im Feld Veröffentlichen den Namen des Eingabethemas **`device/32/data`** ein.

   c. Kopieren Sie die hier gezeigten Beispieldaten und fügen Sie die Beispieldaten in das Bearbeitungsfeld unter dem Themennamen ein.

```
{
  "temperature": 38,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

   d. Wählen Sie Im Thema veröffentlichen, um Ihre MQTT Nachricht zu veröffentlichen.

3. Bestätigen Sie, dass die Textnachricht gesendet wurde.

   a. Im MQTT Client befindet sich unter Abonnements ein grüner Punkt neben dem Thema, das Sie zuvor abonniert haben.

      Der grüne Punkt zeigt an, dass eine oder mehrere neue Nachrichten eingegangen sind, seit Sie sie das letzte Mal angesehen haben.

   b. Wählen Sie unter Abonnements die Option Gerät/+/Daten aus, um zu überprüfen, ob die Nutzlast der Nachricht mit dem übereinstimmt, was Sie gerade veröffentlicht haben, und wie folgt aussieht:

```
{
  "temperature": 38,
  "humidity": 80,
  "barometer": 1013,
```

```
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

c. Überprüfe das Telefon, mit dem du das SNS Thema abonniert hast, und vergewissere dich, dass der Inhalt der Nachrichten-Payload wie folgt aussieht:

```
{"device_id":"32","reported_temperature":38,"max_temperature":30}
```

Beachten Sie, dass es sich bei dem `device_id` Wert um eine Zeichenfolge in Anführungszeichen handelt und der Wert `temperature` numerisch ist. Das liegt daran, dass die `topic()` Funktion die Zeichenfolge aus dem Themennamen der Eingabenachricht extrahiert hat, während der `temperature` Wert den numerischen Wert aus der Nutzlast der Eingabenachricht verwendet.

Wenn Sie den Wert zu einem numerischen `device_id` Wert machen möchten, ersetzen Sie `topic(2)` in der Anweisung zur Regelabfrage durch:

```
cast(topic(2) AS DECIMAL)
```

Beachten Sie, dass die Umwandlung des `topic(2)` Werts in einen numerischen `DECIMAL` Wert nur funktioniert, wenn dieser Teil des Themas nur numerische Zeichen enthält.

4. Versuchen Sie, eine MQTT Nachricht zu senden, bei der die Temperatur den Grenzwert nicht überschreitet.

   a. Wählen Sie im MQTT Client unter Abonnements die Option Als Thema veröffentlichen aus.

   b. Geben Sie im Feld Veröffentlichen den Namen des Eingabethemas **`device/33/data`** ein.

   c. Kopieren Sie die hier gezeigten Beispieldaten und fügen Sie die Beispieldaten in das Bearbeitungsfeld unter dem Themennamen ein.

```
{
  "temperature": 28,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
```

```
  }
}
```

d. Um Ihre MQTT Nachricht zu senden, wählen Sie Im Thema veröffentlichen.

Sie sollten die Nachricht sehen, die Sie im **`device/+/data`** Abonnement gesendet haben. Da der Temperaturwert jedoch unter der Höchsttemperatur in der Regelabfrageanweisung liegt, sollten Sie keine Textnachricht erhalten.

Wenn Sie nicht das richtige Verhalten feststellen, lesen Sie die Tipps zur Fehlerbehebung.

Problembehandlung bei Ihrer SNS Nachrichtenregel

Hier sind einige Dinge, die Sie überprüfen sollten, falls Sie nicht die erwarteten Ergebnisse sehen.

- Sie haben ein Fehlerbanner

  Wenn bei der Veröffentlichung der Eingabemeldung ein Fehler aufgetreten ist, korrigieren Sie diesen Fehler zuerst. Die folgenden Schritte können Ihnen helfen, diesen Fehler zu korrigieren.
- Sie sehen die Eingabemeldung nicht im MQTT Client

  Jedes Mal, wenn Sie Ihre Eingabenachricht zu dem `device/22/data` Thema veröffentlichen, sollte diese Nachricht im MQTT Client erscheinen, sofern Sie den `device/+/data` Themenfilter wie im Verfahren beschrieben abonniert haben.

  Zu überprüfende Dinge

  - Überprüfen Sie den Themenfilter, den Sie abonniert haben

    Wenn Sie das Thema der Eingabenachricht wie im Verfahren beschrieben abonniert haben, sollte Ihnen bei jeder Veröffentlichung eine Kopie der Eingabenachricht angezeigt werden.

    Wenn Sie die Nachricht nicht sehen, überprüfen Sie den Themennamen, den Sie abonniert haben, und vergleichen Sie ihn mit dem Thema, zu dem Sie sie veröffentlicht haben. Bei Themennamen wird Groß- und Kleinschreibung beachtet, und das Thema, das Sie abonniert haben, muss mit dem Thema identisch sein, zu dem Sie die Nachrichtennutzlast veröffentlicht haben.
  - Überprüfen Sie die Funktion zum Veröffentlichen von Nachrichten

Wählen Sie im MQTT Client unter Abonnements die Option device/+/data aus, überprüfen Sie das Thema der Veröffentlichungsnachricht und wählen Sie dann Als Thema veröffentlichen aus. Sie sollten sehen, dass die Nutzlast der Nachricht aus dem Bearbeitungsfeld unter dem Thema in der Nachrichtenliste erscheinen.

- Sie erhalten keine Nachricht SMS

  Damit Ihre Regel funktioniert, muss sie über die richtige Richtlinie verfügen, die sie autorisiert, eine Nachricht zu empfangen und eine SNS Benachrichtigung zu senden, und sie muss die Nachricht empfangen.

  Zu überprüfende Dinge

  - Überprüfen Sie die AWS-Region Ihres MQTT Clients und die Regel, die Sie erstellt haben

    Die Konsole, in der Sie den MQTT Client ausführen, muss sich in derselben AWS Region befinden wie die von Ihnen erstellte Regel.
  - Überprüfen Sie, ob der Temperaturwert in der Nachrichtennutzlast den Testschwellenwert überschreitet

    Wenn der Temperaturwert kleiner oder gleich 30 ist, wie in der Regelabfrageanweisung definiert, führt die Regel keine ihrer Aktionen aus.
  - Überprüfen Sie das Thema der Eingabemeldung in der Regelabfrageanweisung

    Damit die Regel funktioniert, muss sie eine Nachricht mit dem Themennamen erhalten, der dem Themenfilter in der FROM Klausel der Regelabfrageanweisung entspricht.

    Überprüfen Sie die Schreibweise des Themenfilters in der Regelabfrageanweisung mit der Schreibweise des Themas im MQTT Client. Bei Themennamen wird Groß- und Kleinschreibung beachtet, und das Thema der Nachricht muss mit dem Themenfilter in der Regelabfrageanweisung übereinstimmen.
  - Überprüfen Sie den Inhalt der Nutzlast der Input-Nachricht

    Damit die Regel funktioniert, muss sie das Datenfeld in der Nachrichtennutzlast finden, das in der SELECT Anweisung deklariert ist.

    Überprüfen Sie die Schreibweise des `temperature` Felds in der Regelabfrageanweisung mit der Schreibweise der Nachrichtennutzdaten im MQTT Client. Bei Feldnamen wird zwischen Groß- und Kleinschreibung unterschieden, und das `temperature` Feld in der

Regelabfrageanweisung muss mit dem `temperature` Feld in der Nachrichtennutzlast identisch sein.

Stellen Sie sicher, dass das JSON Dokument in der Nachrichten-Payload korrekt formatiert ist. Wenn das Fehler JSON enthält, z. B. ein fehlendes Komma, kann die Regel es nicht lesen.

- Überprüfen Sie das Thema der erneut veröffentlichten Nachricht in der Regelaktion

  Das Thema, zu dem die Regelaktion „Erneut veröffentlichen“ die neue Nachricht veröffentlicht, muss mit dem Thema übereinstimmen, das Sie im Client abonniert haben. MQTT

  Öffnen Sie die Regel, die Sie in der Konsole erstellt haben, und überprüfen Sie das Thema, zu dem die Regelaktion die Nachricht erneut veröffentlicht.
- Überprüfen Sie die Rolle, die von der Regel verwendet wird

  Die Regelaktion muss berechtigt sein, das ursprüngliche Thema zu empfangen und das neue Thema zu veröffentlichen.

  Die Richtlinien, mit denen die Regel autorisiert wird, Nachrichtendaten zu empfangen und erneut zu veröffentlichen, sind spezifisch für die verwendeten Themen. Wenn Sie das Thema ändern, das für die erneute Veröffentlichung der Nachrichtendaten verwendet wird, müssen Sie die Rolle der Regelaktion aktualisieren, damit ihre Richtlinie dem aktuellen Thema entspricht.

  Wenn Sie vermuten, dass dies das Problem ist, bearbeiten Sie die Aktion Regel erneut veröffentlichen und erstellen Sie eine neue Rolle. Neue Rollen, die durch die Regelaktion erstellt wurden, erhalten die erforderlichen Autorisierungen, um diese Aktionen auszuführen.

### Schritt 4: Überprüfen Sie die Ergebnisse und die nächsten Schritte

In diesem Tutorial:

- Sie haben ein SNS Amazon-Benachrichtigungsthema und ein Abonnement erstellt und getestet.
- Sie haben eine einfache SQL Abfrage und Funktionen in einer Regelabfrageanweisung verwendet, um eine neue Nachricht für Ihre Benachrichtigung zu erstellen.
- Sie haben eine AWS IoT Regel zum Senden einer SNS Amazon-Benachrichtigung erstellt, die Ihre benutzerdefinierte Nachrichtennutzlast verwendet hat.
- Sie haben den MQTT Client verwendet, um Ihre AWS IoT Regel zu testen.

### Nächste Schritte

Nachdem Sie einige Textnachrichten mit dieser Regel gesendet haben, versuchen Sie, damit zu experimentieren, um zu sehen, wie sich Änderungen einiger Aspekte des Tutorials auf die Nachricht auswirken und wann sie gesendet wird. Hier sind einige Ideen, die Ihnen den Einstieg erleichtern sollen.

- Ändern Sie die *`device_id`* im Thema der Eingangsnachricht und beobachten Sie die Auswirkung auf den Inhalt der Textnachricht.
- Ändern Sie die in der Regelabfrageanweisung ausgewählten Felder und beobachten Sie die Auswirkungen auf den Inhalt der Textnachricht.
- Ändern Sie den Test in der Regelabfrageanweisung so, dass er auf eine Mindesttemperatur statt auf eine Höchsttemperatur testet. Denken Sie daran, den Namen von `max_temperature` zu ändern!
- Fügen Sie eine Regelaktion zum erneuten Veröffentlichen hinzu, um eine MQTT Nachricht zu senden, wenn eine SNS Benachrichtigung gesendet wird.
- Probieren Sie das nächste Tutorial in dieser Serie und lernen Sie, wie man Tutorial: Gerätedaten in einer DynamoDB-Tabelle speichern.

## Tutorial: Gerätedaten in einer DynamoDB-Tabelle speichern

Dieses Tutorial zeigt, wie Sie eine AWS IoT Regel erstellen, die Nachrichtendaten an eine DynamoDB-Tabelle sendet.

In diesem Tutorial erstellen Sie eine Regel, die Nachrichtendaten von einem imaginären Wettersensorgerät an eine DynamoDB-Tabelle sendet. Die Regel formatiert die Daten vieler Wettersensoren so, dass sie zu einer einzigen Datenbanktabelle hinzugefügt werden können.

Was Sie in diesem Tutorial lernen werden

- So erstellen Sie eine DynamoDB-Tabelle
- So senden Sie Nachrichtendaten aus einer Regel an eine DynamoDB-Tabelle AWS IoT
- Wie verwendet man Ersatzvorlagen in einer Regel AWS IoT
- Wie verwendet man einfache SQL Abfragen und Funktionen in einer Regelabfrageanweisung
- Wie benutzt man den MQTT Client, um eine AWS IoT Regel zu testen

Für dieses Tutorial brauchen Sie ungefähr 30 Minuten.

In diesem Tutorial führen Sie die folgenden Aktivitäten durch:

- Schritt 1: Erstellen Sie die DynamoDB-Tabelle für dieses Tutorial
- Schritt 2: Erstellen Sie eine AWS IoT Regel zum Senden von Daten an die DynamoDB-Tabelle
- Schritt 3: Testen Sie die AWS IoT Regel und die DynamoDB-Tabelle
- Schritt 4: Überprüfen Sie die Ergebnisse und die nächsten Schritte

Stellen Sie vor Beginn dieses Tutorials sicher, dass Sie über Folgendes verfügen:

- Einrichten AWS-Konto

  Sie benötigen Ihre AWS-Konto AWS IoT Handkonsole, um dieses Tutorial abzuschließen.
- Überprüft MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen

  Stellen Sie sicher, dass Sie den MQTT Client verwenden können, um ein Thema zu abonnieren und zu veröffentlichen. In diesem Verfahren verwenden Sie den MQTT Client, um Ihre neue Regel zu testen.
- Übersicht über Amazon DynamoDB überprüft

  Wenn Sie DynamoDB noch nicht verwendet haben, lesen Sie Erste Schritte mit DynamoDB, um sich mit den grundlegenden Konzepten und Funktionen von DynamoDB vertraut zu machen.

### Schritt 1: Erstellen Sie die DynamoDB-Tabelle für dieses Tutorial

In diesem Tutorial erstellen Sie eine DynamoDB-Tabelle mit diesen Attributen, um die Daten der imaginären Wettersensorgeräte aufzuzeichnen:

- `sample_time` ist ein Primärschlüssel und beschreibt den Zeitpunkt, zu dem die Probe aufgenommen wurde.
- `device_id` ist ein Sortierschlüssel und beschreibt das Gerät, das die Probe bereitgestellt hat
- `device_data` sind die vom Gerät empfangenen und durch die Regelabfrageanweisung formatierten Daten

#### Erstellen einer DynamoDB-Tabelle für dieses Tutorial

1. Öffnen Sie die DynamoDB-Konsole und wählen Sie Tabelle erstellen aus.
2. Gehen Sie in Tabelle erstellen wie folgt vor:

a. Geben Sie unter Tabellenname den Tabellennamen **`wx_data`** ein.

b. Geben Sie im Feld Partitionsschlüssel **`sample_time`** ein, und wählen Sie **`Number`** in der Optionsliste neben dem Feld aus.

c. Geben Sie im Feld Sortierschlüssel **`device_id`** ein und wählen Sie **`Number`** in der Optionsliste neben dem Feld aus.

d. Wählen Sie unten auf der Seite Erstellen aus.

Sie definieren `device_data` später, wenn Sie die DynamoDB-Regelaktion konfigurieren.

Schritt 2: Erstellen Sie eine AWS IoT Regel zum Senden von Daten an die DynamoDB-Tabelle

In diesem Schritt verwenden Sie die Regelabfrageanweisung, um die Daten der imaginären Wettersensorgeräte so zu formatieren, dass sie in die Datenbanktabelle geschrieben werden.

Ein Beispiel für eine Nachrichtennutzlast, die von einem Wettersensorgerät empfangen wurde, sieht wie folgt aus:

```
{
  "temperature": 28,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

Für den Datenbankeintrag verwenden Sie die Regelabfrageanweisung, um die Struktur der Nutzlast der Nachricht so zu reduzieren, dass sie wie folgt aussieht:

```
{
  "temperature": 28,
  "humidity": 80,
  "barometer": 1013,
  "wind_velocity": 22,
  "wind_bearing": 255
}
```

In dieser Regel verwenden Sie auch ein paar Ersetzungsvorlagen. Ersatzvorlagen sind Ausdrücke, mit denen Sie dynamische Werte aus Funktionen und Nachrichtendaten einfügen können.

Um die AWS IoT Regel zum Senden von Daten an die DynamoDB-Tabelle zu erstellen

1. Öffnen Sie den Regel-Hub der AWS IoT Konsole. Oder Sie können die AWS IoT Startseite innerhalb von öffnen AWS Management Console und zu Nachrichtenweiterleitung>Regeln navigieren.
2. Um mit der Erstellung Ihrer neuen Regel unter Regeln zu beginnen, wählen Sie Regel erstellen aus.
3. In den Regeleigenschaften:

   a. Geben Sie in Role Name (Rollenname) **`wx_data_ddb`** ein.

      Denken Sie daran, dass ein Regelname in Ihrer Region AWS-Konto und Ihrer Region eindeutig sein muss und keine Leerzeichen enthalten darf. Wir haben in diesem Namen einen Unterstrich verwendet, um die beiden Wörter im Namen der Regel voneinander zu trennen.

   b. Beschreiben Sie die Regel in der Regelbeschreibung.

      Eine aussagekräftige Beschreibung macht es einfacher, sich daran zu erinnern, was diese Regel bewirkt und warum Sie sie erstellt haben. Die Beschreibung kann so lang wie nötig sein, also seien Sie so detailliert wie möglich.
4. Wählen Sie Next (Weiter), um fortzufahren.
5. In SQLeiner Erklärung:

   a. Wählen Sie in der SQLVersion aus**`2016-03-23`**.

   b. Geben Sie im Bearbeitungsfeld für den SQLKontoauszug die folgende Aussage ein:

```
SELECT temperature, humidity, barometer,
  wind.velocity as wind_velocity,
  wind.bearing as wind_bearing,
FROM 'device/+/data'
```

      Diese Aussage:

      - Sucht nach MQTT Nachrichten mit einem Thema, das dem `device/+/data` Themenfilter entspricht.

- Formatiert die Elemente des `wind` Attributs als einzelne Attribute.
- Übergibt die `temperature`, `humidity`, und `barometer` Attribute unverändert.

6. Wählen Sie Next (Weiter), um fortzufahren.
7. In Regelaktionen:

   a. Um die Liste der Regelaktionen für diese Regel zu öffnen, wählen Sie in Aktion 1 die Option **`DynamoDB`**.

   > **Note**
   >
   > Stellen Sie sicher, dass Sie DynamoDB und nicht D ynamoDBv 2 als Regelaktion wählen.

   b. Wählen Sie unter Tabellenname den Namen der DynamoDB-Tabelle aus, die Sie in einem vorherigen Schritt erstellt haben: **`wx_data`**

   Die Felder Partitionsschlüsseltyp und Sortierschlüsseltyp werden mit den Werten aus Ihrer DynamoDB-Tabelle gefüllt.

   c. Geben Sie im Feld Partitionsschlüssel den Wert **`sample_time`** ein.

   d. Geben Sie unter Partition key value (Partitions-Schlüsselwert) **`${timestamp()}`** ein.

   Dies ist die erste der Ersetzungsvorlagen, die Sie in dieser Regel verwenden werden. Anstatt einen Wert aus der Nachrichtennutzlast zu verwenden, wird der von der Zeitstempelfunktion zurückgegebene Wert verwendet. Weitere Informationen finden Sie unter Zeitstempel im AWS IoT Core Entwicklerhandbuch.

   e. Geben Sie unter Sort key (Sortierschlüssel) **`device_id`** ein.

   f. Geben Sie unter Sort key value (Schlüsselwert sortieren) **`${cast(topic(2) AS DECIMAL)}`** ein.

   Dies ist der zweite der Ersetzungsvorlagen den Sie in dieser Regel verwenden werden. Es fügt den Wert des zweiten Elements in den Themennamen ein, bei dem es sich um die ID des Geräts handelt, nachdem es ihn in einen DECIMAL Wert umgewandelt hat, der dem numerischen Format des Schlüssels entspricht. Weitere Informationen zu Themen finden Sie unter Thema im AWS IoT Core Entwicklerhandbuch. Weitere Informationen zum Casting finden Sie unter Besetzung im AWS IoT Core Entwicklerhandbuch.

g. Geben Sie in Write message data to this column (Nachrichtendaten in diese Spalte schreiben) **`device_data`** ein.

   Dadurch wird die `device_data` Spalte in der DynamoDB-Tabelle erstellt.

h. Lassen Sie Operation leer.

i. Wählen Sie IAMunter Rolle die Option Neue Rolle erstellen aus.

j. Geben Sie im Dialogfeld Rolle erstellen als Rollenname wx_ddb_role ein. Diese neue Rolle enthält automatisch eine Richtlinie mit dem Präfix "aws-iot-rule", die es der **`wx_data_ddb`** Regel ermöglicht, Daten an die von Ihnen erstellte **`wx_data`** DynamoDB-Tabelle zu senden.

k. Wählen Sie unter IAMRolle die Option. **`wx_ddb_role`**

l. Wählen Sie unten auf der Seite Next (Weiter) aus.

8. Wählen Sie unten auf der Seite Überprüfen und erstellen die Option Erstellen aus, um die Regel zu erstellen.

### Schritt 3: Testen Sie die AWS IoT Regel und die DynamoDB-Tabelle

Um die neue Regel zu testen, verwenden Sie den MQTT Client, um die in diesem Test verwendeten MQTT Nachrichten zu veröffentlichen und zu abonnieren.

Öffnen Sie den MQTTClient in der AWS IoT Konsole in einem neuen Fenster. Auf diese Weise können Sie die Regel bearbeiten, ohne die Konfiguration Ihres MQTT Clients zu verlieren. Der MQTT Client speichert keine Abonnements oder Nachrichtenprotokolle, wenn Sie ihn verlassen, um zu einer anderen Seite in der Konsole zu wechseln. Sie sollten außerdem ein separates Konsolenfenster für den DynamoDB-Tabellen-Hub in der AWS IoT Konsole öffnen, um die neuen Einträge zu sehen, die Ihre Regel sendet.

Um den MQTT Client zum Testen Ihrer Regel zu verwenden

1. Abonnieren Sie im MQTT Client in der AWS IoT Konsole das Eingabethema,`device/+/data`.

   a. Wählen Sie im MQTT Client die Option Thema abonnieren aus.

   b. Geben Sie für Themenfilter das Thema des Eingabethemenfilters **`device/+/data`** ein.

   c. Wählen Sie Subscribe (Abonnieren) aus.

2. Veröffentlichen Sie jetzt eine Nachricht zum Eingabethema mit einer bestimmten Geräte-ID, **`device/22/data`**. Sie können nicht zu MQTT Themen veröffentlichen, die Platzhalterzeichen enthalten.

a. Wählen Sie im MQTT Client die Option In einem Thema veröffentlichen aus.

b. Geben Sie bei Themenname den Namen des eingegebenen Themas ein, **`device/22/data`**.

c. Geben Sie für Nachrichtennutzlast die folgenden Beispieldaten ein.

```
{
  "temperature": 28,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

d. Um die MQTT Nachricht zu veröffentlichen, wählen Sie Veröffentlichen.

e. Wählen Sie nun im MQTT Client ein Thema abonnieren. Wählen Sie in der Spalte Abonnieren das **`device/+/data`** Abonnement aus. Vergewissern Sie sich, dass die Beispieldaten aus dem vorherigen Schritt dort angezeigt werden.

3. Prüfen Sie, ob die Zeile in der DynamoDB-Tabelle angezeigt wird, die Ihre Regel erstellt hat.

a. Wählen Sie im DynamoDB-Tabellen-Hub in der AWS IoT Konsole wx_data und dann die Registerkarte Elemente aus.

Wenn Sie sich bereits auf der Registerkarte Elemente befinden, müssen Sie möglicherweise die Anzeige aktualisieren, indem Sie das Aktualisierungssymbol in der oberen rechten Ecke der Kopfzeile der Tabelle auswählen.

b. Beachten Sie, dass es sich bei den sample_time-Werten in der Tabelle um Links handelt, und öffnen Sie einen. Wenn Sie gerade Ihre erste Nachricht gesendet haben, ist dies die einzige in der Liste.

Dieser Link zeigt alle Daten in dieser Zeile der Tabelle an.

c. Erweitern Sie den Eintrag device_data, um die Daten anzuzeigen, die sich aus der Regelabfrageanweisung ergeben haben.

d. Erkunden Sie die verschiedenen Darstellungen der Daten, die in dieser Anzeige verfügbar sind. Sie können die Daten in dieser Anzeige auch bearbeiten.

e. Wenn Sie die Überprüfung dieser Datenzeile abgeschlossen haben, klicken Sie auf Speichern, um alle von Ihnen vorgenommenen Änderungen zu speichern, oder klicken Sie auf Abbrechen, um den Vorgang zu beenden, ohne die Änderungen zu speichern.

Wenn Sie nicht das richtige Verhalten feststellen, lesen Sie die Tipps zur Fehlerbehebung.

Problembehandlung bei Ihrer DynamoDB-Regel

Hier sind einige Dinge, die Sie überprüfen sollten, falls Sie nicht die erwarteten Ergebnisse sehen.

- Sie haben ein Fehlerbanner

  Wenn bei der Veröffentlichung der Eingabemeldung ein Fehler aufgetreten ist, korrigieren Sie diesen Fehler zuerst. Die folgenden Schritte können Ihnen helfen, diesen Fehler zu korrigieren.
- Die Eingabemeldung wird im Client nicht angezeigt MQTT

  Jedes Mal, wenn Sie Ihre Eingabenachricht zu dem `device/22/data` Thema veröffentlichen, sollte diese Nachricht im MQTT Client erscheinen, sofern Sie den `device/+/data` Themenfilter wie im Verfahren beschrieben abonniert haben.

  Zu überprüfende Dinge

  - Überprüfen Sie den Themenfilter, den Sie abonniert haben

    Wenn Sie das Thema der Eingabenachricht wie im Verfahren beschrieben abonniert haben, sollte Ihnen bei jeder Veröffentlichung eine Kopie der Eingabenachricht angezeigt werden.

    Wenn Sie die Nachricht nicht sehen, überprüfen Sie den Themennamen, den Sie abonniert haben, und vergleichen Sie ihn mit dem Thema, zu dem Sie sie veröffentlicht haben. Bei Themennamen wird Groß- und Kleinschreibung beachtet, und das Thema, das Sie abonniert haben, muss mit dem Thema identisch sein, zu dem Sie die Nachrichtennutzlast veröffentlicht haben.
  - Überprüfen Sie die Funktion zum Veröffentlichen von Nachrichten

    Wählen Sie im MQTT Client unter Abonnements die Option device/+/data aus, überprüfen Sie das Thema der Veröffentlichungsnachricht und wählen Sie dann Als Thema veröffentlichen aus. Sie sollten sehen, dass die Nutzlast der Nachricht aus dem Bearbeitungsfeld unter dem Thema in der Nachrichtenliste erscheinen.
- Sie finden Ihre Daten nicht in der DynamoDB-Tabelle

Als Erstes müssen Sie die Anzeige aktualisieren, indem Sie oben in der Kopfzeile der Tabelle das Aktualisierungssymbol auswählen. Wenn die Daten, nach denen Sie suchen, nicht angezeigt werden, überprüfen Sie Folgendes.

Zu überprüfende Dinge

- Überprüfe den Namen AWS-Region deines MQTT Kunden und die Regel, die du erstellt hast

  Die Konsole, in der Sie den MQTT Client ausführen, muss sich in derselben AWS Region befinden wie die von Ihnen erstellte Regel.
- Überprüfen Sie das Thema der Eingabemeldung in der Regelabfrageanweisung

  Damit die Regel funktioniert, muss sie eine Nachricht mit dem Themennamen erhalten, der dem Themenfilter in der FROM Klausel der Regelabfrageanweisung entspricht.

  Überprüfen Sie die Schreibweise des Themenfilters in der Regelabfrageanweisung mit der Schreibweise des Themas im MQTT Client. Bei Themennamen wird Groß- und Kleinschreibung beachtet, und das Thema der Nachricht muss mit dem Themenfilter in der Regelabfrageanweisung übereinstimmen.
- Überprüfen Sie den Inhalt der Nutzlast der Input-Nachricht

  Damit die Regel funktioniert, muss sie das Datenfeld in der Nachrichtennutzlast finden, das in der SELECT Anweisung deklariert ist.

  Überprüfen Sie die Schreibweise des `temperature` Felds in der Regelabfrageanweisung mit der Schreibweise der Nachrichtennutzdaten im MQTT Client. Bei Feldnamen wird zwischen Groß- und Kleinschreibung unterschieden, und das `temperature` Feld in der Regelabfrageanweisung muss mit dem `temperature` Feld in der Nachrichtennutzlast identisch sein.

  Stellen Sie sicher, dass das JSON Dokument in der Nachrichten-Payload korrekt formatiert ist. Wenn das Fehler JSON enthält, z. B. ein fehlendes Komma, kann die Regel es nicht lesen.
- Überprüfen Sie die Schlüssel- und Feldnamen, die in der Regelaktion verwendet wurden

  Die in der Themenregel verwendeten Feldnamen müssen mit denen in der JSON Nachrichtennutzlast der veröffentlichten Nachricht übereinstimmen.

  Öffnen Sie die Regel, die Sie in der Konsole erstellt haben, und überprüfen Sie die Feldnamen in der Regelaktionskonfiguration mit denen, die im MQTT Client verwendet werden.

- Überprüfen Sie die Rolle, die von der Regel verwendet wird

  Die Regelaktion muss berechtigt sein, das ursprüngliche Thema zu empfangen und das neue Thema zu veröffentlichen.

  Die Richtlinien, die die Regel autorisieren, Nachrichtendaten zu empfangen und die DynamoDB-Tabelle zu aktualisieren, sind spezifisch für die verwendeten Themen. Wenn Sie das von der Regel verwendete Thema oder den Namen der DynamoDB-Tabelle ändern, müssen Sie die Rolle der Regelaktion aktualisieren, damit ihre Richtlinie entsprechend aktualisiert wird.

  Wenn Sie vermuten, dass dies das Problem ist, bearbeiten Sie die Regelaktion und erstellen Sie eine neue Rolle. Neue Rollen, die durch die Regelaktion erstellt wurden, erhalten die erforderlichen Autorisierungen, um diese Aktionen auszuführen.

Schritt 4: Überprüfen Sie die Ergebnisse und die nächsten Schritte

Nachdem Sie mit dieser Regel einige Nachrichten an die DynamoDB-Tabelle gesendet haben, versuchen Sie, damit zu experimentieren, um zu sehen, wie sich Änderungen einiger Aspekte aus dem Tutorial auf die in die Tabelle geschriebenen Daten auswirken. Hier sind einige Ideen, die Ihnen den Einstieg erleichtern sollen.

- Ändern Sie *`device_id`* geben Sie das Thema der Eingabenachricht ein und beobachten Sie die Auswirkung auf die Daten. Sie könnten dies verwenden, um den Empfang von Daten von mehreren Wettersensoren zu simulieren.
- Ändern Sie die in der Regelabfrageanweisung ausgewählten Felder und beobachten Sie die Auswirkungen auf die Daten. Sie könnten dies verwenden, um die in der Tabelle gespeicherten Daten zu filtern.
- Fügen Sie eine Regelaktion zum erneuten Veröffentlichen hinzu, um für jede Zeile, die der Tabelle hinzugefügt wird, eine MQTT Nachricht zu senden. Sie könnten dies zum Debuggen verwenden.

Nachdem Sie dieses Tutorial abgeschlossen haben, besuchen Sie the section called “Formatieren einer Benachrichtigung mithilfe einer Funktion AWS Lambda ”.

## Tutorial: Formatieren einer Benachrichtigung mithilfe einer AWS Lambda Funktion

Dieses Tutorial zeigt, wie MQTT Nachrichtendaten an eine AWS Lambda Aktion gesendet werden, um sie zu formatieren und an einen anderen AWS Dienst zu senden. In diesem Tutorial verwendet die AWS Lambda Aktion, AWS SDK um die formatierte Nachricht an das SNS Amazon-

Thema zu senden, das Sie in der Anleitung zur the section called “Senden einer SNS Amazon-Benachrichtigung” Vorgehensweise erstellt haben.

In der Anleitung zur Vorgehensweise wurde das JSON Dokumentthe section called “Senden einer SNS Amazon-Benachrichtigung”, das sich aus der Abfrageanweisung der Regel ergab, als Hauptteil der Textnachricht gesendet. Das Ergebnis war eine Textnachricht, die in etwa so aussah wie in diesem Beispiel:

```
{"device_id":"32","reported_temperature":38,"max_temperature":30}
```

In diesem Tutorial verwenden Sie eine AWS Lambda Regelaktion, um eine AWS Lambda Funktion aufzurufen, die die Daten aus der Regelabfrageanweisung in ein benutzerfreundlicheres Format formatiert, z. B. in diesem Beispiel:

```
Device 32 reports a temperature of 38, which exceeds the limit of 30.
```

Die AWS Lambda Funktion, die Sie in diesem Tutorial erstellen, formatiert die Nachrichtenzeichenfolge mithilfe der Daten aus der Regelabfrageanweisung und ruft die SNSVeröffentlichungsfunktion von AWS SDK auf, um die Benachrichtigung zu erstellen.

Was Sie in diesem Tutorial lernen werden

- Wie erstellt und testet man eine AWS Lambda Funktion
- So verwenden Sie die AWS Lambda Funktion AWS SDK in an, um eine SNS Amazon-Benachrichtigung zu veröffentlichen
- Wie verwendet man einfache SQL Abfragen und Funktionen in einer Regelabfrageanweisung
- Wie benutzt man den MQTT Client, um eine AWS IoT Regel zu testen

Für dieses Tutorial brauchen Sie ungefähr 45 Minuten.

In diesem Tutorial führen Sie die folgenden Aktivitäten durch:

- Schritt 1: Erstellen Sie eine AWS Lambda Funktion, die eine Textnachricht sendet
- Schritt 2: Erstellen Sie eine AWS IoT Regel mit einer AWS Lambda Regelaktion
- Schritt 3: Testen Sie die AWS IoT Regel und die AWS Lambda Regelaktion
- Schritt 4: Überprüfen Sie die Ergebnisse und die nächsten Schritte

Stellen Sie vor Beginn dieses Tutorials sicher, dass Sie über Folgendes verfügen:

- Einrichten AWS-Konto

  Sie benötigen Ihre AWS-Konto AWS IoT Handkonsole, um dieses Tutorial abzuschließen.

- Überprüft MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen

  Stellen Sie sicher, dass Sie den MQTT Client verwenden können, um ein Thema zu abonnieren und zu veröffentlichen. In diesem Verfahren verwenden Sie den MQTT Client, um Ihre neue Regel zu testen.

- Sie haben die anderen Regel-Tutorials in diesem Abschnitt abgeschlossen

  Für dieses Tutorial ist das SNS Benachrichtigungsthema erforderlich, das Sie in der Anleitung zur Vorgehensweise erstellt habenthe section called “Senden einer SNS Amazon-Benachrichtigung”. Außerdem wird davon ausgegangen, dass Sie die anderen regelbezogenen Tutorials in diesem Abschnitt abgeschlossen haben.

- AWS Lambda Übersicht überprüft

  Wenn Sie Lambda noch nicht verwendet AWS Lambda haben, lesen Sie AWS Lambdaund Erste Schritte mit Lambda, um sich mit den Begriffen und Konzepten vertraut zu machen.

Schritt 1: Erstellen Sie eine AWS Lambda Funktion, die eine Textnachricht sendet

Die AWS Lambda Funktion in diesem Tutorial empfängt das Ergebnis der Regelabfrageanweisung, fügt die Elemente in eine Textzeichenfolge ein und sendet die resultierende Zeichenfolge SNS als Nachricht in einer Benachrichtigung an Amazon.

Im Gegensatz zum Tutorial zur Vorgehensweisethe section called “Senden einer SNS Amazon-Benachrichtigung”, in dem eine AWS IoT Regelaktion zum Senden der Benachrichtigung verwendet wurde, sendet dieses Tutorial die Benachrichtigung von der Lambda-Funktion mithilfe einer Funktion von. AWS SDK Das eigentliche SNS Amazon-Benachrichtigungsthema, das in diesem Tutorial verwendet wird, ist jedoch dasselbe, das Sie im Tutorial zur Vorgehensweise verwendet habenthe section called “Senden einer SNS Amazon-Benachrichtigung”.

Um eine AWS Lambda Funktion zu erstellen, die eine Textnachricht sendet

1. Erstellen Sie eine neue AWS Lambda Funktion.

a. Wählen Sie in der AWS Lambda Konsole die Option Create function (Funktion erstellen) aus.

b. Wählen Sie unter Funktion erstellen die Option Blueprint verwenden aus.

   Suchen Sie nach dem **`hello-world-python`** Blueprint, wählen Sie ihn aus und wählen Sie dann Konfigurieren aus.

c. Unter Grundlegende Informationen:

   i. Geben Sie unter Funktionsname den Namen dieser Funktion ein, **`format-high-temp-notification`**.

   ii. Wählen Sie unter Ausführungsrolle die Option Neue Rolle aus AWS Richtlinienvorlagen erstellen aus.

   iii. Geben Sie im Feld Rollenname den Namen der neuen Rolle ein, **`format-high-temp-notification-role`**.

   iv. Suchen Sie unter Richtlinienvorlagen — optional nach Amazon SNS Publish Policy und wählen Sie diese aus.

   v. Wählen Sie Funktion erstellen aus.

2. Ändern Sie den Blueprint-Code, um ihn zu formatieren und eine SNS Amazon-Benachrichtigung zu senden.

   a. Nachdem Sie Ihre Funktion erstellt haben, sollte die format-high-temp-notificationDetailseite angezeigt werden. Wenn Sie dies nicht tun, öffnen Sie es auf der Seite Lambda Funktionen.

   b. Wählen Sie auf der format-high-temp-notificationDetailseite die Registerkarte Konfiguration und scrollen Sie zum Bereich Funktionscode.

   c. Wählen Sie im Fenster Funktionscode im Bereich Umgebung die Python-Datei `lambda_function.py` aus.

   d. Löschen Sie im Fenster Funktionscode den gesamten ursprünglichen Programmcode aus dem Blueprint und ersetzen Sie ihn durch diesen Code.

```
import boto3
#
#   expects event parameter to contain:
#   {
#       "device_id": "32",
#       "reported_temperature": 38,
#       "max_temperature": 30,
```

```
#       "notify_topic_arn": "arn:aws:sns:us-
east-1:57EXAMPLE833:high_temp_notice"
#   }
#
#   sends a plain text string to be used in a text message
#
#      "Device {0} reports a temperature of {1}, which exceeds the limit of
 {2}."
#
#   where:
#       {0} is the device_id value
#       {1} is the reported_temperature value
#       {2} is the max_temperature value
#
def lambda_handler(event, context):

    # Create an SNS client to send notification
    sns = boto3.client('sns')

    # Format text message from data
    message_text = "Device {0} reports a temperature of {1}, which exceeds the
 limit of {2}.".format(
            str(event['device_id']),
            str(event['reported_temperature']),
            str(event['max_temperature'])
        )

    # Publish the formatted message
    response = sns.publish(
            TopicArn = event['notify_topic_arn'],
            Message = message_text
        )

    return response
```

e. Wählen Sie Bereitstellen.

3. Suchen Sie in einem neuen Fenster den Amazon-Ressourcennamen (ARN) Ihres SNS Amazon-Themas aus dem Tutorial zur Vorgehensweisethe section called “Senden einer SNS Amazon-Benachrichtigung”.

   a. Öffnen Sie in einem neuen Fenster die Themenseite der SNS Amazon-Konsole.

b. Suchen Sie auf der Seite Themen in der Liste der Amazon-Themen nach dem Benachrichtigungsthema high_temp_notice. SNS

c. Suchen Sie das ARNBenachrichtigungsthema high_temp_notice, das Sie im nächsten Schritt verwenden möchten.

4. Erstellen Sie einen Testfall für Ihre Lambda-Funktion.

a. Wählen Sie auf der Seite Lambda-Funktionen der Konsole auf der format-high-temp-notificationDetailseite in der oberen rechten Ecke der Seite die Option Testereignis auswählen aus (auch wenn es deaktiviert aussieht) und wählen Sie dann Testereignisse konfigurieren aus.

b. Wählen Sie unter Testereignis konfigurieren die Option Neues Testereignis erstellen.

c. Geben Sie unter Event name (Ereignisname) **`SampleRuleOutput`** ein.

d. Fügen Sie dieses JSON Beispieldokument im JSON Editor unter dem Namen des Ereignisses ein. Dies ist ein Beispiel dafür, was Ihre AWS IoT Regel an die Lambda-Funktion sendet.

```
{
  "device_id": "32",
  "reported_temperature": 38,
  "max_temperature": 30,
  "notify_topic_arn": "arn:aws:sns:us-east-1:57EXAMPLE833:high_temp_notice"
}
```

e. Rufen Sie das Fenster auf, das das ARNBenachrichtigungsthema high_temp_notice enthält, und kopieren Sie den Wert. ARN

f. Ersetzen Sie den `notify_topic_arn` Wert im JSON Editor durch den Wert ARN aus Ihrem Benachrichtigungsthema.

Lassen Sie dieses Fenster geöffnet, damit Sie diesen ARN Wert erneut verwenden können, wenn Sie die AWS IoT Regel erstellen.

g. Wählen Sie Create (Erstellen) aus.

5. Testen Sie die Funktion mit Beispieldaten.

a. Vergewissern Sie sich, dass auf der format-high-temp-notificationDetailseite in der oberen rechten Ecke der Seite neben der Schaltfläche Testen SampleRuleOutputangezeigt wird. Wenn nicht, wählen Sie es aus der Liste der verfügbaren Testereignisse aus.

b. Um die Ausgabenachricht der Beispielregel an Ihre Funktion zu senden, wählen Sie Test.

Wenn sowohl die Funktion als auch die Benachrichtigung funktioniert haben, erhalten Sie eine Textnachricht auf dem Telefon, das die Benachrichtigung abonniert hat.

Wenn Sie am Telefon keine Textnachricht erhalten haben, überprüfen Sie das Ergebnis des Vorgangs. Überprüfen Sie im Bereich Funktionscode auf der Registerkarte Ausführungsergebnisse die Antwort auf aufgetretene Fehler. Fahren Sie erst mit dem nächsten Schritt fort, wenn Ihre Funktion die Benachrichtigung an Ihr Telefon senden kann.

Schritt 2: Erstellen Sie eine AWS IoT Regel mit einer AWS Lambda Regelaktion

In diesem Schritt verwenden Sie die Regelabfrageanweisung, um die Daten vom imaginären Wettersensorgerät zu formatieren, um sie an eine Lambda-Funktion zu senden, die eine Textnachricht formatiert und sendet.

Ein Beispiel für eine von den Wettergeräten empfangene Nachrichtennutzlast sieht wie folgt aus:

```
{
  "temperature": 28,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

In dieser Regel verwenden Sie die Regelabfrageanweisung, um eine Nachrichtennutzlast für die Lambda-Funktion zu erstellen, die wie folgt aussieht:

```
{
  "device_id": "32",
  "reported_temperature": 38,
  "max_temperature": 30,
  "notify_topic_arn": "arn:aws:sns:us-east-1:57EXAMPLE833:high_temp_notice"
}
```

Dies enthält alle Informationen, die die Lambda-Funktion benötigt, um die richtige Textnachricht zu formatieren und zu senden.

Um die AWS IoT Regel zum Aufrufen einer Lambda-Funktion zu erstellen

1. Öffnen Sie den Regel-Hub der AWS IoT Konsole.

2. Um mit der Erstellung Ihrer neuen Regel unter Regeln zu beginnen, wählen Sie Erstellen.
3. Gehen Sie im oberen Teil von Regel erstellen wie folgt vor:

   a. Geben Sie im Feld Name den Namen der Regel ein, **`wx_friendly_text`**.

      Denken Sie daran, dass ein Regelname in Ihrer Region AWS-Konto und in Ihrer Region eindeutig sein muss und keine Leerzeichen enthalten darf. Wir haben in diesem Namen einen Unterstrich verwendet, um die beiden Wörter im Namen der Regel voneinander zu trennen.

   b. Beschreiben Sie die Regel im Feld Beschreibung.

      Eine aussagekräftige Beschreibung macht es einfacher, sich daran zu erinnern, was diese Regel bewirkt und warum Sie sie erstellt haben. Die Beschreibung kann so lang wie nötig sein, also seien Sie so detailliert wie möglich.

4. In der Regelabfrageanweisung von Regel erstellen:

   a. Wählen Sie unter SQL Version verwenden die Option aus**`2016-03-23`**.

   b. Geben Sie im Bearbeitungsfeld Regelabfrageanweisung die folgende Anweisung ein:

```
SELECT
  cast(topic(2) AS DECIMAL) as device_id,
  temperature as reported_temperature,
  30 as max_temperature,
  'arn:aws:sns:us-east-1:57EXAMPLE833:high_temp_notice' as notify_topic_arn
FROM 'device/+/data' WHERE temperature > 30
```

   Diese Aussage:

   - Sucht nach MQTT Nachrichten mit einem Thema, das dem `device/+/data` Themenfilter entspricht und deren `temperature` Wert größer als 30 ist.
   - Wählt das zweite Element aus der Themenzeichenfolge aus, konvertiert es in eine Dezimalzahl und weist es dann dem `device_id` Feld zu.
   - Wählt den Wert des `temperature` Felds aus der Nachrichtennutzlast aus und weist ihn dem `reported_temperature` Feld zu.
   - Erstellt einen konstanten Wert, `30`, um den Grenzwert darzustellen, und weist ihn dem `max_temperature` Feld zu.
   - Erstellt einen konstanten Wert für das `notify_topic_arn` Feld.

c. Suchen Sie im Fenster nach, das das ARNBenachrichtigungsthema high_temp_notice enthält, und kopieren Sie den Wert. ARN

d. Ersetzen Sie den Wert (ARN*arn:aws:sns:us-east-1:57EXAMPLE833:high_temp_notice*) im Editor für Regelabfrageanweisungen mit dem Thema ARN Ihres Benachrichtigungsthemas.

5. Gehen Sie im Feld Eine oder mehrere Aktionen festlegen wie folgt vor:

a. Um die Liste der Regelaktionen für diese Regel zu öffnen, wählen Sie Aktion hinzufügen.

b. Wählen Sie unter Aktion auswählen die Option Nachricht an eine Lambda-Funktion senden aus.

c. Um die Konfigurationsseite der ausgewählten Aktion zu öffnen, wählen Sie unten in der Aktionsliste die Option Aktion konfigurieren aus.

6. Gehen Sie in Aktion konfigurieren wie folgt vor:

a. Wählen Sie unter Funktionsname die Option Auswählen aus.

b. Wählen Sie format-high-temp-notification.

c. Wählen Sie unten im Bereich Aktion konfigurieren die Option Aktion hinzufügen aus.

d. Um die Regel zu erstellen, wählen Sie unten im Bereich Eine Regel erstellen die Option Regel erstellen aus.

### Schritt 3: Testen Sie die AWS IoT Regel und die AWS Lambda Regelaktion

Um Ihre neue Regel zu testen, verwenden Sie den MQTT Client, um die von dieser Regel verwendeten MQTT Nachrichten zu veröffentlichen und zu abonnieren.

Öffnen Sie den MQTTClient in der AWS IoT Konsole in einem neuen Fenster. Jetzt können Sie die Regel bearbeiten, ohne die Konfiguration Ihres MQTT Clients zu verlieren. Wenn Sie den MQTT Client verlassen, um zu einer anderen Seite in der Konsole zu wechseln, verlieren Sie Ihre Abonnements oder Nachrichtenprotokolle.

Um den MQTT Client zum Testen Ihrer Regel zu verwenden

1. Abonnieren Sie im MQTT Client in der AWS IoT Konsole die Eingabethemen, in diesem Fall`device/+/data`.

a. Wählen Sie im MQTT Client unter Abonnements die Option Thema abonnieren aus.

b. Geben Sie im Abonnementthema das Thema des Eingabethemenfilters **`device/+/data`** ein.

c. Belassen Sie die übrigen Felder auf ihren Standardeinstellungen.

d. Wählen Sie Thema abonnieren aus.

   In der Spalte Abonnements wird **`device/+/data`** unter In einem Thema veröffentlichen angezeigt.

2. Veröffentlichen Sie eine Nachricht zum Eingabethema mit einer bestimmten Geräte-ID, **`device/32/data`**. Sie können nicht zu MQTT Themen veröffentlichen, die Platzhalterzeichen enthalten.

   a. Wählen Sie im MQTT Client unter Abonnements die Option Als Thema veröffentlichen aus.

   b. Geben Sie im Feld Veröffentlichen den Namen des Eingabethemas **`device/32/data`** ein.

   c. Kopieren Sie die hier gezeigten Beispieldaten und fügen Sie die Beispieldaten in das Bearbeitungsfeld unter dem Themennamen ein.

```
{
  "temperature": 38,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

   d. Um Ihre MQTT Nachricht zu veröffentlichen, wählen Sie Im Thema veröffentlichen.

3. Bestätigen Sie, dass die Textnachricht gesendet wurde.

   a. Im MQTT Client befindet sich unter Abonnements ein grüner Punkt neben dem Thema, das Sie zuvor abonniert haben.

      Der grüne Punkt zeigt an, dass eine oder mehrere neue Nachrichten eingegangen sind, seit Sie sie das letzte Mal angesehen haben.

   b. Wählen Sie unter Abonnements die Option Gerät/+/Daten aus, um zu überprüfen, ob die Nutzlast der Nachricht mit dem übereinstimmt, was Sie gerade veröffentlicht haben, und wie folgt aussieht:

```
{
  "temperature": 38,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

c. Überprüfe das Telefon, mit dem du das SNS Thema abonniert hast, und vergewissere dich, dass der Inhalt der Nachrichten-Payload wie folgt aussieht:

```
Device 32 reports a temperature of 38, which exceeds the limit of 30.
```

Wenn Sie das Thema-ID-Element im Nachrichtenthema ändern, denken Sie daran, dass die Umwandlung des `topic(2)` Werts in einen numerischen Wert nur funktioniert, wenn dieses Element im Nachrichtenthema nur numerische Zeichen enthält.

4. Versuchen Sie, eine MQTT Nachricht zu senden, bei der die Temperatur den Grenzwert nicht überschreitet.

a. Wählen Sie im MQTT Client unter Abonnements die Option Als Thema veröffentlichen aus.

b. Geben Sie im Feld Veröffentlichen den Namen des Eingabethemas **`device/33/data`** ein.

c. Kopieren Sie die hier gezeigten Beispieldaten und fügen Sie die Beispieldaten in das Bearbeitungsfeld unter dem Themennamen ein.

```
{
  "temperature": 28,
  "humidity": 80,
  "barometer": 1013,
  "wind": {
    "velocity": 22,
    "bearing": 255
  }
}
```

d. Um Ihre MQTT Nachricht zu senden, wählen Sie Im Thema veröffentlichen.

Sie sollten die Nachricht sehen, die Sie im **`device/+/data`** Abonnement gesendet haben. Da der Temperaturwert jedoch unter der Höchsttemperatur in der Regelabfrageanweisung liegt, sollten Sie keine Textnachricht erhalten.

Wenn Sie nicht das richtige Verhalten feststellen, lesen Sie die Tipps zur Fehlerbehebung.

Problembehandlung bei Ihrer AWS Lambda Regel und Benachrichtigung

Hier sind einige Dinge, die Sie überprüfen sollten, falls Sie nicht die erwarteten Ergebnisse sehen.

- Sie haben ein Fehlerbanner

  Wenn bei der Veröffentlichung der Eingabemeldung ein Fehler aufgetreten ist, korrigieren Sie diesen Fehler zuerst. Die folgenden Schritte können Ihnen helfen, diesen Fehler zu korrigieren.
- Sie sehen die Eingabemeldung nicht im MQTT Client

  Jedes Mal, wenn Sie Ihre Eingabenachricht zu dem `device/32/data` Thema veröffentlichen, sollte diese Nachricht im MQTT Client erscheinen, sofern Sie den `device/+/data` Themenfilter wie im Verfahren beschrieben abonniert haben.

  Zu überprüfende Dinge

  - Überprüfen Sie den Themenfilter, den Sie abonniert haben

    Wenn Sie das Thema der Eingabenachricht wie im Verfahren beschrieben abonniert haben, sollte Ihnen bei jeder Veröffentlichung eine Kopie der Eingabenachricht angezeigt werden.

    Wenn Sie die Nachricht nicht sehen, überprüfen Sie den Themennamen, den Sie abonniert haben, und vergleichen Sie ihn mit dem Thema, zu dem Sie sie veröffentlicht haben. Bei Themennamen wird Groß- und Kleinschreibung beachtet, und das Thema, das Sie abonniert haben, muss mit dem Thema identisch sein, zu dem Sie die Nachrichtennutzlast veröffentlicht haben.
  - Überprüfen Sie die Funktion zum Veröffentlichen von Nachrichten

    Wählen Sie im MQTT Client unter Abonnements die Option device/+/data aus, überprüfen Sie das Thema der Veröffentlichungsnachricht und wählen Sie dann Als Thema veröffentlichen aus. Sie sollten sehen, dass die Nutzlast der Nachricht aus dem Bearbeitungsfeld unter dem Thema in der Nachrichtenliste erscheinen.

- Sie erhalten keine Nachricht SMS

  Damit Ihre Regel funktioniert, muss sie über die richtige Richtlinie verfügen, die sie autorisiert, eine Nachricht zu empfangen und eine SNS Benachrichtigung zu senden, und sie muss die Nachricht empfangen.

  Zu überprüfende Dinge

  - Überprüfen Sie die AWS-Region Ihres MQTT Clients und die Regel, die Sie erstellt haben

    Die Konsole, in der Sie den MQTT Client ausführen, muss sich in derselben AWS Region befinden wie die von Ihnen erstellte Regel.
  - Überprüfen Sie, ob der Temperaturwert in der Nachrichtennutzlast den Testschwellenwert überschreitet

    Wenn der Temperaturwert kleiner oder gleich 30 ist, wie in der Regelabfrageanweisung definiert, führt die Regel keine ihrer Aktionen aus.
  - Überprüfen Sie das Thema der Eingabemeldung in der Regelabfrageanweisung

    Damit die Regel funktioniert, muss sie eine Nachricht mit dem Themennamen erhalten, der dem Themenfilter in der FROM Klausel der Regelabfrageanweisung entspricht.

    Überprüfen Sie die Schreibweise des Themenfilters in der Regelabfrageanweisung mit der Schreibweise des Themas im MQTT Client. Bei Themennamen wird Groß- und Kleinschreibung beachtet, und das Thema der Nachricht muss mit dem Themenfilter in der Regelabfrageanweisung übereinstimmen.
  - Überprüfen Sie den Inhalt der Nutzlast der Input-Nachricht

    Damit die Regel funktioniert, muss sie das Datenfeld in der Nachrichtennutzlast finden, das in der SELECT Anweisung deklariert ist.

    Überprüfen Sie die Schreibweise des `temperature` Felds in der Regelabfrageanweisung mit der Schreibweise der Nachrichtennutzdaten im MQTT Client. Bei Feldnamen wird zwischen Groß- und Kleinschreibung unterschieden, und das `temperature` Feld in der Regelabfrageanweisung muss mit dem `temperature` Feld in der Nachrichtennutzlast identisch sein.

    Stellen Sie sicher, dass das JSON Dokument in der Nachrichten-Payload korrekt formatiert ist. Wenn das Fehler JSON enthält, z. B. ein fehlendes Komma, kann die Regel es nicht lesen.

- Überprüfen Sie die SNS Amazon-Benachrichtigung

  In Schritt 3 wird beschriebenSchritt 1: Erstellen Sie ein SNS Amazon-Thema, das eine SMS Textnachricht sendet, wie Sie die SNS Amazon-Benachrichtigung testen und die Benachrichtigung testen, um sicherzustellen, dass die Benachrichtigung funktioniert.

- Überprüfen Sie die Lambda-Funktion

  Unter Schritt 1: Erstellen Sie eine AWS Lambda Funktion, die eine Textnachricht sendet, lesen Sie Schritt 5, in dem beschrieben wird, wie Sie die Lambda-Funktion anhand von Testdaten testen und die Lambda-Funktion testen.

- Überprüfen Sie die Rolle, die von der Regel verwendet wird

  Die Regelaktion muss berechtigt sein, das ursprüngliche Thema zu empfangen und das neue Thema zu veröffentlichen.

  Die Richtlinien, mit denen die Regel autorisiert wird, Nachrichtendaten zu empfangen und erneut zu veröffentlichen, sind spezifisch für die verwendeten Themen. Wenn Sie das Thema ändern, das für die erneute Veröffentlichung der Nachrichtendaten verwendet wird, müssen Sie die Rolle der Regelaktion aktualisieren, damit ihre Richtlinie dem aktuellen Thema entspricht.

  Wenn Sie vermuten, dass dies das Problem ist, bearbeiten Sie die Aktion Regel erneut veröffentlichen und erstellen Sie eine neue Rolle. Neue Rollen, die durch die Regelaktion erstellt wurden, erhalten die erforderlichen Autorisierungen, um diese Aktionen auszuführen.

### Schritt 4: Überprüfen Sie die Ergebnisse und die nächsten Schritte

In diesem Tutorial:

- Sie haben eine AWS IoT Regel zum Aufrufen einer Lambda-Funktion erstellt, die eine SNS Amazon-Benachrichtigung gesendet hat, die Ihre benutzerdefinierte Nachrichtennutzlast verwendet hat.
- Sie haben eine einfache SQL Abfrage und Funktionen in einer Regelabfrageanweisung verwendet, um eine neue Nachrichtennutzlast für Ihre Lambda-Funktion zu erstellen.
- Sie haben den MQTT Client verwendet, um Ihre AWS IoT Regel zu testen.

### Nächste Schritte

Nachdem Sie einige Textnachrichten mit dieser Regel gesendet haben, versuchen Sie, damit zu experimentieren, um zu sehen, wie sich Änderungen einiger Aspekte des Tutorials auf die Nachricht auswirken und wann sie gesendet wird. Hier sind einige Ideen, die Ihnen den Einstieg erleichtern sollen.

- Ändern Sie die *device_id* im Thema der Eingangsnachricht und beobachten Sie die Auswirkung auf den Inhalt der Textnachricht.
- Ändern Sie die in der Regelabfrageanweisung ausgewählten Felder, aktualisieren Sie die Lambda-Funktion, um sie in einer neuen Nachricht zu verwenden, und beobachten Sie die Auswirkungen im Inhalt der Textnachricht.
- Ändern Sie den Test in der Regelabfrageanweisung so, dass er auf eine Mindesttemperatur statt auf eine Höchsttemperatur testet. Aktualisieren Sie die Lambda-Funktion, um eine neue Nachricht zu formatieren, und denken Sie daran, den Namen von `max_temperature` zu ändern.
- Weitere Informationen zum Auffinden von Fehlern, die bei der Entwicklung und Verwendung von AWS IoT Regeln auftreten können, finden Sie unterÜberwachung AWS IoT.

## Beibehalten des Gerätestatus mit Geräteschatten, während das Gerät offline ist

In diesen Tutorials erfahren Sie, wie Sie den AWS IoT Device Shadow-Dienst verwenden, um die Statusinformationen eines Geräts zu speichern und zu aktualisieren. Das Schattendokument, bei dem es sich um ein JSON-Dokument handelt, zeigt die Änderung des Gerätestatus auf der Grundlage der von einem Gerät, einer lokalen App oder einem Dienst veröffentlichten Nachrichten. In diesem Tutorial zeigt das Schattendokument die Änderung der Farbe einer Glühbirne. In diesen Tutorials wird auch gezeigt, wie der Schatten diese Informationen auch dann speichert, wenn das Gerät nicht mit dem Internet verbunden ist, und die neuesten Statusinformationen an das Gerät zurückgibt, wenn es wieder online ist und diese Informationen anfordert.

Wir empfehlen Ihnen, diese Tutorials in der Reihenfolge anzusehen, in der sie hier gezeigt werden. Beginnen Sie dabei mit den AWS IoT -Ressourcen, die Sie erstellen müssen, und der erforderlichen Hardwarekonfiguration, damit Sie die Konzepte schrittweise erlernen können. Diese Tutorials zeigen, wie Sie ein Raspberry Pi-Gerät zur Verwendung mit konfigurieren und anschließen AWS IoT. Wenn Sie nicht über die erforderliche Hardware verfügen, können Sie diesen Tutorials folgen, indem Sie sie an ein Gerät Ihrer Wahl anpassen oder ein virtuelles Gerät mit Amazon erstellen EC2.

Übersicht über Tutorial-Szenario

Das Szenario für diese Tutorials ist eine lokale App oder ein Dienst, der die Farbe einer Glühbirne ändert und deren Daten in reservierten Schattenthemen veröffentlicht. Diese Tutorials ähneln der Geräteschatten-Funktionalität, die im interaktiven Tutorial „Erste Schritte“ beschrieben wurde, und sind auf einem Raspberry Pi-Gerät implementiert. Die Tutorials in diesem Abschnitt konzentrieren sich auf einen einzelnen, klassischen Schatten und zeigen, wie Sie benannte Schatten oder mehrere Geräte unterbringen können.

In den folgenden Tutorials erfahren Sie, wie Sie den AWS IoT Device Shadow-Dienst verwenden.

- Tutorial: Ihren Raspberry Pi für die Ausführung der Schattenanwendung vorbereiten

  Dieses Tutorial zeigt, wie Sie ein Raspberry Pi-Gerät für die Verbindung einrichten AWS IoT. Außerdem erstellen Sie ein AWS IoT Richtliniendokument und eine Ding-Ressource, laden die Zertifikate herunter und hängen dann die Richtlinie an diese Ding-Ressource an. Für dieses Tutorial brauchen Sie ungefähr 30 Minuten.

- Tutorial: Installation des Geräte-SDK und Ausführen der Beispielanwendung für Geräteschatten

  Dieses Tutorial zeigt, wie Sie die erforderlichen Tools, Software und das AWS IoT Geräte-SDK für Python installieren und anschließend die Shadow-Beispielanwendung ausführen. Dieses Tutorial baut auf den unter Verbinden eines Raspberry Pi oder eines anderes Gerätes vorgestellten Konzepten auf und nimmt 20 Minuten in Anspruch.

- Tutorial: Interaktion mit Geräteschatten mithilfe der Beispiel-App und des MQTT-Testclients

  Dieses Tutorial zeigt, wie Sie mithilfe der `shadow.py` Beispiel-App und der AWS IoT Konsole die Interaktion zwischen AWS IoT Device Shadows und den Zustandsänderungen der Glühbirne beobachten. Das Tutorial zeigt auch, wie Sie MQTT-Nachrichten an die reservierten Geräteschattenthemen senden. Für dieses Tutorial brauchen Sie ungefähr 45 Minuten.

## AWS IoT Device Shadow-Übersicht

Ein Device Shadow ist eine persistente, virtuelle Darstellung eines Geräts, das von einer Dingressource verwaltet wird, die Sie in der AWS IoT Registrierung erstellen. Das Shadow-Dokument ist ein JSON- oder JavaScript Notationsdokument, das zum Speichern und Abrufen der aktuellen Statusinformationen für ein Gerät verwendet wird. Sie können den Shadow verwenden, um den Status eines Geräts über MQTT-Themen oder HTTP-REST abzurufen und festzulegen APIs, unabhängig davon, ob das Gerät mit dem Internet verbunden ist.

Das Schattendokument enthält eine `state`-Eigenschaft, die die folgenden Aspekte des Gerätezustands beschreibt.

- `desired`: Apps geben die gewünschten Status der Geräteeigenschaften an, indem sie das `desired`-Objekt aktualisieren.
- `reported`: Geräte melden ihren aktuellen Status im `reported`-Objekt.
- `delta`: AWS IoT meldet Unterschiede zwischen dem gewünschten und dem gemeldeten Status im `delta` Objekt.

Hier sehen Sie ein Beispiel für ein Schattenstatusdokument.

```
{
  "state": {
    "desired": {
      "color": "green"
      },
    "reported": {
      "color": "blue"
      },
    "delta": {
      "color": "green"
      }
   }
}
```

Um das Shadow-Dokument eines Geräts zu aktualisieren, können Sie die reservierten MQTT-Themen, den Device Shadow-REST APIs`GET`, der die`UPDATE`, und `DELETE` -Operationen mit HTTP unterstützt, und die AWS IoT CLI verwenden.

Nehmen wir im vorherigen Beispiel an, Sie möchten die `desired` Farbe in `yellow` ändern. Senden Sie dazu eine Anfrage an die UpdateThingShadow API oder veröffentlichen Sie eine Nachricht zum Thema Aktualisieren`$aws/things/THING_NAME/shadow/update`.

```
{
  "state": {
    "desired": {
      "color": yellow
    }
  }
}
```

Aktualisierungen betreffen lediglich die in der Anfrage angegebenen Felder. Veröffentlichen Sie nach erfolgreicher Aktualisierung von Device Shadow den neuen `desired` Status im `delta` Thema,`$aws/things/THING_NAME/shadow/delta`. AWS IoT Das Schattendokument sieht in diesem Fall so aus:

```
{
  "state": {
    "desired": {
      "color": yellow
    },
    "reported": {
      "color": green
    },
    "delta": {
      "color": yellow
      }
  }
}
```

Der neue Status wird dann dem AWS IoT Device Shadow unter Verwendung des `Update` Themas `$aws/things/THING_NAME/shadow/update` mit der folgenden JSON-Nachricht gemeldet:

```
{
  "state": {
    "reported": {
      "color": yellow
    }
  }
}
```

Wenn Sie die aktuellen Statusinformationen abrufen möchten, senden Sie eine Anfrage an die GetThingShadow API oder veröffentlichen Sie eine MQTT-Nachricht im Thema Get`$aws/things/THING_NAME/shadow/get`.

Weitere Informationen zur Verwendung des Geräteschattendienstes finden Sie in AWS IoT Device Shadow-Dienst.

Weitere Informationen zur Verwendung von Geräteschatten in Geräten, Apps und Diensten finden Sie unter Verwenden von Schatten in Geräten und Verwenden von Schatten in Apps und Services.

Informationen zur Interaktion mit AWS IoT Schatten finden Sie unterInteraktion mit Schatten.

Informationen zu den reservierten MQTT-Themen und zu HTTP-REST APIs finden Sie unter MQTT-Themen für Geräteschatten undGeräteschatten-REST-API.

## Tutorial: Ihren Raspberry Pi für die Ausführung der Schattenanwendung vorbereiten

Dieses Tutorial zeigt, wie Sie ein Raspberry Pi-Gerät einrichten und konfigurieren und die AWS IoT Ressourcen erstellen, die ein Gerät benötigt, um eine Verbindung herzustellen und MQTT-Nachrichten auszutauschen.

> **Note**
>
> Wenn Sie the section called “Erstellen Sie ein virtuelles Gerät mit Amazon EC2” planen, können Sie diese Seite überspringen und mit the section called “Konfigurieren Ihres Geräts” weitermachen. Sie werden diese Ressourcen erstellen, wenn Sie Ihr virtuelles Objekt erstellen. Wenn Sie anstelle des Raspberry Pi ein anderes Gerät verwenden möchten, können Sie versuchen, diese Anleitungen zu befolgen, indem Sie sie an ein Gerät Ihrer Wahl anpassen.

In diesem Kurs lernen Sie Folgendes:

- Richten Sie ein Raspberry Pi-Gerät ein und konfigurieren Sie es für die Verwendung mit AWS IoT.
- Erstellen Sie ein AWS IoT Richtliniendokument, das Ihr Gerät zur Interaktion mit AWS IoT Diensten autorisiert.
- Erstellen Sie eine Ding-Ressource in AWS IoT den X.509-Gerätezertifikaten und hängen Sie dann das Richtliniendokument an.

  Das Objekt ist die virtuelle Darstellung Ihres Geräts in der AWS IoT Registrierung. Das Zertifikat authentifiziert Ihr Gerät gegenüber AWS IoT Core, und das Richtliniendokument autorisiert Ihr Gerät zur Interaktion mit Core. AWS IoT

So führen Sie dieses Tutorial aus

Um die `shadow.py` Beispielanwendung für Geräteschatten auszuführen, benötigen Sie ein Raspberry Pi-Gerät, das eine Verbindung zu AWS IoT herstellt. Wir empfehlen, dass Sie dieses Tutorial in der Reihenfolge folgen, in der es hier vorgestellt wird. Beginnen Sie mit der Einrichtung des Raspberry Pi und seines Zubehörs, erstellen Sie dann eine Richtlinie und fügen Sie die Richtlinie einer von Ihnen erstellten Objekt-Ressource hinzu. Anschließend können Sie diesem Tutorial folgen,

indem Sie die vom Raspberry Pi unterstützte grafische Benutzeroberfläche (GUI) verwenden, um die AWS IoT Konsole im Webbrowser des Geräts zu öffnen. Dadurch ist es auch einfacher, die Zertifikate direkt auf Ihren Raspberry Pi herunterzuladen, um eine Verbindung herzustellen. AWS IoT

Stellen Sie vor Beginn dieses Tutorials sicher, dass Sie über Folgendes verfügen:

- Ein AWS-Konto. Wenn dies nicht der Fall ist, führen Sie die unter Einrichten AWS-Konto beschriebenen Schritte aus, bevor Sie fortfahren. Sie benötigen Ihre AWS-Konto AWS IoT Handkonsole, um dieses Tutorial abzuschließen.
- Der Raspberry Pi und das notwendige Zubehör. Sie benötigen:
  - Ein Raspberry Pi 3 Modell B oder ein neueres Modell. Dieses Tutorial funktioniert möglicherweise auf früheren Versionen des Raspberry Pi, aber wir haben es nicht getestet.
  - Raspberry Pi OS (32-Bit) oder höher. Wir empfehlen die neueste Version des Raspberry Pi OS zu verwenden. Frühere Versionen des Betriebssystems funktionieren möglicherweise, aber wir haben es nicht getestet.
  - Eine Ethernet- oder WLAN-Verbindung.
  - Tastatur, Maus, Monitor, Kabel und Netzteile.

Für dieses Tutorial brauchen Sie ungefähr 30 Minuten.

Schritt 1: Einrichten und Konfigurieren des Raspberry Pi-Geräts

In diesem Abschnitt konfigurieren wir ein Raspberry Pi-Gerät für die Verwendung mit AWS IoT.

> **Important**
>
> Die Anpassung dieser Anweisungen an andere Geräte und Betriebssysteme kann eine Herausforderung sein. Sie müssen Ihr Gerät gut genug verstehen, um diese Anweisungen interpretieren und auf Ihr Gerät anwenden zu können. Wenn Sie auf Schwierigkeiten stoßen, können Sie alternativ eine der anderen Geräteoptionen ausprobieren, z. B. Erstellen Sie ein virtuelles Gerät mit Amazon EC2 oderVerwenden Sie Ihren Windows- oder Linux-PC oder Mac als Gerät AWS IoT.

Sie müssen Ihren Raspberry Pi so konfigurieren, dass er das Betriebssystem (OS) starten, eine Verbindung zum Internet herstellen und Ihnen die Interaktion mit ihm über eine Befehlszeilenschnittstelle ermöglicht. Sie können auch die vom Raspberry Pi unterstützte grafische

Benutzeroberfläche (GUI) verwenden, um die AWS IoT Konsole zu öffnen und den Rest dieses Tutorials auszuführen.

So richten Sie den Raspberry Pi ein

1. Setzen Sie die SD-Karte in den MicroSD-Kartensteckplatz im Raspberry Pi ein. Auf einigen SD-Karten ist ein Installationsmanager vorinstalliert, der Sie nach dem Booten der Karte mit einem Menü zur Installation des Betriebssystems auffordert. Sie können auch den Raspberry Pi-Imager verwenden, um das Betriebssystem auf Ihrer Karte zu installieren.
2. Schließen Sie ein HDMI TV oder einen HDMI-Monitor an das HDMI-Kabel an, das an den HDMI-Anschluss des Raspberry Pi angeschlossen ist.
3. Schließe Sie Tastatur und Maus an die USB-Anschlüsse des Raspberry Pi an und schließen Sie dann den Netzadapter an, um die Platine zu starten.

Wenn nach dem Start des Raspberry Pi der Installationsmanager auf der SD-Karte vorinstalliert war, erscheint ein Menü zur Installation des Betriebssystems. Wenn Sie Probleme bei der Installation des Betriebssystems haben, können Sie die folgenden Schritte ausführen. Weitere Informationen zum Einrichten von Raspberry Pi finden Sie unter Einrichten Ihres Raspberry Pi.

Wenn Sie Probleme beim Einrichten des Raspberry Pi haben:

- Überprüfen Sie, ob Sie die SD-Karte eingelegt haben, bevor Sie das Board starten. Wenn Sie die SD-Karte nach dem Booten des Boards einstecken, wird das Installationsmenü möglicherweise nicht angezeigt.
- Vergewissern Sie sich, dass das TV oder der Monitor eingeschaltet und der richtige Eingang ausgewählt ist.
- Stellen Sie sicher, dass Sie Raspberry Pi-kompatible Software verwenden.

Nachdem Sie das Raspberry Pi-Betriebssystem installiert und konfiguriert haben, öffnen Sie den Webbrowser des Raspberry Pi und navigieren Sie zur AWS IoT Core Konsole, um mit den restlichen Schritten in diesem Tutorial fortzufahren.

Wenn Sie die AWS IoT Core Konsole öffnen können, ist Ihr Raspberry Pi bereit und Sie können fortfahrenthe section called “Bereitstellung Ihres Geräts in AWS IoT ”.

Wenn Sie Probleme haben oder zusätzliche Hilfe benötigen, finden Sie weitere Informationen unter Hilfe für Ihren Raspberry Pi erhalten.

## Tutorial: Bereitstellen Ihres Geräts in AWS IoT

In diesem Abschnitt werden die AWS IoT Core Ressourcen erstellt, die in Ihrem Tutorial verwendet werden.

Schritte zur Bereitstellung Ihres Geräts in AWS IoT

- Schritt 1: Erstellen Sie eine AWS IoT Richtlinie für den Device Shadow
- Schritt 2: Erstellen Sie eine Objekt-Ressource und fügen Sie die Richtlinie dem Objekt hinzu
- Schritt 3: Überprüfen Sie die Ergebnisse und die nächsten Schritte

### Schritt 1: Erstellen Sie eine AWS IoT Richtlinie für den Device Shadow

X.509-Zertifikate authentifizieren Ihr Gerät mit. AWS IoT Core AWS IoT Dem Zertifikat sind Richtlinien beigefügt, die es dem Gerät ermöglichen, AWS IoT Operationen wie das Abonnieren oder Veröffentlichen von reservierten MQTT-Themen auszuführen, die vom Device Shadow-Dienst verwendet werden. Ihr Gerät legt sein Zertifikat vor, wenn es eine Verbindung herstellt und Nachrichten an sendet. AWS IoT Core

In diesem Verfahren erstellen Sie eine Richtlinie, die es Ihrem Gerät ermöglicht, die zur Ausführung des Beispielprogramms erforderlichen AWS IoT -Vorgänge auszuführen. Wir empfehlen, dass Sie eine Richtlinie erstellen, die nur Berechtigungen gewährt, die zum Ausführen einer Aufgabe erforderlich sind. Sie erstellen zuerst die AWS IoT Richtlinie und hängen sie dann an das Gerätezertifikat an, das Sie später erstellen werden.

Um eine AWS IoT Richtlinie zu erstellen

1. Wählen Sie im linken Menü Sicher und dann Richtlinien aus. Wenn in Ihrem Konto bereits Richtlinien vorhanden sind, wählen Sie Erstellen aus. Andernfalls wählen Sie auf der Seite Sie haben noch keine Richtlinie erstellt die Option Richtlinie erstellen aus.
2. Auf der Seite Create a policy (Richtlinie erstellen):

    a. Geben Sie im Feld Name einen Namen für die Richtlinie ein (z. B. **`My_Device_Shadow_policy`**). Verwenden Sie keine personenbezogenen Informationen in Ihren Richtliniennamen.

    b. In dem Richtliniendokument beschreiben Sie die Aktionen „Verbinden“, „Abonnieren“, „Empfangen“ und „Veröffentlichen“, die dem Gerät die Erlaubnis geben, die reservierten MQTT-Themen zu veröffentlichen und zu abonnieren.

Kopieren Sie die folgende Beispielrichtlinie und fügen Sie sie in Ihr Richtliniendokument ein. `thingname`Ersetzen Sie es durch den Namen der Sache, die Sie erstellen werden (z. B.`My_light_bulb`), `region` durch die AWS IoT Region, in der Sie die Dienste nutzen, und `account` durch Ihre AWS-Konto Nummer. Weitere Informationen zu AWS IoT Richtlinien finden Sie unterAWS IoT Core Richtlinien.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingname/shadow/get",
        "arn:aws:iot:region:account:topic/$aws/things/thingname/shadow/update"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingname/shadow/get/
accepted",
        "arn:aws:iot:region:account:topic/$aws/things/thingname/shadow/get/
rejected",
        "arn:aws:iot:region:account:topic/$aws/things/thingname/shadow/update/
accepted",
        "arn:aws:iot:region:account:topic/$aws/things/thingname/shadow/update/
rejected",
        "arn:aws:iot:region:account:topic/$aws/things/thingname/shadow/update/
delta"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
```

```
      "Resource": [
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingname/shadow/
get/accepted",
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingname/shadow/
get/rejected",
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingname/shadow/
update/accepted",
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingname/shadow/
update/rejected",
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingname/shadow/
update/delta"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iot:Connect",
      "Resource": "arn:aws:iot:region:account:client/test-*"
    }
  ]
}
```

Schritt 2: Erstellen Sie eine Objekt-Ressource und fügen Sie die Richtlinie dem Objekt hinzu

Geräte, mit denen eine Verbindung besteht, AWS IoT können durch Ding-Ressourcen in der AWS IoT Registrierung dargestellt werden. Eine Objekt-Ressource steht für ein bestimmtes Gerät oder eine logische Einheit, z. B. die Glühbirne in diesem Tutorial.

Um zu erfahren, wie Sie ein Ding in erstellen AWS IoT, folgen Sie den unter beschriebenen SchrittenDies erstellt ein Objekt. Hier sind einige wichtige Dinge, die Sie beachten sollten, wenn Sie die Schritte in diesem Tutorial befolgen:

1. Wählen Sie Ein einzelnes Objekt erstellen und geben Sie im Feld Name einen Namen für das Objekt ein, der `thingname` entspricht (z. B. `My_light_bulb`), den Sie bei der Erstellung der Richtlinie zuvor angegeben haben.

   Es ist nicht möglich, einen Objektnamen nach dem Erstellen umzubenennen. Wenn Sie dem Objekt einen anderen Namen als `thingname` gegeben haben, erstellen Sie ein neues Objekt mit dem Namen `thingname` und löschen Sie das alte Objekt.

> **Note**
>
> Verwenden Sie keine personenbezogenen Informationen in Ihren Objektnamen. Der Name des Objekts kann in unverschlüsselten Mitteilungen und Berichten vorkommen.

2. Wir empfehlen, dass Sie alle Zertifikatsdateien auf der Seite Zertifikat erstellt! in ein Verzeichnis herunterladen, in dem Sie sie leicht finden können. Sie müssen diese Dateien installieren, um die Beispielanwendung ausführen zu können.

   Wir empfehlen Ihnen, die Dateien in ein `certs` Unterverzeichnis in Ihrem home Verzeichnis auf dem Raspberry Pi herunterzuladen und sie jeweils mit einem einfacheren Namen zu benennen, wie in der folgenden Tabelle vorgeschlagen.

   Namen der Zertifikatsdateien

| Datei | Dateipfad |
|---|---|
| CA-Stammzertifikat | `~/certs/Amazon-root-CA-1.pem` |
| Gerätezertifikat | `~/certs/device.pem.crt` |
| Privater Schlüssel | `~/certs/private.pem.key` |

3. Nachdem Sie das Zertifikat aktiviert haben, mit dem Verbindungen hergestellt werden sollen AWS IoT, wählen Sie Richtlinie anhängen und stellen Sie sicher, dass Sie die Richtlinie, die Sie zuvor erstellt haben (z. B.**`My_Device_Shadow_policy`**), an das Ding anhängen.

   Nachdem Sie ein Ding erstellt haben, können Sie sehen, dass Ihre Dingressource in der Liste der Dinge in der AWS IoT Konsole angezeigt wird.

### Schritt 3: Überprüfen Sie die Ergebnisse und die nächsten Schritte

In diesem Kurs haben Sie Folgendes gelernt:

- Einrichten und Konfigurieren des Raspberry Pi-Geräts.
- Erstellen Sie ein AWS IoT Richtliniendokument, das Ihr Gerät zur Interaktion mit AWS IoT Diensten autorisiert.
- Erstellen einer Objekt-Ressource und des zugehörigen X.509-Gerätezertifikats und Anhängen des Richtliniendokuments.

Nächste Schritte

Sie können jetzt das AWS IoT Geräte-SDK für Python installieren, die `shadow.py` Beispielanwendung ausführen und Device Shadows verwenden, um den Status zu steuern. Weitere Informationen darüber, wie Sie dieses Tutorial ausführen, finden Sie unter Tutorial: Installation des Geräte-SDK und Ausführen der Beispielanwendung für Geräteschatten.

## Tutorial: Installation des Geräte-SDK und Ausführen der Beispielanwendung für Geräteschatten

In diesem Abschnitt wird gezeigt, wie Sie die erforderliche Software und das AWS IoT Device SDK für Python installieren und die `shadow.py` Beispielanwendung ausführen können, um das Shadow-Dokument zu bearbeiten und den Status des Shadows zu kontrollieren.

In diesem Kurs lernen Sie Folgendes:

- Verwenden Sie die installierte Software und AWS IoT das Geräte-SDK für Python, um die Beispiel-App auszuführen.
- Lernen, wie die Eingabe eines Werts mithilfe der Beispiel-App den gewünschten Wert in der AWS IoT Konsole veröffentlicht.
- Prüfen der `shadow.py` Beispiel-App an und wie sie das MQTT-Protokoll verwendet, um den Status des Schattens zu aktualisieren.

Bevor Sie dieses Tutorial ausführen:

Sie müssen Ihr Raspberry Pi-Gerät eingerichtet AWS-Konto, konfiguriert und eine AWS IoT Sache und Richtlinie erstellt haben, die dem Gerät die Erlaubnis geben, die MQTT-reservierten Themen des Device Shadow-Dienstes zu veröffentlichen und zu abonnieren. Weitere Informationen finden Sie unter Tutorial: Ihren Raspberry Pi für die Ausführung der Schattenanwendung vorbereiten.

Sie müssen auch Git, Python und das AWS IoT Device SDK für Python installiert haben. Dieses Tutorial baut auf den im Tutorial Verbinden eines Raspberry Pi oder eines anderes Gerätes vorgestellten Konzepten auf. Wenn Sie dieses Tutorial noch nicht ausprobiert haben, empfehlen wir Ihnen, die in diesem Tutorial beschriebenen Schritte zu befolgen, um die Zertifikatsdateien und das Geräte-SDK zu installieren, und dann zu diesem Tutorial zurückzukehren, um die `shadow.py` Beispiel-App auszuführen.

In diesem Tutorial führen Sie die folgenden Aktivitäten durch:

- Schritt 1: shadow.py-Beispiel-App ausführen
- Schritt 2: Geräte-SDK-Beispiel-App shadow.py prüfen
- Schritt 3: Probleme mit der shadow.py-Beispiel-App beheben
- Schritt 4: Ergebnisse überprüfen und nächste Schritte

Für dieses Tutorial brauchen Sie ungefähr 20 Minuten.

Schritt 1: shadow.py-Beispiel-App ausführen

Bevor Sie die `shadow.py` Beispiel-App ausführen, benötigen Sie zusätzlich zu den Namen und dem Speicherort der installierten Zertifikatsdateien die folgenden Informationen.

Werte für Anwendungsparameter

| Parameter | Wo der Wert gefunden werden kann |
| --- | --- |
| *your-iot-thing-name* | Name der AWS IoT Sache, die Sie zuvor erstellt habenthe section called “Schritt 2: Erstellen Sie eine Objekt-Ressource und fügen Sie die Richtlinie dem Objekt hinzu”.<br><br>Um diesen Wert zu finden, wählen Sie in der AWS IoT Konsole Verwalten und dann Objekte aus. |
| *your-iot-endpoint* | Der *your-iot-endpoint* Wert hat das Format:*endpoint_id* `-ats.iot.` *region*`.amazonaws.com` , zum Beispiel`a3qj468EXAMPLE-ats.iot.us-west-2.amazonaws.com` . So finden Sie diesen Wert:<br><br>1. Wählen Sie in der AWS IoT -Konsole Verwalten und danach Objekte aus.<br>2. Wählen Sie das IoT-Objekt, das Sie für Ihr Gerät erstellt haben, My_Light_Bulb, das Sie zuvor verwendet haben, und wählen Sie dann Interagieren aus. Ihr Endpunkt wird |

| Parameter | Wo der Wert gefunden werden kann |
| --- | --- |
| | im Abschnitt HTTPS auf der Seite mit den Objekt-Details angezeigt. |

Installieren und Ausführen der Beispiel-App

1. Navigieren Sie zum Verzeichnis der Beispiel-App.

```
cd ~/aws-iot-device-sdk-python-v2/samples
```

2. Ersetzen Sie im Befehlszeilenfenster *your-iot-endpoint* und *your-iot-thing-name* wie angegeben und führen Sie diesen Befehl aus.

```
python3 shadow.py --ca_file ~/certs/Amazon-root-CA-1.pem --cert ~/certs/
device.pem.crt --key ~/certs/private.pem.key --endpoint your-iot-endpoint --
thing_name your-iot-thing-name
```

3. Beachten Sie, dass die Beispiel-App:

    1. Stellt eine Verbindung zum AWS IoT-Dienst für Ihr Konto her.
    2. `Delta`-Ereignisse und `Update` und `Get`-Antworten abonniert.
    3. Sie dazu auffordert, einen gewünschten Wert in das Terminal einzugeben.
    4. Die Ausgabe sieht ähnlich aus wie:

```
Connecting to a3qEXAMPLEffp-ats.iot.us-west-2.amazonaws.com with client ID
 'test-0c8ae2ff-cc87-49d2-a82a-ae7ba1d0ca5a'...
Connected!
Subscribing to Delta events...
Subscribing to Update responses...
Subscribing to Get responses...
Requesting current shadow state...
Launching thread to read user input...
Finished getting initial shadow state.
Shadow contains reported value 'off'.
Enter desired value:
```

> **Note**
>
> Wenn Sie Probleme beim Ausführen der `shadow.py`-Beispiel-App haben, überprüfen Sie the section called “Schritt 3: Probleme mit der `shadow.py`-Beispiel-App beheben”. Um zusätzliche Informationen zu erhalten, die Ihnen bei der Behebung des Problems helfen könnten, fügen Sie den `--verbosity debug` Parameter zur Befehlszeile hinzu, sodass die Beispiel-App detaillierte Meldungen darüber anzeigt, was sie tut.

Geben Sie Werte ein und beobachten Sie die Aktualisierungen im Schattendokument

Sie können Werte in das Terminal eingeben, um den `desired`-Wert anzugeben, wodurch auch der `reported`-Wert aktualisiert wird. Angenommen, Sie geben die Farbe `yellow` im Terminal ein. Der `reported`-Wert wird ebenfalls auf die Farbe `yellow` aktualisiert. Im Folgenden werden die im Terminal angezeigten Meldungen angezeigt:

```
Enter desired value:
yellow
Changed local shadow value to 'yellow'.
Updating reported shadow value to 'yellow'...
Update request published.
Finished updating reported shadow value to 'yellow'.
```

Wenn Sie diese Aktualisierungsanforderung veröffentlichen, AWS IoT wird ein klassischer Standard-Shadow für die Ding-Ressource erstellt. Sie können die Aktualisierungsanforderung beobachten, die Sie für die `desired` Werte `reported` und in der AWS IoT Konsole veröffentlicht haben, indem Sie sich das Shadow-Dokument für die von Ihnen erstellte Ding-Ressource ansehen (z. B.`My_light_bulb`). Um das Update im Schattendokument zu sehen:

1. Wählen Sie in der AWS IoT Konsole Manage und anschließend Things aus.
2. Wählen Sie in der angezeigten Liste das Objekt aus, das Sie erstellt haben, wählen Sie Schatten und anschließend Klassischer Schatten.

Das Schattendokument sollte wie folgt aussehen und für die `reported`- und `desired`-Werte die Farbe `yellow` anzeigen. Sie sehen diese Werte im Abschnitt Schattenstatus des Dokuments.

```
{
"desired": {
```

```
  "welcome": "aws-iot",
  "color": "yellow"
},
"reported": {
  "welcome": "aws-iot",
  "color": "yellow"
}
}
```

Sie sehen auch einen Abschnitt mit den Metadaten, der die Zeitstempelinformationen und die Versionsnummer der Anfrage enthält.

Sie können die Version des Statusdokuments verwenden, um sicherzustellen, dass Sie die neueste Version eines Geräteschattendokuments aktualisieren. Wenn Sie eine weitere Aktualisierungsanfrage senden, wird die Versionsnummer um 1 erhöht. Geben Sie bei einer Aktualisierungsanfrage eine Version an, lehnt der Service die Anfrage mit einem Konflikt-Antwortcode HTTP 409 ab, wenn die aktuelle Version des Statusdokuments nicht der angegebenen Version entspricht.

```
{
"metadata": {
  "desired": {
    "welcome": {
      "timestamp": 1620156892
    },
    "color": {
      "timestamp": 1620156893
    }
  },
  "reported": {
    "welcome": {
      "timestamp": 1620156892
    },
    "color": {
      "timestamp": 1620156893
    }
  }
},
"version": 10
}
```

Um mehr über das Schattendokument zu erfahren und Änderungen an den Statusinformationen einzusehen, fahren Sie mit dem nächsten Tutorial Tutorial: Interaktion mit Geräteschatten mithilfe der

Beispiel-App und des MQTT-Testclients fort, wie im Schritt 4: Ergebnisse überprüfen und nächste Schritte Abschnitt dieses Tutorials beschrieben. Optional können Sie im folgenden Abschnitt auch mehr über den `shadow.py`-Beispielcode und dessen Verwendung des MQTT-Protokolls erfahren.

Schritt 2: Geräte-SDK-Beispiel-App shadow.py prüfen

In diesem Abschnitt wird die `shadow.py`-Beispiel-App aus dem AWS IoT -Geräte-SDK v2 für Python beschrieben, die in diesem Tutorial verwendet wird. Hier werden wir uns ansehen, wie es AWS IoT Core mithilfe des MQTT- und MQTT-über-WSS-Protokolls eine Verbindung herstellt. Die AWS Common Runtime (AWS-CRT) -Bibliothek bietet Unterstützung für Low-Level-Kommunikationsprotokolle und ist im AWS IoT Device SDK v2 für Python enthalten.

Dieses Tutorial verwendet zwar MQTT und MQTT über WSS, AWS IoT unterstützt aber Geräte, die HTTPS-Anfragen veröffentlichen. Ein Beispiel für ein Python-Programm, das eine HTTP-Nachricht von einem Gerät sendet, finden Sie im HTTPS-Codebeispiel unter Verwendung der Python `requests`-Bibliothek.

Informationen darüber, wie Sie eine fundierte Entscheidung darüber treffen können, welches Protokoll Sie für die Kommunikation mit Ihrem Gerät verwenden möchten, finden Sie unter Wählen Sie ein Anwendungsprotokoll für die Kommunikation mit Ihrem Gerät.

MQTT

Das `shadow.py` Beispiel ruft `mtls_from_path` (hier gezeigt) in `mqtt_connection_builder`, um AWS IoT Core mithilfe des MQTT-Protokolls eine Verbindung herzustellen. `mtls_from_path`verwendet X.509-Zertifikate und TLS v1.2 zur Authentifizierung des Geräts. Die AWS-CRT-Bibliothek verarbeitet die untergeordneten Details dieser Verbindung.

```
mqtt_connection = mqtt_connection_builder.mtls_from_path(
  endpoint=args.endpoint,
  cert_filepath=args.cert,
  pri_key_filepath=args.key,
  ca_filepath=args.ca_file,
  client_bootstrap=client_bootstrap,
  on_connection_interrupted=on_connection_interrupted,
  on_connection_resumed=on_connection_resumed,
  client_id=args.client_id,
  clean_session=False,
  keep_alive_secs=6
)
```

- `endpoint`ist Ihr AWS IoT Endpunkt, den Sie über die Befehlszeile eingegeben haben, und `client_id` ist die ID, die dieses Gerät in der eindeutig identifiziert. AWS-Region
- `cert_filepath`, `pri_key_filepath` und `ca_filepath` sind die Pfade zu den Zertifikats- und privaten Schlüsseldateien des Geräts sowie zur Root-CA-Datei.
- `client_bootstrap` ist das allgemeine Runtime-Objekt, das Socket-Kommunikationsaktivitäten verarbeitet und vor dem Aufruf von `mqtt_connection_builder.mtls_from_path` instanziiert wird.
- `on_connection_interrupted` und `on_connection_resumed` sind Callback-Funktionen, die aufgerufen werden, wenn die Verbindung des Geräts unterbrochen und wieder aufgenommen wird.
- `clean_session` gibt an, ob eine neue, persistente Sitzung gestartet werden soll oder ob, falls eine vorhanden ist, die Verbindung zu einer bestehenden wiederhergestellt werden soll. `keep_alive_secs` ist der Keep-Alive-Wert in Sekunden, der in der `CONNECT`-Anfrage gesendet werden soll. In diesem Intervall wird automatisch ein Ping gesendet. Der Server geht davon aus, dass die Verbindung unterbrochen ist, wenn er nach dem 1,5-fachen dieses Werts keinen Ping erhält.

Das `shadow.py` Beispiel ruft auch `websockets_with_default_aws_signing` in `mqtt_connection_builder` auf, um mithilfe des MQTT-Protokolls über WSS eine Verbindung zu AWS IoT Core herzustellen. MQTT über WSS verwendet ebenfalls dieselben Parameter wie MQTT und verwendet diese zusätzlichen Parameter:

- `region`ist die AWS Signaturregion, die von der Signature V4-Authentifizierung verwendet `credentials_provider` wird, und sind die AWS Anmeldeinformationen, die für die Authentifizierung bereitgestellt werden. Die Region wird von der Befehlszeile aus übergeben, und das `credentials_provider`-Objekt wird unmittelbar vor dem Aufruf von `mqtt_connection_builder.websockets_with_default_aws_signing` instanziiert.
- `websocket_proxy_options` sind die HTTP-Proxyoptionen, wenn ein Proxyhost verwendet wird. In der `shadow.py` Beispiel-App wird dieser Wert unmittelbar vor dem Aufruf von `mqtt_connection_builder.websockets_with_default_aws_signing` instanziiert.

Abonnieren von Shadow-Themen und -Ereignissen

Das `shadow.py`-Beispiel versucht, eine Verbindung herzustellen, und wartet, bis die Verbindung vollständig hergestellt ist. Wenn es nicht verbunden ist, werden Befehle in die Warteschlange gestellt. Sobald die Verbindung hergestellt ist, abonniert das Beispiel Delta-Ereignisse und Aktualisierungs-

und Abrufnachrichten und veröffentlicht Nachrichten mit einer QoS-Stufe (Quality of Service) von 1 (`mqtt.QoS.AT_LEAST_ONCE`).

Wenn ein Gerät eine Nachricht mit QoS Level 1 abonniert, speichert der Message Broker die Nachrichten, die das Gerät abonniert hat, bis sie an das Gerät gesendet werden können. Der Message Broker sendet die Nachrichten erneut, bis er eine PUBACK-Antwort vom Gerät erhält.

Weitere Informationen zum MQTT-Protokoll finden Sie unter Überprüfen Sie das MQTT Protokoll und MQTT.

Weitere Informationen zur Verwendung von MQTT, MQTT über WSS, persistente Sitzungen und QoS-Stufen, die in diesem Tutorial verwendet werden, finden Sie unter Sehen Sie sich die SDK Gerätebeispiel-App pubsub.py an.

Schritt 3: Probleme mit der **`shadow.py`**-Beispiel-App beheben

Wenn Sie die `shadow.py`-Beispiel-App ausführen, sollten im Terminal einige Meldungen und eine Aufforderung zur Eingabe eines `desired`-Werts angezeigt werden. Wenn das Programm einen Fehler ausgibt, können Sie zum Debuggen des Fehlers zunächst überprüfen, ob Sie den richtigen Befehl für Ihr System ausgeführt haben.

In einigen Fällen weist die Fehlermeldung möglicherweise auf Verbindungsprobleme hin und sieht ähnlich aus wie: `Host name was invalid for dns resolution` oder `Connection was closed unexpectedly`. In solchen Fällen können Sie Folgendes überprüfen:

- Die Endpunktadresse im Befehl

  Das `endpoint`-Argument in dem Befehl, den Sie zum Ausführen der Beispiel-App eingegeben haben (z. B. `a3qEXAMPLEffp-ats.iot.us-west-2.amazonaws.com`). Diesen Wert können Sie auch in der AWS IoT Konsole prüfen.

  Um zu überprüfen, ob Sie den richtigen Wert verwendet haben:

  1. Wählen Sie in der AWS IoT -Konsole Verwalten und danach Objekte.
  2. Wählen Sie das Objekt aus, das Sie für Ihre Beispiel-App erstellt haben (z. B. My_Light_Bulb), und wählen Sie dann Interagieren.

  Ihr Endpunkt wird im Abschnitt HTTPS auf der Seite mit den Objekt-Details angezeigt. Sie sollten auch eine Meldung sehen, die besagt: `This thing already appears to be connected.`
- Aktivierung des Zertifikats überprüfen

Zertifikate authentifizieren Ihr Gerät mit AWS IoT Core.

Um zu überprüfen, ob Ihr Zertifikat aktiv ist:

1. Wählen Sie in der AWS IoT -Konsole Verwalten und danach Objekte.
2. Wählen Sie das Objekt aus, das Sie für Ihre Beispiel-App erstellt haben (z. B. My_Light_Bulb), und wählen Sie dann Sicherheit.
3. Wählen Sie das Zertifikat aus und wählen Sie dann auf der Detailseite des Zertifikats die Option „Zertifikat auswählen“ und dann auf der Detailseite des Zertifikats die Option Aktionen aus.

Wenn in der Dropdownliste Aktivieren nicht verfügbar ist und Sie nur Deaktivieren auswählen können, ist Ihr Zertifikat aktiv. Wenn nicht, wählen Sie Aktivieren und führen Sie das Beispielprogramm erneut aus.

Wenn das Programm immer noch nicht ausgeführt wird, überprüfen Sie die Namen der Zertifikatsdateien im `certs`-Ordner.

- Überprüfen der mit der Objekt-Ressource verknüpften Richtlinie

  Zertifikate authentifizieren zwar Ihr Gerät, aber AWS IoT Richtlinien gestatten es dem Gerät, bestimmte AWS IoT Vorgänge auszuführen, wie z. B. das Abonnieren oder Veröffentlichen von MQTT-Themen, die für MQTT reserviert sind.

  Um zu überprüfen, ob die richtige Richtlinie angehängt ist:

  1. Suchen Sie das Zertifikat wie zuvor beschrieben und wählen Sie dann Richtlinien aus.
  2. Wählen Sie die angezeigte Richtlinie aus und überprüfen Sie, ob sie die Aktionen `connect`, `subscribe`, `receive` und `publish` beschreibt, die dem Gerät die Erlaubnis geben, die reservierten MQTT-Themen zu veröffentlichen und zu abonnieren.

     Eine Beispielrichtlinie finden Sie unter Schritt 1: Erstellen Sie eine AWS IoT Richtlinie für den Device Shadow.

Wenn Ihnen Fehlermeldungen angezeigt werden, die auf Probleme beim Herstellen einer Verbindung hinweisen AWS IoT, kann dies an den Berechtigungen liegen, die Sie für die Richtlinie verwenden. In diesem Fall empfehlen wir, mit einer Richtlinie zu beginnen, die vollen Zugriff auf AWS IoT Ressourcen gewährt, und dann das Beispielprogramm erneut auszuführen. Sie können entweder die aktuelle Richtlinie bearbeiten oder die aktuelle Richtlinie auswählen, Trennen auswählen und dann eine weitere Richtlinie erstellen, die vollen Zugriff gewährt, und diese an Ihre

Objekt-Ressource anhängen. Sie können die Richtlinie später nur auf die Aktionen und Richtlinien beschränken, die Sie zur Ausführung des Programms benötigen.

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

- Überprüfen der Installation Ihres Geräte-SDKs

  Wenn das Programm immer noch nicht ausgeführt wird, können Sie das Geräte-SDK erneut installieren, um sicherzustellen, dass Ihre SDK-Installation vollständig und korrekt ist.

Schritt 4: Ergebnisse überprüfen und nächste Schritte

In diesem Kurs haben Sie gelernt, wie Sie:

- Installieren Sie die erforderliche Software, Tools und das AWS IoT Geräte-SDK für Python.
- Die Beispiel-App `shadow.py` das MQTT-Protokoll zum Abrufen und Aktualisieren des aktuellen Status des Schattens verwendet.
- Führen Sie die Beispiel-App für Device Shadows aus und beobachten Sie die Aktualisierung des Shadow-Dokuments in der AWS IoT Konsole. Sie haben darüber hinaus gelernt, Probleme und Fehler bei der Ausführung des Programms zu beheben.

Nächste Schritte

Sie können jetzt die `shadow.py`-Beispielanwendung ausführen und Geräteschatten verwenden, um den Status zu kontrollieren. Sie können die Aktualisierungen des Schattendokuments in der AWS IoT -Konsole verfolgen und Delta-Ereignisse beobachten, auf die die Beispiel-App reagiert. Mit dem MQTT-Testclient können Sie die reservierten Schattenthemen abonnieren und die Nachrichten beobachten, die die Themen bei der Ausführung des Beispielprogramms erhalten. Weitere

Informationen darüber, wie Sie dieses Tutorial ausführen, finden Sie unter Tutorial: Interaktion mit Geräteschatten mithilfe der Beispiel-App und des MQTT-Testclients.

## Tutorial: Interaktion mit Geräteschatten mithilfe der Beispiel-App und des MQTT-Testclients

Um mit der `shadow.py`-Beispiel-App zu interagieren, geben Sie im Terminal einen Wert für den `desired`-Wert ein. Sie können beispielsweise Farben angeben, die den Ampeln ähneln und AWS IoT auf die Anfrage reagieren und die gemeldeten Werte aktualisieren.

In diesem Kurs lernen Sie Folgendes:

- Verwenden der `shadow.py`-Beispiel-App, um die gewünschten Status anzugeben und den aktuellen Status des Schattens zu aktualisieren.
- Bearbeiten Sie das Schattendokument, um Delta-Ereignisse und die Reaktion der `shadow.py`-Beispiel-App auf diese Ereignisse zu beobachten.
- Verwenden Sie den MQTT-Testclient, um Schattenthemen zu abonnieren und Updates zu beobachten, wenn Sie das Beispielprogramm ausführen.

Für dieses Tutorial benötigen Sie Folgendes:

Richten Sie Ihr Raspberry Pi-Gerät ein AWS-Konto, konfigurieren Sie es und erstellen Sie eine AWS IoT Sache und Richtlinie. Sie müssen auch die erforderliche Software, das Geräte-SDK und die Zertifikatsdateien installiert haben und das Beispielprogramm im Terminal ausführen. Weitere Informationen finden Sie in den vorherigen Tutorials Tutorial: Ihren Raspberry Pi für die Ausführung der Schattenanwendung vorbereiten und Schritt 1: shadow.py-Beispiel-App ausführen. Sie müssen diese Tutorials abschließen, wenn das noch nicht geschehen ist.

In diesem Tutorial führen Sie die folgenden Aktivitäten durch:

- Schritt 1: Die gewünschten und gemeldeten Werte mithilfe der shadow.py-Beispiel-App aktualisieren
- Schritt 2: Nachrichten aus der shadow.py-Beispiel-App im MQTT-Testclient anzeigen
- Schritt 3: Fehlerbehebung bei Interaktionen mit Geräteschatten
- Schritt 4: Überprüfen der Ergebnisse und nächste Schritte

Für dieses Tutorial brauchen Sie ungefähr 45 Minuten.

Schritt 1: Die gewünschten und gemeldeten Werte mithilfe der **`shadow.py`**-Beispiel-App aktualisieren

Im vorherigen Tutorial haben Sie gelerntSchritt 1: shadow.py-Beispiel-App ausführen, wie Sie eine Nachricht beobachten können, die im Shadow-Dokument in der AWS IoT Konsole veröffentlicht wurde, wenn Sie einen gewünschten Wert eingeben, wie im Abschnitt beschriebenTutorial: Installation des Geräte-SDK und Ausführen der Beispielanwendung für Geräteschatten.

Im vorherigen Beispiel haben wir die gewünschte Farbe auf `yellow` eingestellt. Nachdem Sie jeden Wert eingegeben haben, fordert Sie das Terminal auf, einen anderen `desired`-Wert einzugeben. Wenn Sie erneut denselben Wert eingeben (`yellow`), erkennt die App dies und fordert Sie auf, einen neuen `desired`-Wert einzugeben.

```
Enter desired value:
yellow
Local value is already 'yellow'.
Enter desired value:
```

Nehmen wir nun an, dass Sie die Farbe eingeben`green`. AWS IoT beantwortet die Anfrage und aktualisiert den `reported` Wert auf`green`. Auf diese Weise erfolgt die Aktualisierung, wenn sich der `desired`-Status vom `reported`-Status unterscheidet, was zu einem Delta führt.

So simuliert die **`shadow.py`**-Beispiel-App Geräteschatten-Interaktionen:

1. Geben Sie einen `desired`-Wert (sagen wir `yellow`) in das Terminal ein, um den gewünschten Status zu veröffentlichen.
2. Da sich der `desired`-Status vom `reported`-Status unterscheidet (sagen wir die Farbe `green`), tritt ein Delta auf, und die App, die das Delta abonniert hat, empfängt diese Nachricht.
3. Die App reagiert auf die Nachricht und aktualisiert ihren Status auf den `desired`-Wert `yellow`.
4. Die App veröffentlicht dann eine Aktualisierungsnachricht mit dem neuen gemeldeten Wert des Gerätestatus, `yellow`.

Im Folgenden werden die im Terminal angezeigten Meldungen angezeigt, aus denen hervorgeht, wie die Aktualisierungsanforderung veröffentlicht wird.

```
Enter desired value:
green
Changed local shadow value to 'green'.
Updating reported shadow value to 'green'...
Update request published.
```

```
Finished updating reported shadow value to 'green'.
```

In der AWS IoT Konsole spiegelt das Shadow-Dokument den aktualisierten Wert von sowohl `green` für die `reported` `desired` Felder als auch wider, und die Versionsnummer wird um 1 erhöht. Wenn die vorherige Versionsnummer beispielsweise als 10 angezeigt wurde, wird die aktuelle Versionsnummer als 11 angezeigt.

> **Note**
>
> Durch das Löschen eines Schattens wird seine Versionsnummer nicht sofort auf null zurückgesetzt. Sie werden feststellen, dass die Schattenversion um 1 erhöht wird, wenn Sie eine Aktualisierungsanforderung veröffentlichen oder einen anderen Schatten mit demselben Namen erstellen.

Das Schattendokument berbeiten, um Delta-Ereignisse zu beobachten

Die `shadow.py`-Beispiel-App hat auch `delta`-Ereignisse abonniert und reagiert, wenn sich der `desired`-Wert ändert. Sie können den `desired`-Wert beispielsweise in die Farbe `red` ändern. Bearbeiten Sie dazu in der AWS IoT Konsole das Shadow-Dokument, indem Sie auf Bearbeiten klicken und dann den `desired` Wert `red` in der JSON-Datei auf festlegen, während Sie den `reported` Wert auf `green` beibehalten. Bevor Sie die Änderungen speichern, lassen Sie das Terminal auf dem Raspberry Pi geöffnet, da im Terminal Meldungen angezeigt werden, wenn die Änderung erfolgt.

```
{
"desired": {
  "welcome": "aws-iot",
  "color": "red"
},
"reported": {
  "welcome": "aws-iot",
  "color": "green"
}
}
```

Nachdem Sie den neuen Wert gespeichert haben, reagiert die `shadow.py`-Beispiel-App auf diese Änderung und zeigt im Terminal Meldungen an, die auf das Delta hinweisen. Sie sollten dann die folgenden Meldungen unter der Aufforderung zur Eingabe des `desired`-Werts sehen.

```
Enter desired value:
Received shadow delta event.
Delta reports that desired value is 'red'. Changing local value...
Changed local shadow value to 'red'.
Updating reported shadow value to 'red'...
Finished updating reported shadow value to 'red'.
Enter desired value:
Update request published.
Finished updating reported shadow value to 'red'.
```

Schritt 2: Nachrichten aus der **`shadow.py`**-Beispiel-App im MQTT-Testclient anzeigen

Sie können den MQTT-Testclient in der AWS IoT Konsole verwenden, um MQTT-Nachrichten zu überwachen, die zu Ihrem AWS-Kontoübermittelt werden. Wenn Sie reservierte MQTT-Themen abonnieren, die vom Geräteschattendienst verwendet werden, können Sie die Nachrichten beobachten, die von den Themen beim Ausführen der Beispiel-App empfangen wurden.

Wenn Sie den MQTT-Testclient noch nicht verwendet haben, können Sie sich MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen ansehen. Auf diese Weise lernen Sie, wie Sie den MQTT-Testclient in der AWS IoT Konsole verwenden, um MQTT-Nachrichten anzuzeigen, während sie durch den Message Broker laufen.

1. Öffnen des MQTT-Testclients

   Öffnen Sie den MQTT-Testclient in der AWS IoT -Konsole in einem neuen Fenster, damit Sie die von den MQTT-Themen empfangenen Nachrichten beobachten können, ohne die Konfiguration Ihres MQTT-Testclients zu verlieren. Der MQTT-Testclient speichert keine Abonnements oder Nachrichtenprotokolle, wenn Sie ihn verlassen, um zu einer anderen Seite in der Konsole zu wechseln. In diesem Abschnitt des Tutorials können Sie das Shadow-Dokument Ihres Dings und AWS IoT den MQTT-Testclient in separaten Fenstern öffnen, um die Interaktion mit Device Shadows einfacher beobachten zu können.

2. Abonnieren der reservierten MQTT-Schatten-Themen

   Sie können den MQTT-Testclient verwenden, um die Namen der reservierten MQTT-Themen von Geräteschatten einzugeben und sie zu abonnieren, um Updates zu erhalten, wenn Sie die `shadow.py`-Beispiel-App ausführen. So abonnieren Sie MQTT-Themen:

   a. Wählen Sie im MQTT-Testclient in der AWS IoT Konsole die Option Thema abonnieren aus.

b. Geben Sie im Abschnitt Themenfilter Folgendes ein: $aws/things/ ***thingname*** /shadow/update/ #. Hier ist `thingname` der Name der Objekt-Ressource, die Sie zuvor erstellt haben (z. B. `My_light_bulb`).

c. Behalten Sie die Standardwerte für die zusätzlichen Konfigurationseinstellungen bei und wählen Sie dann Abonnieren.

Durch die Verwendung des Platzhalters # im Themenabonnement können Sie mehrere MQTT-Themen gleichzeitig abonnieren und alle Nachrichten, die zwischen dem Gerät und seinem Schatten ausgetauscht werden, in einem einzigen Fenster beobachten. Weitere Informationen über Platzhalterzeichen und ihre Verwendung finden Sie unter MQTT-Themen.

3. Ausführen des **`shadow.py`**-Beispielprogramms und Beobachten der Meldungen

Wenn Sie in Ihrem Befehlszeilenfenster des Raspberry Pi das Programm getrennt haben, führen Sie die Beispiel-App erneut aus und sehen Sie sich die Meldungen im MQTT-Testclient in der AWS IoT Konsole an.

a. Geben Sie den folgenden Befehl ein, um das Beispielprogramm neu zu starten. Ersetzen Sie *`your-iot-thing-name`* und durch die Namen des Objekts, das Sie zuvor erstellt haben (z. B.), und durch den AWS IoT Endpunkt, `My_light_bulb` der *`your-iot-endpoint`* mit dem Gerät interagieren soll.

```
cd ~/aws-iot-device-sdk-python-v2/samples
python3 shadow.py --ca_file ~/certs/Amazon-root-CA-1.pem --cert ~/certs/
device.pem.crt --key ~/certs/private.pem.key --endpoint your-iot-endpoint --
thing_name your-iot-thing-name
```

Die `shadow.py`-Beispiel-App wird dann ausgeführt und ruft den aktuellen Schattenstatus ab. Wenn Sie den Schatten oder den aktuellen Status gelöscht haben, setzt das Programm den aktuellen Wert auf `off` und fordert Sie dann auf, einen `desired`-Wert einzugeben.

```
Connecting to a3qEXAMPLEffp-ats.iot.us-west-2.amazonaws.com with client ID
 'test-0c8ae2ff-cc87-49d2-a82a-ae7ba1d0ca5a'...
Connected!
Subscribing to Delta events...
Subscribing to Update responses...
Subscribing to Get responses...
Requesting current shadow state...
Launching thread to read user input...
```

```
Finished getting initial shadow state.
Shadow document lacks 'color' property. Setting defaults...
Changed local shadow value to 'off'.
Updating reported shadow value to 'off'...
Update request published.
Finished updating reported shadow value to 'off'...
Enter desired value:
```

Wenn das Programm jedoch ausgeführt wurde und Sie es neu gestartet haben, wird der letzte Farbwert im Terminal gemeldet. Im MQTT-Testclient werden Sie ein Update zu den Themen $aws/things/ /shadow/get und ***thingname*** $aws/things//sehen. ***thingname*** shadow/get/accepted

Nehmen wir an, die zuletzt gemeldete Farbe war `green`. Im Folgenden ***thingname*** wird shadow/get/accepted der Inhalt der JSON-Datei $aws/things//gezeigt.

```
{
"state": {
  "desired": {
    "welcome": "aws-iot",
    "color": "green"
  },
  "reported": {
    "welcome": "aws-iot",
    "color": "green"
  }
},
"metadata": {
  "desired": {
    "welcome": {
      "timestamp": 1620156892
    },
    "color": {
      "timestamp": 1620161643
    }
  },
  "reported": {
    "welcome": {
      "timestamp": 1620156892
    },
    "color": {
      "timestamp": 1620161643
```

```
    }
  }
},
"version": 10,
"timestamp": 1620173908
}
```

b. Geben Sie einen `desired`-Wert in das Terminal ein, z. B. `yellow`. Die `shadow.py`-Beispiel-App reagiert und zeigt im Terminal die folgenden Meldungen an, die die Änderung des `reported`-Werts auf `yellow` zeigen.

```
Enter desired value:
yellow
Changed local shadow value to 'yellow'.
Updating reported shadow value to 'yellow'...
Update request published.
Finished updating reported shadow value to 'yellow'.
```

Im MQTT-Testclient in der AWS IoT Konsole sehen Sie unter Abonnements, dass die folgenden Themen eine Nachricht erhalten haben:

- $aws/things/ ***thingname*** /shadow/update: zeigt, dass sich beide Werte in der Farbe ändern. `desired` `updated` `yellow`
- $aws/things/***thingname***/shadow/update/accepted: zeigt die aktuellen Werte der Zustände und deren Metadaten und Versionsinformationen an. `desired` `reported`
- $aws/things/***thingname***/shadow/update/documents: zeigt die vorherigen und aktuellen Werte der Zustände und deren Metadaten und Versionsinformationen an. `desired` `reported`

Da das Dokument $aws/things/***thingname***/shadow/update/documentsauch Informationen enthält, die in den anderen beiden Themen enthalten sind, können wir es überprüfen, um die Statusinformationen einzusehen. Der vorherige Status zeigt den auf `green` festgelegten Wert, seine Metadaten und Versionsinformationen sowie den aktuellen Status `yellow`, auf den der gemeldete Wert aktualisiert wurde.

```
{
"previous": {
  "state": {
```

```
    "desired": {
      "welcome": "aws-iot",
      "color": "green"
    },
    "reported": {
      "welcome": "aws-iot",
      "color": "green"
    }
  },
  "metadata": {
    "desired": {
      "welcome": {
        "timestamp": 1617297888
      },
      "color": {
        "timestamp": 1617297898
      }
    },
    "reported": {
      "welcome": {
        "timestamp": 1617297888
      },
      "color": {
        "timestamp": 1617297898
      }
    }
  },
  "version": 10
},
"current": {
  "state": {
    "desired": {
      "welcome": "aws-iot",
      "color": "yellow"
    },
    "reported": {
      "welcome": "aws-iot",
      "color": "yellow"
    }
  },
  "metadata": {
    "desired": {
      "welcome": {
        "timestamp": 1617297888
```

```
      },
      "color": {
        "timestamp": 1617297904
      }
    },
    "reported": {
      "welcome": {
        "timestamp": 1617297888
      },
      "color": {
        "timestamp": 1617297904
      }
    }
  },
  "version": 11
},
"timestamp": 1617297904
}
```

c. Wenn Sie nun einen anderen `desired`-Wert eingeben, sehen Sie weitere Änderungen an den `reported`-Werten und Nachrichtenaktualisierungen, die in diesen Themen eingegangen sind. Die Versionsnummer wird ebenfalls um 1 erhöht. Wenn Sie beispielsweise den Wert `green` eingeben, meldet der vorherige Status den Wert `yellow` und der aktuelle Status meldet den Wert `green`.

4. Bearbeiten des Schattendokuments, um Delta-Ereignisse zu beobachten

   Um Änderungen am Delta-Thema zu beobachten, bearbeiten Sie das Schattendokument in der AWS IoT -Konsole. Sie können den `desired`-Wert beispielsweise in die Farbe `red` ändern. Wählen Sie dazu in der AWS IoT Konsole Bearbeiten und setzen Sie dann den `desired` Wert im JSON-Format auf Rot, während Sie den Wert auf beibehalten. `reported` `green` Lassen Sie das Terminal geöffnet, bevor Sie die Änderung speichern, da die Deltameldung im Terminal angezeigt wird.

   ```
   {
   "desired": {
     "welcome": "aws-iot",
     "color": "red"
   },
   "reported": {
     "welcome": "aws-iot",
     "color": "green"
   ```

```
}
}
```

Die `shadow.py`-Beispiel-App reagiert auf diese Änderung und zeigt im Terminal Meldungen an, die auf das Delta hinweisen. Im MQTT-Testclient haben die `update`-Themen eine Nachricht erhalten, die Änderungen an den `desired`- und `reported`-Werten anzeigt.

Sie sehen auch, dass das Thema $aws/things//***thingname***eine Nachricht erhalten hat. shadow/update/delta Um die Nachricht zu sehen, wählen Sie dieses Thema aus, das unter Abonnements aufgeführt ist.

```
{
"version": 13,
"timestamp": 1617318480,
"state": {
  "color": "red"
},
"metadata": {
  "color": {
    "timestamp": 1617318480
  }
}
}
```

Schritt 3: Fehlerbehebung bei Interaktionen mit Geräteschatten

Wenn Sie die Schatten-Beispiel-App ausführen, können Probleme bei der Beobachtung von Interaktionen mit dem Geräteschattendienst auftreten.

Wenn das Programm erfolgreich ausgeführt wird und Sie zur Eingabe eines `desired`-Werts auffordert werden, sollten Sie in der Lage sein, die Geräteschatten-Interaktionen mithilfe des Schattendokuments und des MQTT-Testclients wie zuvor beschrieben zu beobachten. Wenn Sie die Interaktionen jedoch nicht sehen können, können Sie Folgendes überprüfen:

- Überprüfe den Namen des Dings und seinen Schatten in der Konsole AWS IoT

  Wenn Sie die Meldungen im Schattendokument nicht sehen, überprüfen Sie den Befehl und stellen Sie sicher, dass er mit dem Namen des Objekts in der AWS IoT Konsole übereinstimmt. Sie können auch überprüfen, ob Sie einen klassischen Schatten haben, indem Sie Ihre Objekt-

Ressource und dann Schatten auswählen. Dieses Tutorial konzentriert sich hauptsächlich auf Interaktionen mit dem klassischen Schatten.

Sie können auch überprüfen, ob das von Ihnen verwendete Gerät mit dem Internet verbunden ist. Wählen Sie in der AWS IoT Konsole das Objekt aus, das Sie zuvor erstellt haben, und wählen Sie dann Interagieren aus. Auf der Seite mit den Objekt-Details solltest Sie hier eine Meldung sehen, die besagt: `This thing already appears to be connected.`

- Überprüfen der reservierten abonnierten MQTT-Themen

  Wenn Sie die Nachrichten nicht im MQTT-Testclient sehen, überprüfen Sie, ob die Themen, die Sie abonniert haben, richtig formatiert sind. MQTT Device Shadow-Themen haben das Format $aws/things/ ***thingname*** /shadow/ und können diesem Format `delete` folgen, je nachdem `updateget`, welche Aktionen Sie mit dem Shadow ausführen möchten. Dieses Tutorial verwendet das Thema $aws/things/ ***thingname*** /shadow/ #. Stellen Sie also sicher, dass Sie es richtig eingegeben haben, wenn Sie das Thema im Themenfilterbereich des Testclients abonniert haben.

  Achten Sie bei der Eingabe des Themennamens darauf, dass der mit dem Namen der Sache *`thingname`* übereinstimmt, die Sie zuvor erstellt haben. AWS IoT Sie können auch zusätzliche MQTT-Themen abonnieren, um zu sehen, ob ein Update erfolgreich durchgeführt wurde. Sie können beispielsweise das Thema $aws/things/***thingname***/abonnieren, um eine Nachricht shadow/update/rejected zu erhalten, wenn eine Aktualisierungsanforderung fehlschlägt, sodass Sie Verbindungsprobleme debuggen können. Weitere Informationen zu den reservierten Themen finden Sie unter the section called “Schatten-Themen” und MQTT-Themen für Geräteschatten.

Schritt 4: Überprüfen der Ergebnisse und nächste Schritte

In diesem Kurs haben Sie gelernt, wie Sie:

- Die `shadow.py`-Beispiel-App verwenden, um die gewünschten Status anzugeben und den aktuellen Status des Schattens zu aktualisieren.
- Bearbeiten Sie das Schattendokument, um Delta-Ereignisse und die Reaktion der `shadow.py`-Beispiel-App auf diese Ereignisse zu beobachten.
- Verwenden Sie den MQTT-Testclient, um Schattenthemen zu abonnieren und Updates zu beobachten, wenn Sie das Beispielprogramm ausführen.

Nächste Schritte

Sie können zusätzliche reservierte MQTT-Themen abonnieren, um Aktualisierungen der Schattenanwendung zu beobachten. Wenn Sie beispielsweise nur das Thema $aws/things/***thingname***/abonnieren, werden Ihnen nur die aktuellen Statusinformationen angezeigtshadow/update/accepted, wenn ein Update erfolgreich durchgeführt wurde.

Sie können auch zusätzliche Schattenthemen abonnieren, um Probleme zu beheben oder mehr über die Geräteschatten-Interaktionen zu erfahren sowie mögliche Probleme mit den Geräteschatten-Interaktionen zu debuggen. Weitere Informationen erhalten Sie unter the section called “Schatten-Themen” und MQTT-Themen für Geräteschatten.

Sie können Ihre Anwendung auch erweitern, indem Sie Named Shadows verwenden oder zusätzliche Hardware verwenden, die mit dem Raspberry Pi verbunden ist, LEDs und Zustandsänderungen anhand von Nachrichten beobachten, die vom Terminal gesendet werden.

Weitere Informationen zum Geräteschattendienst und zur Verwendung des Dienstes in Geräten, Apps und Diensten finden Sie unter AWS IoT Device Shadow-Dienst, Verwenden von Schatten in Geräten und Verwenden von Schatten in Apps und Services.

## Tutorial: Erstellen eines benutzerdefinierten Autorisierers für AWS IoT Core

Dieses Tutorial zeigt die Schritte zum Erstellen, Validieren und Verwenden einer benutzerdefinierten Authentifizierung mithilfe von AWS CLI. Optional können Sie mithilfe dieses Tutorials Postman verwenden, um Daten mithilfe AWS IoT Core von Publish an zu senden. HTTP API

In diesem Tutorial erfahren Sie, wie Sie eine exemplarische Lambda-Funktion erstellen, die die Autorisierungs- und Authentifizierungslogik implementiert, und einen benutzerdefinierten Autorisierer mithilfe des create-authorizer-Aufrufs mit aktivierter Tokensignatur. Der Autorisierer wird dann mit dem validierttest-invoke-authorizer, und schließlich können Sie Daten an senden, AWS IoT Core indem Sie das HTTP MQTT Testthema Publizieren API verwenden. In der Beispielanforderung wird angegeben, welcher Autorisierer mithilfe des Headers aufgerufen werden soll, und die `x-amz-customauthorizer-name` Anforderungsheader werden übergeben. token-key-name `x-amz-customauthorizer-signature`

Was Sie in diesem Tutorial lernen werden:

- So erstellen Sie eine Lambda-Funktion als benutzerdefinierten Autorisierer-Handler
- Wie erstelle ich einen benutzerdefinierten Autorisierer mit aktivierter Tokensignatur AWS CLI
- So testen Sie Ihren benutzerdefinierten Autorisierer mit dem Befehl test-invoke-authorizer

- So veröffentlichen Sie ein MQTT Thema mithilfe von Postman und validieren die Anfrage mit Ihrem benutzerdefinierten Autorisierer

Für dieses Tutorial brauchen Sie ungefähr 60 Minuten.

In diesem Tutorial führen Sie die folgenden Aktivitäten durch:

- Schritt 1: Erstellen einer Lambda-Funktion für Ihren benutzerdefinierten Autorisierer
- Schritt 2: Erstellen eines öffentlichen und eines privaten Schlüsselpaars für Ihren benutzerdefinierten Autorisierer
- Schritt 3: Erstellen Sie eine benutzerdefinierte Autorisierungsressource und deren Autorisierung
- Schritt 4: Testen Sie den Authorizer, indem Sie ihn anrufen test-invoke-authorizer
- Schritt 5: Testen Sie das Veröffentlichen von MQTT Nachrichten mit Postman
- Schritt 6: Nachrichten im MQTT Testclient anzeigen
- Schritt 7: Überprüfen der Ergebnisse und die nächsten Schritte
- Schritt 8: Bereinigen

Stellen Sie vor Beginn dieses Tutorials sicher, dass Sie über Folgendes verfügen:

- Einrichten AWS-Konto

  Sie benötigen Ihre AWS IoT Handkonsole AWS-Konto , um dieses Tutorial abzuschließen.

  Das Konto, das Sie für dieses Tutorial verwenden, funktioniert am besten, wenn es mindestens die folgenden AWS -verwalteten Richtlinien umfasst:

  - `IAMFullAccess`
  - `AWSIoTFullAccess`
  - `AWSLambda_FullAccess`

  > **Important**
  >
  > Die in diesem Tutorial verwendeten IAM Richtlinien sind toleranter, als Sie sie in einer Produktionsimplementierung befolgen sollten. Stellen Sie in einer Produktionsumgebung sicher, dass Ihre Konto- und Ressourcenrichtlinien nur die erforderlichen Berechtigungen gewähren.

> Wenn Sie IAM Richtlinien für die Produktion erstellen, legen Sie fest, welchen Zugriff Benutzer und Rollen benötigen, und entwerfen Sie dann die Richtlinien, die es ihnen ermöglichen, nur diese Aufgaben auszuführen.
> Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in IAM

- Installiert AWS CLI

  Informationen zur Installation von finden Sie AWS CLI unter Installation von AWS CLI. Für dieses Tutorial ist AWS CLI Version `aws-cli/2.1.3 Python/3.7.4 Darwin/18.7.0 exe/x86_64` oder höher erforderlich.

- SSLTools öffnen

  Die Beispiele in diesem Tutorial verwenden Libre SSL 2.6.5. Sie können für dieses Tutorial auch die Tools von Open SSL v1.1.1i verwenden.

- AWS Lambda Übersicht überprüft

  Wenn Sie Lambda noch nicht verwendet AWS Lambda haben, lesen Sie AWS Lambdaund Erste Schritte mit Lambda, um sich mit den Begriffen und Konzepten vertraut zu machen.

- Es wurde überprüft, wie Anfragen in Postman erstellt werden.

  Weitere Informationen finden Sie unter Erstellen von Anfragen.

- Benutzerdefinierte Autorisierer wurden aus dem vorherigen Tutorial entfernt.

  Sie AWS-Konto können nur eine begrenzte Anzahl von benutzerdefinierten Autorisierern gleichzeitig konfigurieren. Weitere Informationen zum Erstellen eines benutzerdefinierten Autorisierers finden Sie unter the section called “Schritt 8: Bereinigen”.

## Schritt 1: Erstellen einer Lambda-Funktion für Ihren benutzerdefinierten Autorisierer

Die benutzerdefinierte Authentifizierung in AWS IoT Core verwendet Autorisierungsressourcen, die Sie zur Authentifizierung und Autorisierung von Clients erstellen. Die Funktion, die Sie in diesem Abschnitt erstellen, authentifiziert und autorisiert Clients, wenn sie sich mit Ressourcen verbinden und auf sie zugreifen. AWS IoT Core AWS IoT

Die Lambda-Funktion bewirkt Folgendes:

- Wenn eine Anfrage von kommttest-invoke-authorizer, gibt sie eine IAM Richtlinie mit einer `Deny` Aktion zurück.

- Wenn eine Anfrage von Postman kommt HTTP und der `actionToken` Parameter den Wert von hat`allow`, wird eine IAM Richtlinie mit einer `Allow` Aktion zurückgegeben. Andernfalls wird eine IAM Richtlinie mit einer `Deny` Aktion zurückgegeben.

So erstellen Sie die Lambda-Funktion für Ihren benutzerdefinierten Autorisierer

1. Öffnen Sie auf der Lambda-Konsole die Option Funktionen.
2. Wählen Sie Funktion erstellen.
3. Bestätigen Sie, dass Ohne Vorgabe erstellen ausgewählt ist.
4. Unter Grundlegende Informationen:

   a. Geben Sie unter Funktionsname **`custom-auth-function`** ein.

   b. Bestätigen Sie unter Laufzeit Node.js 18.x
5. Wählen Sie Funktion erstellen aus.

   Lambda erstellt eine Node.js-Funktion und eine Ausführungsrolle, die der Funktion die Berechtigung zum Hochladen von Protokollen gewährt. Die Lambda-Funktion übernimmt die Ausführungsrolle, wenn Sie Ihre Funktion aufrufen, und verwendet die Ausführungsrolle, um Anmeldeinformationen für die zu erstellen AWS SDK und Daten aus Ereignisquellen zu lesen.
6. Um den Code und die Konfiguration der Funktion im AWS Cloud9Editor zu sehen, wählen Sie custom-auth-functionim Designerfenster und dann im Navigationsbereich des Editors die Option index.js aus.

   Für Skriptsprachen wie Node.js enthält Lambda eine grundlegende Funktion, die eine Erfolgsantwort zurückgibt. Sie können den AWS Cloud9-Editor verwenden, um Ihre Funktion zu bearbeiten, solange Ihr Quellcode nicht größer als 3 MB ist.
7. Ersetzen Sie den Code index.js im Editor durch den folgenden Code:

```
// A simple Lambda function for an authorizer. It demonstrates
// How to parse a CLI and Http password to generate a response.

export const handler = async (event, context, callback) => {

    //Http parameter to initiate allow/deny request
    const HTTP_PARAM_NAME='actionToken';
    const ALLOW_ACTION = 'Allow';
    const DENY_ACTION = 'Deny';
```

```
    //Event data passed to Lambda function
    var event_str = JSON.stringify(event);
    console.log('Complete event :'+ event_str);

    //Read protocolData from the event json passed to Lambda function
    var protocolData = event.protocolData;
    console.log('protocolData value---> ' + protocolData);

    //Get the dynamic account ID from function's ARN to be used
    // as full resource for IAM policy
    var ACCOUNT_ID = context.invokedFunctionArn.split(":")[4];
    console.log("ACCOUNT_ID---"+ACCOUNT_ID);

    //Get the dynamic region from function's ARN to be used
    // as full resource for IAM policy
    var REGION = context.invokedFunctionArn.split(":")[3];
    console.log("REGION---"+REGION);

    //protocolData data will be undefined if testing is done via CLI.
    // This will help to test the set up.
    if (protocolData === undefined) {

        //If CLI testing, pass deny action as this is for testing purpose only.
        console.log('Using the test-invoke-authorizer cli for testing only');
        callback(null, generateAuthResponse(DENY_ACTION,ACCOUNT_ID,REGION));

    } else{

        //Http Testing from Postman
        //Get the query string from the request
        var queryString = event.protocolData.http.queryString;
        console.log('queryString values -- ' + queryString);
        /*         global URLSearchParams       */
        const params = new URLSearchParams(queryString);
        var action = params.get(HTTP_PARAM_NAME);

        if(action!=null && action.toLowerCase() === 'allow'){

            callback(null, generateAuthResponse(ALLOW_ACTION,ACCOUNT_ID,REGION));

        }else{

            callback(null, generateAuthResponse(DENY_ACTION,ACCOUNT_ID,REGION));
```

```
        }

    }

};

// Helper function to generate the authorization IAM response.
var generateAuthResponse = function(effect,ACCOUNT_ID,REGION) {

    var full_resource = "arn:aws:iot:"+ REGION + ":" + ACCOUNT_ID + ":*";
    console.log("full_resource---"+full_resource);

    var authResponse = {};
    authResponse.isAuthenticated = true;
    authResponse.principalId = 'principalId';

    var policyDocument = {};
    policyDocument.Version = '2012-10-17';
    policyDocument.Statement = [];
    var statement = {};
    statement.Action = 'iot:*';
    statement.Effect = effect;
    statement.Resource = full_resource;
    policyDocument.Statement[0] = statement;
    authResponse.policyDocuments = [policyDocument];
    authResponse.disconnectAfterInSeconds = 3600;
    authResponse.refreshAfterInSeconds = 600;

    console.log('custom auth policy function called from http');
    console.log('authResponse --> ' + JSON.stringify(authResponse));
    console.log(authResponse.policyDocuments[0]);

    return authResponse;
}
```

8. Wählen Sie Bereitstellen.
9. Nachdem Änderungen bereitgestellt über dem Editor angezeigt wird:
    a. Scrollen Sie zum Abschnitt Funktionsübersicht über dem Editor.
    b. Kopieren Sie die Funktion ARN und speichern Sie sie, um sie später in diesem Tutorial zu verwenden.
10. Testen Sie Ihre Funktion.

a. Wählen Sie die Registerkarte Test.

b. Wählen Sie unter Verwendung der Standard-Testeinstellungen Aufrufen.

c. Wenn der Test erfolgreich war, öffnen Sie in den Ausführungsergebnissen die Ansicht Details. Sie sollten das Richtliniendokument sehen, das die Funktion zurückgegeben hat.

   Wenn der Test fehlgeschlagen ist oder Sie kein Richtliniendokument finden, überprüfen Sie den Code, um die Fehler zu finden und zu korrigieren.

## Schritt 2: Erstellen eines öffentlichen und eines privaten Schlüsselpaars für Ihren benutzerdefinierten Autorisierer

Ihr benutzerdefinierter Autorisierer benötigt für seine Authentifizierung einen öffentlichen und einen privaten Schlüssel. Die Befehle in diesem Abschnitt verwenden Open SSL Tools, um dieses key pair zu erstellen.

So erstellen Sie das Paar aus öffentlichem und privatem Schlüssel für Ihren benutzerdefinierten Autorisierer

1. Erstellen Sie die Datei mit dem privaten Schlüssel.

   ```
   openssl genrsa -out private-key.pem 4096
   ```

2. Überprüfen Sie den Speicherort der Datei mit dem privaten Schlüssel, die Sie gerade erstellt haben.

   ```
   openssl rsa -check -in private-key.pem -noout
   ```

   Wenn der Befehl keine Fehler anzeigt, ist die Datei mit dem privaten Schlüssel gültig.

3. Erstellen Sie die Datei mit dem öffentlichen Schlüssel.

   ```
   openssl rsa -in private-key.pem -pubout -out public-key.pem
   ```

4. Überprüfen Sie die Datei mit dem öffentlichen Schlüssel.

   ```
   openssl pkey -inform PEM -pubin -in public-key.pem -noout
   ```

   Wenn der Befehl keine Fehler anzeigt, ist die Datei mit dem öffentlichen Schlüssel gültig.

## Schritt 3: Erstellen Sie eine benutzerdefinierte Autorisierungsressource und deren Autorisierung

Der AWS IoT benutzerdefinierte Autorisierer ist die Ressource, die alle in den vorherigen Schritten erstellten Elemente zusammenfasst. In diesem Abschnitt erstellen Sie eine benutzerdefinierte Autorisierer-Ressource und erteilen ihr die Erlaubnis, die zuvor erstellte Lambda-Funktion auszuführen. Sie können eine benutzerdefinierte Autorisierungsressource erstellen, indem Sie die AWS IoT Konsole AWS CLI, den oder den verwenden. AWS API

Für dieses Tutorial müssen Sie nur einen benutzerdefinierten Autorisierer erstellen. In diesem Abschnitt wird beschrieben, wie Sie mithilfe der AWS IoT Konsole und der erstellen AWS CLI, sodass Sie die Methode verwenden können, die für Sie am bequemsten ist. Es gibt keinen Unterschied zwischen den mithilfe dieser beiden Methoden erstellen benutzerdefinierten Autorisierer-Ressourcen.

Erstellen Sie eine benutzerdefinierte Authorizer-Ressource

Wählen Sie eine dieser Optionen, um Ihre benutzerdefinierte Autorisierer-Ressource zu erstellen.

- Erstellen Sie mithilfe der Konsole einen benutzerdefinierten Autorisierer AWS IoT
- So erstellen Sie einen benutzerdefinierten Autorisierer mithilfe der AWS CLI

So erstellen Sie einen benutzerdefinierten Autorisierer (Konsole)

1. Öffnen Sie die Seite Benutzerdefinierter Autorisierer der AWS IoT Konsole und wählen Sie Create Authorizer aus.
2. In Autorisierer erstellen:
    a. Geben Sie in das Feld Autorisierer-Name **`my-new-authorizer`** ein.
    b. Markieren Sie unter Autorisierer-Status die Option Aktiv.
    c. Wählen Sie in der Autorisierer-Funktion die Lambda-Funktion aus, die Sie zuvor erstellt haben.
    d. Unter Token-Validierung – optional:
        i. Aktivieren Sie die Token-Validierung.
        ii. Geben Sie **`tokenKeyName`** in das Feld Token-Schlüsselname ein.
        iii. Wählen Sie Schlüssel hinzufügen.
        iv. Geben Sie unter Schlüsselname **`FirstKey`** ein.

v. Geben Sie in das Feld Öffentlicher Schlüssel den Inhalt der Datei `public-key.pem` ein. Achten Sie darauf, die Zeilen aus der Datei mit `-----BEGIN PUBLIC KEY-----` und `-----END PUBLIC KEY-----` einzuschließen und dem Inhalt der Datei keine Zeilenvorschübe, Zeilenumbrüche oder andere Zeichen hinzuzufügen oder aus ihm zu entfernen. Die Zeichenfolge, die Sie eingeben, sollte in etwa wie im folgenden Beispiel aussehen.

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAvEBzOk4vhN+3LgslvEWt
sLCqNmt5Damas3bmiTRvq2gjRJ6KXGTGQChqArAJwL1a9dkS9+maaXC3vc6xzx9z
QPu/vQOe5tyzz1MsKdmtFGxMqQ3qjEXAMPLEOmqyUKPP5mff58k6ePSfXAnzBH0q
lg2HioefrpU5OSAnpuRAjYKofKjbc2Vrn6N2G7hV+IfTBvCElf0csalS/Rk4phD5
oa4Y0GHISRnevypg5C8n9Rrz91PWGqP6M/q5DNJJXjMyleG92hQgu1N696bn5Dw8
FhedszFa6b2x6xrItZFzewNQkPMLMFhNrQIIyvshtT/F1LVCS5+v8AQ8UGGDfZmv
QeqAMAF7WgagDMXcfgKSVU8yid2sIm56qsCLMvD2Sq8Lgzpey9N5ON1o1Cvldwvc
KrJJtgwW6hVqRGuShnownLpgG86M6neZ5sRMbVNZO8OzcobLngJ0Ibw9KkcUdklW
gvZ6HEJqBY2XE70iEXAMPLETPHzhqvK6Ei1HGxpHsXx6BNft582J1VpgYjXha8oa
/NN7l7Zbj/euAb41IVtmX8JrD9z613d1iM5L8HluJlUzn62Q+VeNV2tdA7MfPfMC
8btGYladFAnitThaz6+F0VSBJPu7pZQoLnqyEp5zLMtF+kFl2yOBmGAP0RBivRd9
JWBUCG0bqcLQPeQyjbXSOfUCAwEAAQ==
-----END PUBLIC KEY-----
```

3. Wählen Sie Autorisierer erstellen.
4. Wenn die benutzerdefinierte Autorisierer-Ressource erstellt wurde, wird die Liste der benutzerdefinierten Autorisierer angezeigt und Ihr neuer benutzerdefinierter Autorisierer sollte in der Liste angezeigt werden. Sie können dann mit dem nächsten Abschnitt fortfahren, um ihn zu testen.

   Wenn Sie einen Fehler sehen, überprüfen Sie den Fehler und versuchen Sie erneut, Ihren benutzerdefinierten Autorisierer zu erstellen, und überprüfen Sie die Einträge erneut. Beachten Sie, dass jeder Benutzer einen eindeutigen Namen haben muss.

So erstellen Sie einen benutzerdefinierten Autorisierer (AWS CLI)

1. Ersetzen Sie Ihre Werte durch `authorizer-function-arn` und `token-signing-public-keys`, und führen Sie dann den folgenden Befehl aus:

```
aws iot create-authorizer \
--authorizer-name "my-new-authorizer" \
--token-key-name "tokenKeyName" \
```

```
--status ACTIVE \
--no-signing-disabled \
--authorizer-function-arn "arn:aws:lambda:Region:57EXAMPLE833:function:custom-auth-function" \
--token-signing-public-keys FirstKey="-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAvEBzOk4vhN+3LgslvEWt
sLCqNmt5Damas3bmiTRvq2gjRJ6KXGTGQChqArAJwL1a9dkS9+maaXC3vc6xzx9z
QPu/vQOe5tyzz1MsKdmtFGxMqQ3qjEXAMPLEOmqyUKPP5mff58k6ePSfXAnzBH0q
lg2HioefrpU5OSAnpuRAjYKofKjbc2Vrn6N2G7hV+IfTBvCElf0csalS/Rk4phD5
oa4Y0GHISRnevypg5C8n9Rrz91PWGqP6M/q5DNJJXjMyleG92hQgu1N696bn5Dw8
FhedszFa6b2x6xrItZFzewNQkPMLMFhNrQIIyvshtT/F1LVCS5+v8AQ8UGGDfZmv
QeqAMAF7WgagDMXcfgKSVU8yid2sIm56qsCLMvD2Sq8Lgzpey9N5ON1o1Cvldwvc
KrJJtgwW6hVqRGuShnownLpgG86M6neZ5sRMbVNZO8OzcobLngJ0Ibw9KkcUdklW
gvZ6HEJqBY2XE70iEXAMPLETPHzhqvK6Ei1HGxpHsXx6BNft582J1VpgYjXha8oa
/NN7l7Zbj/euAb41IVtmX8JrD9z613d1iM5L8HluJlUzn62Q+VeNV2tdA7MfPfMC
8btGYladFAnitThaz6+F0VSBJPu7pZQoLnqyEp5zLMtF+kFl2yOBmGAP0RBivRd9
JWBUCG0bqcLQPeQyjbXSOfUCAwEAAQ==
-----END PUBLIC KEY-----"
```

Wobei gilt:

- Der `authorizer-function-arn` Wert ist der Amazon-Ressourcenname (ARN) der Lambda-Funktion, die Sie für Ihren benutzerdefinierten Authorizer erstellt haben.
- Der Wert `token-signing-public-keys` umfasst den Namen des Schlüssels, **`FirstKey`**, und den Inhalt der Datei `public-key.pem`. Achten Sie darauf, die Zeilen aus der Datei mit `-----BEGIN PUBLIC KEY-----` und `-----END PUBLIC KEY-----` einzuschließen und dem Inhalt der Datei keine Zeilenvorschübe, Zeilenumbrüche oder andere Zeichen hinzuzufügen oder aus ihm zu entfernen.

  Hinweis: Seien Sie vorsichtig bei der Eingabe des öffentlichen Schlüssels, da jede Wertänderung des öffentlichen Schlüssels diesen unbrauchbar macht.

2. Wenn der benutzerdefinierte Autorisierer erstellt wurde, gibt der Befehl den Namen und den Namen ARN der neuen Ressource zurück, z. B. im Folgenden.

```
{
    "authorizerName": "my-new-authorizer",
    "authorizerArn": "arn:aws:iot:Region:57EXAMPLE833:authorizer/my-new-authorizer"
}
```

Speichern Sie den Wert `authorizerArn` zur Verwendung im nächsten Schritt.

Denken Sie daran, dass jeder Benutzer einen eindeutigen Namen haben muss.

### Autorisieren der benutzerdefinierten Autorisierer-Ressource

In diesem Abschnitt erteilen Sie der benutzerdefinierten Autorisierer-Ressource, die Sie gerade erstellt haben, die Berechtigung zum Ausführen der Lambda-Funktion. Um die Berechtigung zu erteilen, können Sie den Befehl add-permission CLI verwenden.

Erteilen Sie Ihrer Lambda-Funktion die Erlaubnis mit dem AWS CLI

1. Geben Sie nach der Eingabe Ihrer Werte den folgenden Befehl ein. Beachten Sie, dass der Wert `statement-id` eindeutig sein muss. Ersetzen Sie *`Id-1234`* durch einen anderen Wert, wenn Sie dieses Tutorial schon einmal ausgeführt haben oder wenn Sie einen Fehler `ResourceConflictException` angezeigt bekommen.

   ```
   aws lambda add-permission  \
   --function-name "custom-auth-function" \
   --principal "iot.amazonaws.com" \
   --action "lambda:InvokeFunction" \
   --statement-id "Id-1234" \
   --source-arn authorizerArn
   ```

2. Wenn der Befehl erfolgreich ist, gibt er eine Berechtigungsanweisung zurück, wie in diesem Beispiel. Sie können mit dem nächsten Abschnitt fortfahren, um den benutzerdefinierten Autorisierer zu testen.

   ```
   {
       "Statement": "{\"Sid\":\"Id-1234\",\"Effect\":\"Allow\",\"Principal
   \":{\"Service\":\"iot.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction
   \",\"Resource\":\"arn:aws:lambda:Region:57EXAMPLE833:function:custom-
   auth-function\",\"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":
   \"arn:aws:lambda:Region:57EXAMPLE833:function:custom-auth-function\"}}}"
   }
   ```

   Wenn der Befehl nicht erfolgreich ist, wird ein Fehler zurückgegeben, wie in diesem Beispiel. Sie müssen den Fehler überprüfen und korrigieren, bevor Sie fortfahren können.

```
An error occurred (AccessDeniedException) when calling the AddPermission operation:
 User: arn:aws:iam::57EXAMPLE833:user/EXAMPLE-1 is not authorized to perform:
 lambda:AddPer
mission on resource: arn:aws:lambda:Region:57EXAMPLE833:function:custom-auth-
function
```

## Schritt 4: Testen Sie den Authorizer, indem Sie ihn anrufen test-invoke-authorizer

Wenn alle Ressourcen definiert sind, rufen Sie in diesem Abschnitt test-invoke-authorizer von der Befehlszeile aus auf, um den Autorisierungsdurchgang zu testen.

Beachten Sie, dass der Autorisierer nicht definiert ist, wenn er von der Befehlszeile aus aufgerufen `protocolData` wird, sodass der Autorisierer immer ein Dokument zurückgibt. DENY Dieser Test bestätigt jedoch, dass Ihr benutzerdefinierter Autorisierer und Ihre Lambda-Funktion korrekt konfiguriert sind – auch wenn die Lambda-Funktion nicht vollständig getestet wird.

Um Ihren benutzerdefinierten Authorizer und seine Lambda-Funktion zu testen, verwenden Sie AWS CLI

1. Führen Sie in dem Verzeichnis, welches die `private-key.pem`-Datei, die Sie in einem vorherigen Schritt erstellt haben, enthält, den folgenden Befehl aus.

   ```
   echo -n "tokenKeyValue" | openssl dgst -sha256 -sign private-key.pem | openssl
    base64 -A
   ```

   Mit diesem Befehl wird eine Signaturzeichenfolge zur Verwendung im nächsten Schritt generiert. Die Signaturzeichenfolge sollte wie folgt aussehen:

   ```
   dBwykzlb+fo+JmSGdwoGr8dyC2qB/IyLefJJr+rbCvmu9Jl4KHAA9DG+V
   +MMWu09YSA86+64Y3Gt4tOykpZqn9mn
   VB1wyxp+0bDZh8hmqUAUH3fwi3fPjBvCa4cwNuLQNqBZzbCvsluv7i2IMjEg
   +CPY0zrWt1jr9BikgGPDxWkjaeeh
   bQHHTo357TegKs9pP30Uf4TrxypNmFswA5k7QIc01n4bIyRTm90OyZ94R4bdJsHNig1JePgnuOBvMGCEFE09jGjj
   szEHfgAUAQIWXiVGQj16BU1xKpTGSiTAwheLKUjITOEXAMPLECK3aHKYKY
   +d1vTvdthKtYHBq8MjhzJ0kggbt29V
   QJCb8RilN/P5+vcVniSXWPplyB5jkYs9UvG08REoy64AtizfUhvSul/r/F3VV8ITtQp3aXiUtcspACi6ca
   +tsDuX
   f3LzCwQQF/YSUy02u5XkWn
   +sto6KCkpNlkD0wU8gl3+kOzxrthnQ8gEajd5Iylx230iqcXo3osjPha7JDyWM5o+K
   ```

```
EWckTe91I1mokDr5sJ4JXixvnJTVSx1li49IalW4en1DAkc1a0s2U2UNm236EXAMPLELotyh7h
+flFeloZlAWQFH
xRlXsPqiVKS1ZIUClaZWprh/orDJplpiWfBgBIOgokJIDGP9gwhXIIk7zWrGmWpMK9o=
```

Kopieren Sie diese Signaturzeichenfolge zur Verwendung im nächsten Schritt. Achten Sie darauf, keine zusätzlichen Zeichen einzufügen oder Zeichen wegzulassen.

2. Ersetzen Sie in diesem Befehl den Wert `token-signature` durch die Signaturzeichenfolge aus dem vorherigen Schritt und führen Sie diesen Befehl aus, um Ihren Autorisierer zu testen.

```
aws iot test-invoke-authorizer \
--authorizer-name my-new-authorizer \
--token tokenKeyValue \
--token-signature dBwykzlb+fo+JmSGdwoGr8dyC2qB/IyLefJJr
+rbCvmu9Jl4KHAA9DG+V+MMWu09YSA86+64Y3Gt4tOykpZqn9mnVB1wyxp
+0bDZh8hmqUAUH3fwi3fPjBvCa4cwNuLQNqBZzbCvsluv7i2IMjEg
+CPY0zrWt1jr9BikgGPDxWkjaeehbQHHTo357TegKs9pP30Uf4TrxypNmFswA5k7QIc01n4bIyRTm90OyZ94R4bdJsh
+d1vTvdthKtYHBq8MjhzJ0kggbt29VQJCb8RilN/
P5+vcVniSXWPplyB5jkYs9UvG08REoy64AtizfUhvSul/r/F3VV8ITtQp3aXiUtcspACi6ca
+tsDuXf3LzCwQQF/YSUy02u5XkWn
+sto6KCkpNlkD0wU8gl3+kOzxrthnQ8gEajd5Iylx230iqcXo3osjPha7JDyWM5o
+KEWckTe91I1mokDr5sJ4JXixvnJTVSx1li49IalW4en1DAkc1a0s2U2UNm236EXAMPLELotyh7h
+flFeloZlAWQFHxRlXsPqiVKS1ZIUClaZWprh/orDJplpiWfBgBIOgokJIDGP9gwhXIIk7zWrGmWpMK9o=
```

Wenn der Befehl erfolgreich ist, gibt er die Informationen zurück, die von Ihrer benutzerdefinierten Autorisierungsfunktion generiert wurden, wie in diesem Beispiel.

```
{
    "isAuthenticated": true,
    "principalId": "principalId",
    "policyDocuments": [
        "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Action\":\"iot:*\",\"Effect
\":\"Deny\",\"Resource\":\"arn:aws:iot:Region:57EXAMPLE833:*\"}]}"
    ],
    "refreshAfterInSeconds": 600,
    "disconnectAfterInSeconds": 3600
}
```

Wenn bei diesem Befehl ein Fehler zurückgegeben wird, überprüfen Sie den Fehler und überprüfen Sie erneut die Befehle, die Sie in diesem Abschnitt verwendet haben.

## Schritt 5: Testen Sie das Veröffentlichen von MQTT Nachrichten mit Postman

1. Um Ihren Gerätedaten-Endpunkt über die Befehlszeile abzurufen, rufen Sie describe-endpoint auf, wie hier dargestellt

   ```
   aws iot describe-endpoint --output text --endpoint-type iot:Data-ATS
   ```

   Speichern Sie diese Adresse, um sie *device_data_endpoint_address* in einem späteren Schritt zu verwenden.

2. Öffnen Sie ein neues Postman-Fenster und erstellen Sie eine neue HTTP POST Anfrage.

   a. Öffnen Sie auf Ihrem Computer die Postman-App.

   b. Wählen Sie in Postman im Menü Datei die Option Neu….

   c. Wählen Sie im Dialogfeld Neu die Option Anfrage.

   d. Unter Anfrage speichern:

      i. Geben Sie unter Name der Anfrage **`Custom authorizer test request`** ein.

      ii. Wählen Sie unter Sammlung oder Ordner zum Speichern auswählen: eine Sammlung aus bzw. erstellen Sie eine, in der diese Anfrage gespeichert werden soll.

      iii. Wählen Sie Speichern unter. ***collection_name***

3. Erstellen Sie die POST Anfrage, um Ihren benutzerdefinierten Authorizer zu testen.

   a. Wählen Sie in der Auswahl der Anforderungsmethode neben dem URL Feld die Option. POST

   b. Erstellen Sie in dem URL Feld das URL für Ihre Anfrage, indem Sie in einem vorherigen Schritt Folgendes URL zusammen mit dem *device_data_endpoint_address* Befehl from the describe-endpoint verwenden.

      ```
      https://device_data_endpoint_address:443/topics/test/cust-auth/topic?
      qos=0&actionToken=allow
      ```

      Beachten Sie, dass dies den `actionToken=allow` Abfrageparameter URL beinhaltet, der Ihre Lambda-Funktion anweist, ein Richtliniendokument zurückzugeben, das den Zugriff AWS IoT auf ermöglicht. Nachdem Sie den eingegeben habenURL, werden die Abfrageparameter auch auf der Registerkarte Params von Postman angezeigt.

   c. Wählen Sie auf der Registerkarte Auth im Feld Typ die Option Keine Auth.

d. Auf der Registerkarte Header:

i. Wenn ein Host-Schlüssel aktiviert ist, deaktivieren Sie diesen.

ii. Fügen Sie diese neuen Header am Ende der Header-Liste hinzu, und bestätigen Sie, dass sie aktiviert sind. Ersetzen Sie den **`Host`** Wert durch Ihren *`device_data_endpoint_address`* und den **`x-amz-customauthorizer-signature`** Wert durch die Signaturzeichenfolge, die Sie mit dem test-invoke-authorize Befehl im vorherigen Abschnitt verwendet haben.

| Schlüssel | Wert |
| --- | --- |
| **`x-amz-customauthorizer-name`** | **`my-new-authorizer`** |
| **`Host`** | *`device_data_endpoint_address`* |
| **`tokenKeyName`** | **`tokenKeyValue`** |

| Schlüssel | Wert |
| --- | --- |
| **x-amz-customauthorizer-signature** | *dBwykzlb+fo+JmSGdwoGr8dyC2qB/IyLefJJr+rbCvmu9Jl4KHAA9DG+V+MMWu09YSA86+64Y3Gt4tOykpZqn9mnVB1wyxp+0bDZh8hmqUAUH3fwi3fPjBvCa4cwNuLQNqBZzbCvsluv7i2IMjEg+CPY0zrWt1jr9BikgGPDxWkjaeehbQHHTo357TegKs9pP30Uf4TrxypNmFswA5k7QIc01n4bIyRTm90OyZ94R4bdJsHNig1JePgnuOBvMGCEFE09jGjjszEHfgAUAQIWXiVGQj16BU1xKpTGSiTAwheLKUjITOEXAMPLECK3aHKYKY+d1vTvdthKtYHBq8MjhzJ0kggbt29VQJCb8RilN/P5+vcVniSXWPplyB5jkYs9UvG08REoy64AtizfUhvSul/r/F3VV8ITtQp3aXiUtcspACi6ca+tsDuXf3LzCwQQF/YSUy02u5XkWn+sto6KCkpNlkD0wU8gl3+kOzxrthnQ8gEajd5Iylx230iqcXo3osjPha7JDyWM5o+KEWckTe91I1mokDr5sJ4JXixvnJTVSx1li49IalW4en1DAkc1a0s2U2UNm236EXAMPLELotyh7h+flFeloZlAWQFHxRlXsPqiVKS1ZIUClaZWprh/orDJplpiWfBgBIOgokJIDGP9gwhXIIk7zWrGmWpMK9o=* |

e. Auf der Registerkarte „Text“:

i. Wählen Sie im Optionsfeld für das Datenformat die Option Raw.

ii. Wählen Sie in der Datentypliste JavaScript.

iii. Geben Sie in das Textfeld die JSON folgende Nachrichten-Payload für Ihre Testnachricht ein:

```
{
```

```
    "data_mode": "test",
    "vibration": 200,
    "temperature": 40
}
```

4. Wählen Sie Senden aus, um die Anfrage zu senden.

   Wenn die Anfrage erfolgreich war, wird Folgendes zurückgegeben:

   ```
   {
       "message": "OK",
       "traceId": "ff35c33f-409a-ea90-b06f-fbEXAMPLE25c"
   }
   ```

   Die erfolgreiche Antwort weist darauf hin, dass Ihr benutzerdefinierter Autorisierer die Verbindung zu zugelassen hat AWS IoT und dass die Testnachricht an den Broker in zugestellt wurde. AWS IoT Core

   Wenn ein Fehler zurückgegeben wird, überprüfen Sie die Fehlermeldung*device_data_endpoint_address*, die Signaturzeichenfolge und die anderen Header-Werte.

Bewahren Sie diese Anfrage in Postman auf, um Sie im nächsten Abschnitt zu verwenden.

## Schritt 6: Nachrichten im MQTT Testclient anzeigen

Im vorherigen Schritt haben Sie mithilfe AWS IoT von Postman simulierte Gerätenachrichten an gesendet. Die erfolgreiche Antwort wies darauf hin, dass Ihr benutzerdefinierter Autorisierer die Verbindung zum AWS IoT gestattet hat und dass die Testnachricht an den Broker in AWS IoT Core zugestellt wurde. In diesem Abschnitt verwenden Sie den MQTT Testclient in der AWS IoT Konsole, um den Nachrichteninhalt dieser Nachricht so zu sehen, wie es bei anderen Geräten und Diensten der Fall ist.

So zeigen Sie die von Ihrem benutzerdefinierten Autorisierer autorisierten Testnachrichten an

1. Öffnen Sie in der AWS IoT Konsole den MQTTTestclient.
2. Geben Sie auf der Registerkarte Thema abonnieren im Themenfilter **`test/cust-auth/topic`** ein – das Nachrichtenthema aus dem vorherigen Abschnitt, das im Postman-Beispiel verwendet wurde.

3. Wählen Sie Abonnieren.

   Lassen Sie dieses Fenster für den nächsten Schritt geöffnet.

4. Wählen Sie in Postman in der Anfrage, die Sie für den vorherigen Abschnitt erstellt haben, die Option Senden.

   Überprüfen Sie die Antwort, um sicherzustellen, dass sie erfolgreich war. Falls nicht, beheben Sie den Fehler, wie im vorherigen Abschnitt beschrieben.

5. Im MQTTTestclient sollten Sie einen neuen Eintrag sehen, der das Nachrichtenthema und, falls erweitert, die Nachrichten-Payload aus der Anfrage enthält, die Sie von Postman gesendet haben.

   Wenn Sie Ihre Nachrichten im MQTTTestclient nicht sehen, sollten Sie Folgendes überprüfen:

   - Stellen Sie sicher, dass Ihre Postman-Anfrage erfolgreich zurückgegeben wurde. Wenn die Verbindung AWS IoT abgelehnt wird und ein Fehler zurückgegeben wird, wird die Nachricht in der Anfrage nicht an den Message Broker weitergeleitet.
   - Stellen Sie sicher, dass die zum Öffnen der AWS IoT Konsole AWS-Region verwendeten AWS-Konto und dieselben sind, die Sie im URL Postman verwenden.
   - Stellen Sie sicher, dass Sie den entsprechenden Endpunkt für den benutzerdefinierten Authorizer verwenden. Der Standard-IoT-Endpunkt unterstützt möglicherweise nicht die Verwendung benutzerdefinierter Autorisierer mit Lambda-Funktionen. Stattdessen können Sie Domänenkonfigurationen verwenden, um einen neuen Endpunkt zu definieren und diesen Endpunkt dann für den benutzerdefinierten Autorisierer anzugeben.
   - Stellen Sie sicher, dass Sie das Thema im MQTTTestclient korrekt eingegeben haben. Beim Themenfilter wird die Groß-/Kleinschreibung berücksichtigt. Im Zweifelsfall können Sie auch das **#** Thema abonnieren, das alle MQTT Nachrichten abonniert, die den Message Broker passieren AWS-Konto und zum Öffnen der AWS IoT Konsole AWS-Region verwendet werden.

## Schritt 7: Überprüfen der Ergebnisse und die nächsten Schritte

In diesem Tutorial:

- Haben Sie eine Lambda-Funktion als benutzerdefinierten Autorisierer-Handler erstellt.
- Haben Sie einen benutzerdefinierten Autorisierer mit aktivierter Token-Signatur erstellt.
- Haben Sie Ihren benutzerdefinierten Autorisierer mit dem Befehl test-invoke-authorizer getestet.

- Sie haben ein MQTT Thema mit Postman veröffentlicht und die Anfrage mit Ihrem benutzerdefinierten Autorisierer validiert
- Sie haben den MQTTTestclient verwendet, um die von Ihrem Postman-Test gesendeten Nachrichten anzusehen

Nächste Schritte

Nachdem Sie einige Nachrichten von Postman gesendet haben, um zu überprüfen, ob der benutzerdefinierte Autorisierer funktioniert, versuchen Sie zu experimentieren, um festzustellen, wie sich Änderungen an verschiedenen Aspekten dieses Tutorials auf die Ergebnisse auswirken. Hier sind einige Beispiele, die Ihnen den Einstieg erleichtern sollen.

- Ändern Sie die Signaturzeichenfolge so, dass sie nicht mehr gültig ist, um zu sehen, wie unbefugte Verbindungsversuche behandelt werden. Sie sollten eine Fehlerantwort wie diese erhalten, und die Nachricht sollte nicht im MQTTTestclient erscheinen.

```
{
    "message": "Forbidden",
    "traceId": "15969756-a4a4-917c-b47a-5433e25b1356"
}
```

- Weitere Informationen zum Auffinden von Fehlern, die bei der Entwicklung und Verwendung von AWS IoT Regeln auftreten können, finden Sie unterÜberwachung AWS IoT.

## Schritt 8: Bereinigen

Wenn Sie dieses Tutorial wiederholen möchten, müssen Sie möglicherweise einige Ihrer benutzerdefinierten Autorisierer entfernen. Sie AWS-Konto können nur eine begrenzte Anzahl von benutzerdefinierten Autorisierern gleichzeitig konfigurieren. Sie erhalten einen, `LimitExceededException` wenn Sie versuchen, einen neuen hinzuzufügen, ohne einen vorhandenen benutzerdefinierten Autorisierer zu entfernen.

So entfernen Sie einen benutzerdefinierten Autorisierer (Konsole)

1. Öffnen Sie die Seite Benutzerdefinierter Autorisierer der AWS IoT Konsole und suchen Sie in der Liste der benutzerdefinierten Autorisierer nach dem benutzerdefinierten Autorisierer, den Sie entfernen möchten.

2. Öffnen Sie die Seite mit den Details des benutzerdefinierten Autorisierers, und wählen Sie aus dem Menü Aktionen die Option Bearbeiten.
3. Heben Sie die Auswahl von Autorisierer aktivieren auf, und wählen Sie dann Aktualisieren.

   Während ein benutzerdefinierter Autorisierer aktiv ist, können Sie ihn nicht löschen.
4. Öffnen Sie auf der Seite mit den Details des benutzerdefinierten Autorisierers das Menü Aktionen, und wählen Sie Löschen.

So entfernen Sie einen benutzerdefinierten Autorisierer (AWS CLI)

1. Listen Sie die benutzerdefinierten Autorisierer auf, die Sie installiert haben, und suchen Sie nach dem Namen des benutzerdefinierten Autorisierers, den Sie löschen möchten.

   ```
   aws iot list-authorizers
   ```
2. Legen Sie den benutzerdefinierten Autorisierer auf `inactive` fest, indem Sie diesen Befehl ausführen, nachdem Sie *`Custom_Auth_Name`* durch `authorizerName` des benutzerdefinierten Autorisierers, der gelöscht werden soll, ersetzt haben.

   ```
   aws iot update-authorizer --status INACTIVE --authorizer-name Custom_Auth_Name
   ```
3. Löschen Sie den benutzerdefinierten Autorisierer, indem Sie diesen Befehl ausführen, nachdem Sie *`Custom_Auth_Name`* durch `authorizerName` des benutzerdefinierten Autorisierers, der gelöscht werden soll, ersetzt haben.

   ```
   aws iot delete-authorizer --authorizer-name Custom_Auth_Name
   ```

## Tutorial: Überwachung der Bodenfeuchte mit einem AWS IoT Raspberry Pi

Dieses Tutorial zeigt Ihnen, wie Sie einen Raspberry Pi, einen Feuchtigkeitssensor, verwenden und AWS IoT den Bodenfeuchtigkeitsgehalt einer Zimmerpflanze oder eines Gartens überwachen. Der Raspberry Pi führt Code aus, der den Feuchtigkeitsgehalt und die Temperatur vom Sensor liest und die Daten dann an sendet AWS IoT. Sie erstellen eine Regel AWS IoT , die eine E-Mail an eine Adresse sendet, die ein Amazon SNS SNS-Thema abonniert hat, wenn der Feuchtigkeitsgehalt unter einen Schwellenwert fällt.

> **Note**
>
> Dieses Tutorial ist möglicherweise nicht aktuell. Einige Verweise wurden möglicherweise seit der ursprünglichen Veröffentlichung dieses Themas ersetzt.

Inhalt


- Voraussetzungen
- Einrichten AWS IoT
  - Schritt 1: Erstellen Sie die AWS IoT Richtlinie
  - Schritt 2: Erstellen Sie das AWS IoT Ding, das Zertifikat und den privaten Schlüssel
  - Schritt 3: Erstellen eines Amazon-SNS-Themas und -Abonnements
  - Schritt 4: Erstellen Sie eine AWS IoT Regel zum Senden einer E-Mail
- Einrichten des Raspberry Pi und des Feuchtesensors


## Voraussetzungen

Zum Durchführen dieses Tutorials benötigen Sie Folgendes:

- Ein. AWS-Konto
- Ein IAM-Benutzer mit Administratorberechtigungen.
- Ein Entwicklungscomputer mit Windows, macOS, Linux oder Unix für den Zugriff auf die AWS IoT -Konsole.
- Ein Raspberry Pi 3B oder 4B mit dem neuesten Raspberry Pi-Betriebssystem. Installationsanweisungen finden Sie unter Installieren eines Betriebssystems auf der Raspberry Pi-Website.
- Ein Monitor, eine Tastatur, eine Maus und eine WLAN-Verbindung oder eine Ethernet-Verbindung für Ihren Raspberry Pi.
- Ein mit Raspberry Pi kompatibler Feuchtigkeitssensor. Bei dem in diesem Tutorial verwendeten Sensor handelt es sich um einen Adafruit STEMMA I2C Capacitive Moisture Sensor mit einer JST 4-adrigen Kabelbuchsenleiste.

## Einrichten AWS IoT

Um dieses Tutorial abzuschließen, müssen Sie die folgenden Ressourcen erstellen. Um ein Gerät zu verbinden AWS IoT, erstellen Sie ein IoT-Ding, ein Gerätezertifikat und eine AWS IoT Richtlinie.

- AWS IoT Irgendein Ding.

  Ein Objekt stellt ein physisches Gerät (in diesem Fall Ihr Rasberry Pi) dar und enthält statische Metadaten über das Gerät.
- Ein Gerätezertifikat.

  Alle Geräte müssen über ein Gerätezertifikat verfügen, um eine Verbindung herzustellen und sich mit AWS IoT zu authentifizieren.
- Eine AWS IoT Richtlinie.

  Jedem Gerätezertifikat sind eine oder mehrere AWS IoT Richtlinien zugeordnet. Diese Richtlinien legen fest, auf welche AWS IoT Ressourcen das Gerät zugreifen kann.
- Ein AWS IoT Root-CA-Zertifikat.

  Geräte und andere Clients verwenden ein AWS IoT Root-CA-Zertifikat, um den AWS IoT Server zu authentifizieren, mit dem sie kommunizieren. Weitere Informationen finden Sie unter Serverauthentifizierung.
- Eine AWS IoT Regel.

  Eine Regel enthält eine Abfrage und mindestens eine Regelaktion. Die Abfrage extrahiert Daten aus Gerätenachrichten, um zu bestimmen, ob die Nachrichtendaten verarbeitet werden sollen. Die Regelaktion gibt an, was zu tun ist, wenn die Daten mit der Abfrage übereinstimmen.
- Ein Amazon SNS-Thema und ein Themenabonnement.

  Die Regel überwacht die Feuchtigkeitsdaten über Ihren Raspberry Pi. Wenn der Wert unter einem Schwellenwert liegt, wird eine Nachricht an das Amazon-SNS-Thema gesendet. Amazon SNS sendet diese Nachricht an alle E-Mail-Adressen, die das Thema abonniert haben.

### Schritt 1: Erstellen Sie die AWS IoT Richtlinie

Erstellen Sie eine AWS IoT Richtlinie, die es Ihrem Raspberry Pi ermöglicht, eine Verbindung herzustellen und Nachrichten an diese zu senden AWS IoT.

1. Wenn in der AWS IoT -Konsole die Schaltfläche Erste Schritte erscheint, klicken Sie darauf. Erweitern Sie andernfalls im Navigationsbereich  Sicherheit und wählen Sie dann Richtlinien aus.
2. Wenn das Dialogfeld You don‘t have any policies yet (Sie haben noch keine Richtlinien) angezeigt wird, wählen Sie Create a policy (Richtlinie erstellen) aus. Wählen Sie andernfalls Erstellen.
3. Geben Sie einen Namen für die AWS IoT Richtlinie ein (z. B.**`MoistureSensorPolicy`**).
4. Ersetzen Sie im Abschnitt Add statements (Anweisungen hinzufügen) die vorhandene Richtlinie durch das folgende JSON-Objekt. Ersetzen Sie *`region`* und *`account`* durch Ihre AWS-Konto Nummer AWS-Region und.

```
{
   "Version": "2012-10-17",
   "Statement": [{
         "Effect": "Allow",
         "Action": "iot:Connect",
         "Resource": "arn:aws:iot:region:account:client/RaspberryPi"
      },
      {
         "Effect": "Allow",
         "Action": "iot:Publish",
         "Resource": [
            "arn:aws:iot:region:account:topic/$aws/things/RaspberryPi/shadow/
update",
            "arn:aws:iot:region:account:topic/$aws/things/RaspberryPi/shadow/
delete",
            "arn:aws:iot:region:account:topic/$aws/things/RaspberryPi/shadow/get"
         ]
      },
      {
         "Effect": "Allow",
         "Action": "iot:Receive",
         "Resource": [
            "arn:aws:iot:region:account:topic/$aws/things/RaspberryPi/shadow/
update/accepted",
            "arn:aws:iot:region:account:topic/$aws/things/RaspberryPi/shadow/
delete/accepted",
            "arn:aws:iot:region:account:topic/$aws/things/RaspberryPi/shadow/get/
accepted",
            "arn:aws:iot:region:account:topic/$aws/things/RaspberryPi/shadow/
update/rejected",
```

```
            "arn:aws:iot:region:account:topic/$aws/things/RaspberryPi/shadow/
delete/rejected"
         ]
      },
      {
         "Effect": "Allow",
         "Action": "iot:Subscribe",
         "Resource": [
            "arn:aws:iot:region:account:topicfilter/$aws/things/RaspberryPi/shadow/
update/accepted",
            "arn:aws:iot:region:account:topicfilter/$aws/things/RaspberryPi/shadow/
delete/accepted",
            "arn:aws:iot:region:account:topicfilter/$aws/things/RaspberryPi/shadow/
get/accepted",
            "arn:aws:iot:region:account:topicfilter/$aws/things/RaspberryPi/shadow/
update/rejected",
            "arn:aws:iot:region:account:topicfilter/$aws/things/RaspberryPi/shadow/
delete/rejected"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "iot:GetThingShadow",
            "iot:UpdateThingShadow",
            "iot:DeleteThingShadow"
         ],
         "Resource": "arn:aws:iot:region:account:thing/RaspberryPi"

      }
   ]
}
```

5. Wählen Sie Erstellen aus.

### Schritt 2: Erstellen Sie das AWS IoT Ding, das Zertifikat und den privaten Schlüssel

Erstellen Sie in der AWS IoT Registrierung ein Ding, das Ihren Raspberry Pi repräsentiert.

1. Wählen Sie in der AWS IoT -Konsole im Navigationsbereich Manage (Verwalten) und dann Things (Objekte).

2. Wenn das Dialogfeld You don‘t have any things yet (Sie haben noch keine Objekte) angezeigt wird, wählen Sie Register a thing (Objekt registrieren) aus. Wählen Sie andernfalls Erstellen.
3. Wählen Sie auf der Seite „ AWS IoT Dinge erstellen“ die Option Ein einzelnes Ding erstellen aus.
4. Geben Sie auf der Seite Add your device to the device registry (Ihr Gerät zur Geräteregistrierung hinzufügen) einen Namen für Ihr IoT-Objekt ein (z. B. **`RaspberryPi`**) und wählen Sie dann Next (Weiter). Sie können den Namen eines Objekts nicht mehr ändern, nachdem Sie es erstellt haben. Um den Namen eines Objekts zu ändern, müssen Sie ein neues Objekt erstellen, diesem den neuen Namen geben und dann das alte Objekt löschen.
5. Wählen Sie auf der Seite Add a certificate for your thing (Fügen Sie ein Zertifikat für Ihr Objekt hinzu.) die Option Create certificate (Zertifikat erstellen).
6. Klicken Sie auf die Download-Links, um das Zertifikat, den privaten Schlüssel und das CA-Stammzertifikat herunterzuladen.

   > **Important**
   >
   > Dies ist das einzige Mal, dass Sie Ihr Zertifikat und Ihren privaten Schlüssel herunterladen können.

7. Wählen Sie Aktivieren aus, um Ihr Zertifikat zu aktivieren. Das Zertifikat muss aktiv sein, damit ein Gerät eine Verbindung mit AWS IoT herstellen kann.
8. Wählen Sie Attach a policy (Richtlinie anfügen) aus.
9. Wählen MoistureSensorPolicySie unter Richtlinie für Ihr Ding hinzufügen die Option und anschließend Ding registrieren aus.

### Schritt 3: Erstellen eines Amazon-SNS-Themas und -Abonnements

Erstellen eines Amazon-SNS-Themas und -Abonnements.

1. Klicken Sie in der AWS SNS-Konsole im Navigationsbereich auf Themen und wählen Sie dann Thema erstellen aus.
2. Wählen Sie Typ als Standard und geben Sie einen Namen für das Thema ein (z. B.**`MoistureSensorTopic`**).
3. Geben Sie einen Anzeigenamen für das Thema ein (z. B. **`Moisture Sensor Topic`**). Dies ist der Name, der für Ihr Thema in der Amazon SNS -Konsole angezeigt wird.
4. Wählen Sie Thema erstellen aus.

5. Wählen Sie auf der Seite mit den Details des Amazon SNS-Themas die Option Create subscription (Abonnement erstellen) aus.
6. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.
7. Geben Sie unter Endpunkt Ihre E-Mail-Adresse ein.
8. Klicken Sie auf Create subscription (Abonnement erstellen).
9. Öffnen Sie Ihren E-Mail-Client und suchen Sie nach einer Nachricht mit dem Betreff **`MoistureSensorTopic`**. Öffnen Sie die E-Mail und klicken Sie auf den Link Confirm subscription (Abonnement bestätigen).

> **Important**
>
> Sie erhalten keine E-Mail-Benachrichtigungen von diesem Amazon SNS-Thema, bis Sie das Abonnement bestätigen.

Sie sollten eine E-Mail-Nachricht mit dem von Ihnen eingegebenen Text erhalten.

Schritt 4: Erstellen Sie eine AWS IoT Regel zum Senden einer E-Mail

Eine AWS IoT Regel definiert eine Abfrage und eine oder mehrere Aktionen, die ausgeführt werden sollen, wenn eine Nachricht von einem Gerät empfangen wird. Die AWS IoT Regel-Engine wartet auf Nachrichten, die von Geräten gesendet werden, und bestimmt anhand der in den Nachrichten enthaltenen Daten, ob Maßnahmen ergriffen werden sollten. Weitere Informationen finden Sie unter Regeln für AWS IoT.

In diesem Tutorial veröffentlicht Ihr Raspberry Pi Nachrichten auf `aws/things/RaspberryPi/shadow/update`. Dies ist ein internes MQTT-Thema, das von Geräten und dem Thing Shadow-Service verwendet wird. Der Raspberry Pi veröffentlicht Nachrichten in der folgenden Form:

```
{
    "reported": {
        "moisture" : moisture-reading,
        "temp" : temperature-reading
    }
}
```

Sie erstellen eine Abfrage, die die Feuchtigkeits- und Temperaturdaten aus der eingehenden Nachricht extrahiert. Sie erstellen auch eine Amazon SNS-Aktion, die die Daten übernimmt und

an Abonnenten des Amazon SNS-Themas sendet, wenn der Feuchtigkeitswert unter einem Schwellenwert liegt.

Erstellen Sie eine Amazon SNS-Regel

1. Wählen Sie in der AWS IoT Konsole Nachrichtenrouting und dann Regeln aus. Wenn das Dialogfeld You don't have any rules yet (Sie haben noch keine Regeln) angezeigt wird, wählen Sie Create a rule (Regel erstellen) aus. Wählen Sie andernfalls Regel erstellen.
2. Geben Sie auf der Seite mit den Regeleigenschaften einen Regelnamen wie **`MoistureSensorRule`** ein und geben Sie eine kurze Regelbeschreibung ein, z.B. **`Sends an alert when soil moisture level readings are too low`**.
3. Wählen Sie Weiter und konfigurieren Sie Ihre SQL-Anweisung. Wählen Sie die SQL-Version 2016-03-23 und geben Sie die folgende AWS IoT SQL-Abfrageanweisung ein:

   ```
   SELECT * FROM '$aws/things/RaspberryPi/shadow/update/accepted' WHERE
    state.reported.moisture < 400
   ```

   Diese Anweisung löst die Regelaktion aus, wenn der `moisture`-Lesevorgang kleiner als `400` ist.

   > **Note**
   >
   > Möglicherweise müssen Sie einen anderen Wert verwenden. Nachdem Sie den Code auf Ihrem Raspberry Pi ausgeführt haben, können Sie die Werte sehen, die Sie von Ihrem Sensor erhalten, indem Sie den Sensor berühren, ihn in Wasser platzieren oder ihn in einem Übertopf platzieren.

4. Wählen Sie Weiter und hängen Sie Regelaktionen an. Wählen Sie für Aktion 1 Einfacher Benachrichtigungsservice aus. Die Beschreibung für diese Regelaktion lautet Eine Nachricht als SNS-Push-Benachrichtigung senden.
5. Wählen Sie als SNS-Thema das Thema, das Sie in, erstellt haben Schritt 3: Erstellen eines Amazon-SNS-Themas und -Abonnements MoistureSensorTopic, und behalten Sie das Nachrichtenformat RAW bei. Wählen Sie für IAM Role (IAM-Rolle) die Option Create a New Role (Neue Rolle erstellen) aus. Geben Sie einen Namen für die Rolle ein, beispielsweise **`LowMoistureTopicRole`**, und wählen Sie dann Rolle erstellen aus.

6. Wählen Sie Weiter aus, um die Regel zu überprüfen, und klicken Sie dann auf Erstellen, um die Regel zu erstellen.

## Einrichten des Raspberry Pi und des Feuchtesensors

Setzen Sie Ihre Micro-SD-Karte in den Raspberry Pi ein, schließen Sie Ihren Monitor, Ihre Tastatur, Ihre Maus und Ihr Ethernet-Kabel an, falls Sie kein WLAN verwenden. Schließen Sie das Stromkabel noch nicht an.

Schließen Sie das JST-Überbrückungskabel an den Feuchtigkeitssensor an. Die andere Seite des Kabels hat vier Drähte:

- Grün: I2C SCL
- Weiß: I2C SDA
- Rot: Stromversorgung (3,5 V)
- Schwarz: Erdung

Halten Sie den Raspberry Pi mit der Ethernet-Buchse auf der rechten Seite. In dieser Ausrichtung befinden sich oben zwei Reihen von GPIO-Stiften. Verbinden Sie die Drähte vom Feuchtigkeitssensor in der folgenden Reihenfolge mit der unteren Reihe der Stifte. Beginnen Sie mit dem Stift ganz links. Schließen Sie rot (Strom), weiß (SDA) und grün (SCL) an. Überspringen Sie einen Stift und schließen Sie dann den schwarzen Draht (Erdung) an. Weitere Informationen finden Sie unter Python Computer Wiring.

Schließen Sie das Stromkabel an den Raspberry Pi und das andere Ende an eine Steckdose an, um ihn einzuschalten.

Konfigurieren Ihres Raspberry Pi

1. Wählen Sie unter Welcome to Raspberry Pi (Willkommen bei Raspberry Pi), Next (Weiter).
2. Wählen Sie Ihr Land, Ihre Sprache, die Zeitzone und das Tastaturlayout. Wählen Sie Weiter aus.
3. Geben Sie ein Passwort für Ihren Raspberry Pi ein und wählen Sie dann Next (Weiter).
4. Wählen Sie Ihr WLAN und klicken Sie dann auf Next (Weiter). Wenn Sie kein WLAN verwenden, wählen Sie Skip (Überspringen) aus.
5. Wählen Sie Next (Weiter), um nach Software-Updates zu suchen. Wenn die Updates abgeschlossen sind, wählen Sie Restart (Neu starten), um Ihren Raspberry Pi neu zu starten.

Nach dem Start Ihres Raspberry Pi aktivieren Sie die I2C-Schnittstelle.

1. Klicken Sie in der oberen linken Ecke des Raspbian-Desktops auf das Raspberry-Symbol, wählen Sie Preferences (Einstellungen) und dann Raspberry Pi Configuration (Raspberry Pi-Konfiguration).
2. Wählen Sie auf der Registerkarte Interfaces (Schnittstellen) für I2C die Option Enable (Aktivieren).
3. Wählen Sie OK aus.

Die Bibliotheken für den STEMMA-Feuchtigkeitssensor von Adafruit sind dafür geschrieben. CircuitPython Um sie auf einem Raspberry Pi auszuführen, müssen Sie die neueste Version von Python 3 installieren.

1. Führen Sie die folgenden Befehle über eine Eingabeaufforderung aus, um Ihre Raspberry Pi-Software zu aktualisieren:

   ```
   sudo apt-get update
   ```

   ```
   sudo apt-get upgrade
   ```
2. Führen Sie den folgenden Befehl aus, um Ihre Python 3-Installation zu aktualisieren:

   ```
   sudo pip3 install --upgrade setuptools
   ```
3. Führen Sie den folgenden Befehl aus, um die Raspberry Pi GPIO-Bibliotheken zu installieren:

   ```
   pip3 install RPI.GPIO
   ```
4. Führen Sie den folgenden Befehl aus, um die Adafruit Blinka-Bibliotheken zu installieren:

   ```
   pip3 install adafruit-blinka
   ```

   Weitere Informationen finden Sie unter CircuitPython Bibliotheken auf dem Raspberry Pi installieren.
5. Führen Sie den folgenden Befehl aus, um die Adafruit Seesaw-Bibliotheken zu installieren:

   ```
   sudo pip3 install adafruit-circuitpython-seesaw
   ```
6. Führen Sie den folgenden Befehl aus, um das AWS IoT Device SDK für Python zu installieren:

   ```
   pip3 install AWSIoTPythonSDK
   ```

Ihr Raspberry Pi verfügt jetzt über alle erforderlichen Bibliotheken. Erstellen Sie eine Datei mit dem Namen **`moistureSensor.py`** und kopieren Sie den folgenden Python-Code in die Datei:

```
from adafruit_seesaw.seesaw import Seesaw
from AWSIoTPythonSDK.MQTTLib import AWSIoTMQTTShadowClient
from board import SCL, SDA

import logging
import time
import json
import argparse
import busio

# Shadow JSON schema:
#
# {
#   "state": {
#       "desired":{
#           "moisture":<INT VALUE>,
#           "temp":<INT VALUE>
#       }
#   }
# }

# Function called when a shadow is updated
def customShadowCallback_Update(payload, responseStatus, token):

    # Display status and data from update request
    if responseStatus == "timeout":
        print("Update request " + token + " time out!")

    if responseStatus == "accepted":
        payloadDict = json.loads(payload)
        print("~~~~~~~~~~~~~~~~~~~~~")
        print("Update request with token: " + token + " accepted!")
        print("moisture: " + str(payloadDict["state"]["reported"]["moisture"]))
        print("temperature: " + str(payloadDict["state"]["reported"]["temp"]))
        print("~~~~~~~~~~~~~~~~~~~~~\n\n")

    if responseStatus == "rejected":
        print("Update request " + token + " rejected!")
```

```
# Function called when a shadow is deleted
def customShadowCallback_Delete(payload, responseStatus, token):

     # Display status and data from delete request
    if responseStatus == "timeout":
        print("Delete request " + token + " time out!")

    if responseStatus == "accepted":
        print("~~~~~~~~~~~~~~~~~~~~~~~")
        print("Delete request with token: " + token + " accepted!")
        print("~~~~~~~~~~~~~~~~~~~~~~~\n\n")

    if responseStatus == "rejected":
        print("Delete request " + token + " rejected!")


# Read in command-line parameters
def parseArgs():

    parser = argparse.ArgumentParser()
    parser.add_argument("-e", "--endpoint", action="store", required=True, dest="host",
 help="Your device data endpoint")
    parser.add_argument("-r", "--rootCA", action="store", required=True,
 dest="rootCAPath", help="Root CA file path")
    parser.add_argument("-c", "--cert", action="store", dest="certificatePath",
 help="Certificate file path")
    parser.add_argument("-k", "--key", action="store", dest="privateKeyPath",
 help="Private key file path")
    parser.add_argument("-p", "--port", action="store", dest="port", type=int,
 help="Port number override")
    parser.add_argument("-n", "--thingName", action="store", dest="thingName",
 default="Bot", help="Targeted thing name")
    parser.add_argument("-id", "--clientId", action="store", dest="clientId",
 default="basicShadowUpdater", help="Targeted client id")

    args = parser.parse_args()
    return args


# Configure logging
# AWSIoTMQTTShadowClient writes data to the log
def configureLogging():

    logger = logging.getLogger("AWSIoTPythonSDK.core")
```

```
    logger.setLevel(logging.DEBUG)
    streamHandler = logging.StreamHandler()
    formatter = logging.Formatter('%(asctime)s - %(name)s - %(levelname)s -
 %(message)s')
    streamHandler.setFormatter(formatter)
    logger.addHandler(streamHandler)


# Parse command line arguments
args = parseArgs()

if not args.certificatePath or not args.privateKeyPath:
    parser.error("Missing credentials for authentication.")
    exit(2)

# If no --port argument is passed, default to 8883
if not args.port:
    args.port = 8883


# Init AWSIoTMQTTShadowClient
myAWSIoTMQTTShadowClient = None
myAWSIoTMQTTShadowClient = AWSIoTMQTTShadowClient(args.clientId)
myAWSIoTMQTTShadowClient.configureEndpoint(args.host, args.port)
myAWSIoTMQTTShadowClient.configureCredentials(args.rootCAPath, args.privateKeyPath,
 args.certificatePath)

# AWSIoTMQTTShadowClient connection configuration
myAWSIoTMQTTShadowClient.configureAutoReconnectBackoffTime(1, 32, 20)
myAWSIoTMQTTShadowClient.configureConnectDisconnectTimeout(10) # 10 sec
myAWSIoTMQTTShadowClient.configureMQTTOperationTimeout(5) # 5 sec

# Initialize Raspberry Pi's I2C interface
i2c_bus = busio.I2C(SCL, SDA)

# Intialize SeeSaw, Adafruit's Circuit Python library
ss = Seesaw(i2c_bus, addr=0x36)

# Connect to AWS IoT
myAWSIoTMQTTShadowClient.connect()

# Create a device shadow handler, use this to update and delete shadow document
deviceShadowHandler =
 myAWSIoTMQTTShadowClient.createShadowHandlerWithName(args.thingName, True)
```

```
# Delete current shadow JSON doc
deviceShadowHandler.shadowDelete(customShadowCallback_Delete, 5)

# Read data from moisture sensor and update shadow
while True:

    # read moisture level through capacitive touch pad
    moistureLevel = ss.moisture_read()

    # read temperature from the temperature sensor
    temp = ss.get_temp()

    # Display moisture and temp readings
    print("Moisture Level: {}".format(moistureLevel))
    print("Temperature: {}".format(temp))

    # Create message payload
    payload = {"state":{"reported":{"moisture":str(moistureLevel),"temp":str(temp)}}}

    # Update shadow
    deviceShadowHandler.shadowUpdate(json.dumps(payload), customShadowCallback_Update,
 5)
    time.sleep(1)
```

Speichern Sie die Datei an einem Speicherort, an dem Sie sie finden können. Führen Sie `moistureSensor.py` über die Befehlszeile mit den folgenden Parametern aus:

Endpunkt

Ihr benutzerdefinierter AWS IoT Endpunkt. Weitere Informationen finden Sie unter Geräteschatten-REST-API.

rootCA

Der vollständige Pfad zu Ihrem AWS IoT Root-CA-Zertifikat.

cert

Der vollständige Pfad zu Ihrem AWS IoT Gerätezertifikat.

Schlüssel

Der vollständige Pfad zum privaten Schlüssel Ihres AWS IoT Gerätezertifikats.

thingName

Ihr Objektname (in diesem Fall `RaspberryPi`).

clientId

Die MQTT-Client-ID. Verwenden Sie `RaspberryPi`.

Die Befehlszeile sollte wie folgt aussehen:

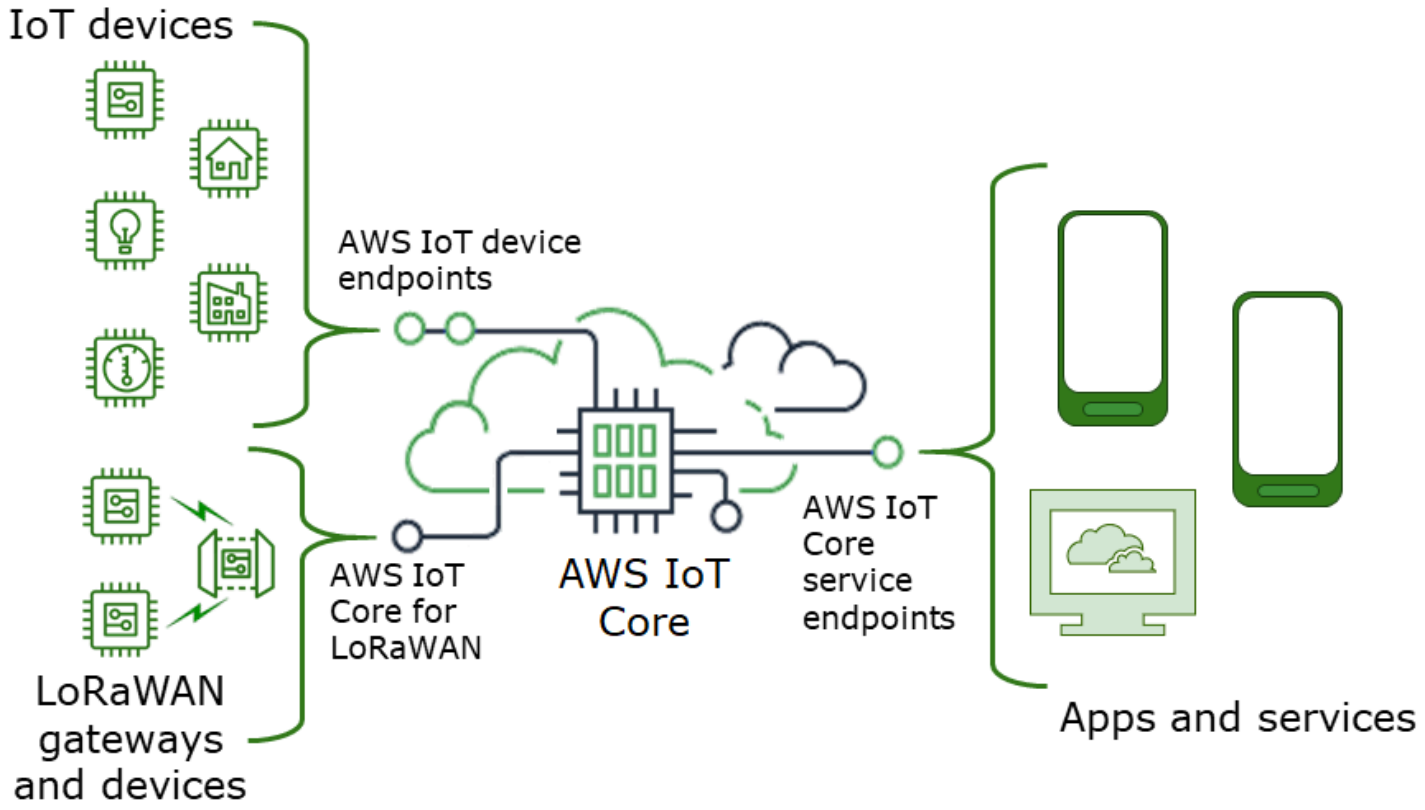
```
python3 moistureSensor.py --endpoint your-endpoint --rootCA ~/certs/
AmazonRootCA1.pem --cert ~/certs/raspberrypi-certificate.pem.crt --key
~/certs/raspberrypi-private.pem.key --thingName RaspberryPi --clientId
RaspberryPi
```

Versuchen Sie, den Sensor zu berühren, ihn in einen Übertopf zu legen oder ihn in ein Glas Wasser zu legen, um zu sehen, wie der Sensor auf verschiedene Feuchtigkeitsstufen reagiert. Bei Bedarf können Sie den Schwellenwert in `MoistureSensorRule` ändern. Wenn der Messwert des Feuchtigkeitssensors unter den in der SQL-Abfrageanweisung Ihrer Regel angegebenen Wert fällt, wird eine Nachricht im Amazon SNS SNS-Thema AWS IoT veröffentlicht. Sie sollten eine E-Mail-Nachricht erhalten, die die Feuchtigkeits- und Temperaturdaten enthält.

Nachdem Sie den Empfang von E-Mail-Nachrichten von Amazon SNS überprüft haben, drücken Sie CTRL+C (STRG+C), um das Python-Programm zu beenden. Es ist unwahrscheinlich, dass das Python-Programm so viele Nachrichten sendet, dass Kosten anfallen, aber es hat sich bewährt, das Programm zu beenden, wenn Sie fertig sind.

# Verbinden mit AWS IoT Core

AWS IoT Core unterstützt Verbindungen mit IoT-Geräten, drahtlosen Gateways, Diensten und Apps. Geräte stellen eine Verbindung her, AWS IoT Core damit sie Daten an AWS IoT Dienste und andere Geräte senden und Daten von diesen empfangen können. Apps und andere Dienste stellen ebenfalls eine Verbindung her, AWS IoT Core um die IoT-Geräte zu steuern und zu verwalten und die Daten aus Ihrer IoT-Lösung zu verarbeiten. In diesem Abschnitt wird beschrieben, wie Sie AWS IoT Core für jeden Aspekt Ihrer IoT-Lösung die beste Art der Verbindung und Kommunikation auswählen.




Es gibt verschiedene Möglichkeiten, mit zu interagieren. AWS IoT Apps und Dienste können die WAN-Regionen Endpunkte von AWS IoT Core – Steuerebene und -Endpunkte verwenden, mit denen Geräte eine Verbindung herstellen können, AWS IoT Core indem sie AWS IoT Geräteendpunkte oder AWS IoT Core für LoRa WAN-Regionen und -Endpunkte verwenden.

## Endpunkte von AWS IoT Core – Steuerebene

Die AWS IoT Core Endpunkte auf der Steuerungsebene bieten Zugriff auf Funktionen zur Steuerung und Verwaltung Ihrer AWS IoT Lösung.

- Endpunkte

  Die Endpunkte von AWS IoT Core – Steuerebene und AWS IoT Core Device Advisor – Steuerebene sind regionsspezifisch und unter AWS IoT Core -Endpunkte und -Kontingente aufgeführt. Die Endpunkte haben folgende Formate:

| Zweck des Endpunkts | Endpunkt-Format | Dient |
| --- | --- | --- |
| AWS IoT Core – Steuerebene | `iot.aws-region .amazonaws.com` | AWS IoT API für die Steuerungsebene |
| AWS IoT Core Device Advisor — Steuerungsebene | `api.iotdeviceadvisor. aws-region .amazonaws.com` | AWS IoT Core Device Advisor-API für Steuerungsebene |

- SDKs und Tools

  Sie AWS SDKsbieten sprachspezifischen Support für AWS IoT Core APIs die und andere APIs AWS Dienste. The AWS Mobile SDKs bietet App-Entwicklern plattformspezifischen Support für die AWS IoT Core API und andere AWS Dienste auf Mobilgeräten.

  Das AWS CLIbietet Befehlszeilenzugriff auf die Funktionen, die von den Dienstendpunkten bereitgestellt werden. AWS IoT AWS Tools für PowerShell stellt Tools zur Verwaltung von AWS Diensten und Ressourcen in der PowerShell Skriptumgebung bereit.

- Authentifizierung

  Die Dienstendpunkte verwenden IAM-Benutzer und AWS Anmeldeinformationen, um Benutzer zu authentifizieren.

- Weitere Informationen

  Weitere Informationen und Links zu SDK-Referenzen finden Sie unter the section called “Connect zu AWS IoT Core Service-Endpunkten her”.

# AWS IoT Geräteendpunkte

Die AWS IoT Geräteendpunkte unterstützen die Kommunikation zwischen Ihren IoT-Geräten und AWS IoT.

- Endpunkte

  Die Geräteendpunkte unterstützen AWS IoT Core und AWS IoT Device Management funktionieren. Sie sind spezifisch für Sie AWS-Konto und Sie können anhand des describe-endpoint Befehls sehen, um welche es sich handelt.

| Zweck des Endpunkts | Endpunkt-Format | Dient |
|---|---|---|
| AWS IoT Core – Datenebene | Siehe ???. | AWS IoT Datenebene-API |
| AWS IoT Device Management – Jobdaten | Siehe ???. | AWS IoT Datenebene-API für Jobs |
| AWS IoT Device Advisor — Datenebene | Siehe ???. | Nicht zutreffend |
| AWS IoT Device Management – Fleet Hub | Nicht zutreffend | Nicht zutreffend |
| AWS IoT Device Management – Secure Tunneling | `api.tunneling.iot.` *`aws-region`* `.amazonaws.com` | AWS IoT Sichere Tunneling-API |

  Weitere Informationen zu diesen Endpunkten und den Funktionen, die sie unterstützen, finden Sie unter the section called “AWS IoT Gerätedaten und Dienstendpunkte”.

- SDKs

  Das AWS IoT Gerät SDKs bietet sprachspezifische Unterstützung für die Protokolle Message Queueing Telemetry Transport (MQTT) und WebSocket Secure (WSS), mit denen Geräte kommunizieren. AWS IoTAWS Mobil SDKsbietet auch Unterstützung für die MQTT-Gerätekommunikation und andere AWS IoT APIs Dienste auf APIs Mobilgeräten. AWS

- Authentifizierung

  Die Geräteendpunkte verwenden X.509-Zertifikate oder AWS IAM-Benutzer mit Anmeldeinformationen, um Benutzer zu authentifizieren.

- Weitere Informationen

Weitere Informationen und Links zu SDK-Referenzen finden Sie unter the section called “AWS IoT Gerät SDKs”.

# AWS IoT Core für WAN-Gateways und -Geräte LoRa

AWS IoT Core für LoRa WAN verbindet drahtlose Gateways und Geräte mit. AWS IoT Core

- Endpunkte

  AWS IoT Core für LoRa WAN verwaltet die Gateway-Verbindungen zu konto- und regionsspezifischen Endpunkten AWS IoT Core . Gateways können eine Verbindung zum CUPS-Endpunkt (Configuration and Update Server) Ihres Kontos herstellen, AWS IoT Core der für WAN bereitgestellt wird. LoRa

| Zweck des Endpunkts | Endpunkt-Format | Dient |
|---|---|---|
| Konfigurations- und Aktualisierungsserver (CUPS) | *account-specific-prefix* .cups.lorawan. *aws-region* .amazonaws.com:443 | Gateway-Kommunikation mit dem von AWS IoT Core for LoRa WAN bereitgestellten Configuration and Update Server |
| LoRaWAN-Netzwerkserver (LNS) | *account-specific-prefix* .gateway.lorawan. *aws-region* .amazonaws.com:443 | Gateway-Kommunikation mit dem LoRa WAN-Netzwerkserver, bereitgestellt von AWS IoT Core for LoRa WAN |

- SDKs

  Die AWS IoT Wireless-API, AWS IoT Core auf der das LoRa WAN basiert, wird vom AWS SDK unterstützt. Weitere Informationen finden Sie unter AWS SDKs und Toolkits.

- Authentifizierung

  AWS IoT Core Verwenden Sie für die LoRa WAN-Gerätekommunikation X.509-Zertifikate, um die Kommunikation mit zu sichern. AWS IoT

- Weitere Informationen

Weitere Informationen zur Konfiguration und Verbindung drahtloser Geräte finden Sie unter AWS IoT Core LoRaWAN-Regionen und -Endpunkte.

# Connect zu AWS IoT Core Service-Endpunkten her

Sie können auf die Funktionen der AWS IoT Core Steuerungsebene zugreifen AWS CLI, indem Sie das AWS SDK für Ihre bevorzugte Sprache verwenden oder indem Sie die REST-API direkt aufrufen. Wir empfehlen, das AWS CLI oder ein AWS SDK für die Interaktion zu verwenden AWS IoT Core , da sie die bewährten Methoden für das Aufrufen von AWS Diensten enthalten. Der APIs direkte Aufruf von REST ist eine Option, aber Sie müssen die erforderlichen Sicherheitsanmeldedaten angeben, die den Zugriff auf die API ermöglichen.

> **Note**
>
> IoT-Geräte sollten AWS IoT Gerät SDKs verwenden. Die Geräte SDKs sind für die Verwendung auf Geräten optimiert, unterstützen die MQTT-Kommunikation mit AWS IoT Geräten und unterstützen die AWS IoT APIs am häufigsten verwendeten Geräte. Weitere Informationen über das Gerät SDKs und die Funktionen, die es bietet, finden Sie unterAWS IoT Gerät SDKs.
> Mobilgeräte sollten AWS Mobil SDKs verwenden. Die Mobilgeräte SDKs bieten Unterstützung für AWS IoT APIs die Kommunikation mit MQTT-Geräten und andere AWS Dienste auf Mobilgeräten. APIs Weitere Informationen über das Handy SDKs und die Funktionen, die es bietet, finden Sie unterAWS Mobil SDKs.

Sie können AWS Amplify Tools und Ressourcen in Web- und Mobilanwendungen verwenden, um einfacher eine Verbindung herzustellen AWS IoT Core. Weitere Informationen zum Herstellen einer Verbindung mit Amplify finden Sie PubSubin der Amplify-Dokumentation. AWS IoT Core

In den folgenden Abschnitten werden die Tools beschrieben SDKs , die Sie zur Entwicklung und Interaktion mit AWS IoT anderen AWS Diensten verwenden können. Eine vollständige Liste der AWS Tools und Entwicklungskits, mit denen Apps erstellt und verwaltet werden können AWS, finden Sie unter Tools, auf denen Sie aufbauen können AWS.

## AWS CLI für AWS IoT Core

Das AWS CLI bietet Befehlszeilenzugriff auf. AWS APIs

- Installation

  Informationen zur Installation von finden Sie unter Installation von. AWS CLI AWS CLI
- Authentifizierung

  Der AWS CLI verwendet Anmeldeinformationen von Ihrem AWS-Konto.
- Referenz

  Informationen zu den AWS CLI Befehlen für diese AWS IoT Core Dienste finden Sie unter:
  - AWS CLI Befehlsreferenz für IoT
  - AWS CLI Befehlsreferenz für IoT-Daten
  - AWS CLI Befehlsreferenz für IoT-Jobdaten
  - AWS CLI Befehlsreferenz für sicheres IoT-Tunneling

Tools zur Verwaltung von AWS Diensten und Ressourcen in der PowerShell Skriptumgebung finden Sie unter AWS Tools für. PowerShell

## AWS SDKs

Damit AWS SDKs können Ihre Apps und kompatiblen Geräte andere AWS Dienste aufrufen AWS IoT APIs . APIs Dieser Abschnitt enthält Links zur AWS SDKs und zur API-Referenzdokumentation für APIs die AWS IoT Core Dienste.

Sie AWS SDKs unterstützen diese AWS IoT Core APIs

- AWS IoT
- AWS IoT Datenebene
- AWS IoT Datenebene für Jobs
- AWS IoT Sicheres Tunneling
- AWS IoT Drahtlos

C++

So installieren Sie AWS SDK für C++ und nutzen es zum Herstellen einer Verbindung mit dem AWS IoT:

1. Folgen Sie den Anweisungen unter Erste Schritte mit dem AWS SDK for C++

In diesen Anweisungen wird beschrieben, wie Sie:

- Das SDK aus Quelldateien installieren und erstellen
- Anmeldeinformationen bereitstellen, um das SDK mit Ihrem AWS-Konto zu verwenden
- Das SDK in Ihrer App oder Ihrem Dienst initialisieren und beenden
- Erstellen Sie ein CMake Projekt, um Ihre App oder Ihren Dienst zu erstellen

2. Eine Beispiel-App erstellen und ausführen Beispiel-Apps, die das AWS SDK für C++ verwenden, finden Sie unter AWS SDK für C++ -Codebeispiele.

Dokumentation für die AWS IoT Core Dienste, die der AWS SDK für C++ unterstützt

- AWS: :Io TClient „-Referenzdokumentation
- Aws: :Io TData Plane: TData PlaneClient :Io Referenzdokumentation
- Aws: :Io TJobsDataPlane: :Io Referenzdokumentation TJobs DataPlaneClient
- Aws: :Io TSecure Tunneling: :Io Referenzdokumentation TSecure TunnelingClient

Go

So installieren Sie AWS SDK für Go und nutzen es zum Herstellen einer Verbindung mit dem AWS IoT:

1. Folgen Sie den Anweisungen unter Erste Schritte mit dem AWS SDK für Go

   In diesen Anweisungen wird beschrieben, wie Sie:

   - Installieren Sie das AWS SDK für Go
   - Den Zugriffsschlüssel für das SDK beziehen, um auf Ihr AWS-Konto zuzugreifen
   - Pakete in den Quellcode unserer Apps oder Dienste importieren

2. Eine Beispiel-App erstellen und ausführen. Informationen zu Beispiel-Apps, die AWS SDK für Go nutzen, finden Sie unter AWS SDK für Go -Codebeispiele.

Dokumentation für die AWS IoT Core Dienste, die der AWS SDK für Go unterstützt

- Referenzdokumentation zu IoT
- Referenzdokumentation zu Io TData Plane
- Io TJobs DataPlane Referenzdokumentation

- Referenzdokumentation zu Io TSecure Tunneling

Java

So installieren Sie AWS SDK für Java und nutzen es zum Herstellen einer Verbindung mit dem AWS IoT:

1. Folgen Sie den Anweisungen unter Erste Schritte mit AWS SDK for Java 2.x

   In diesen Anweisungen wird beschrieben, wie Sie:

   - Melden Sie sich an AWS und erstellen Sie einen IAM-Benutzer
   - Das SDK herunterladen
   - Richten Sie AWS Anmeldeinformationen und Region ein
   - Das SDK mit Apache Maven verwenden
   - Das SDK mit Gradle verwenden
2. Mit einem der AWS SDK for Java 2.x Codebeispiele eine Beispiel-App erstellen und ausführen.
3. Die SDK-API-Referenzdokumentation prüfen

Dokumentation für die AWS IoT Core Dienste, die der AWS SDK für Java unterstützt

- IotClient Referenzdokumentation
- IotDataPlaneClient Referenzdokumentation
- IotJobsDataPlaneClient Referenzdokumentation
- TSecureTunnelingClient Io-Referenzdokumentation

JavaScript

Um das zu installieren AWS SDK für JavaScript und es für die Verbindung zu verwenden AWS IoT:

1. Folgen Sie den Anweisungen in Einrichten von AWS SDK für JavaScript. Diese Anweisungen gelten für die Verwendung von AWS SDK für JavaScript im Browser und mit Node.JS. Stellen Sie sicher, dass Sie die für Ihre Installation geltenden Anweisungen befolgen.

   In diesen Anweisungen wird beschrieben, wie Sie:

   - Auf Voraussetzungen prüfen

- Installieren Sie das SDK für JavaScript
- Laden Sie das SDK für JavaScript

2. Eine Beispiel-App erstellen und ausführen, um mit dem SDK zu beginnen, wie in der Option Erste Schritte für Ihre Umgebung beschrieben wird.
   - Beginnen Sie mit dem AWS SDK für JavaScript im Browser, oder
   - Beginnen Sie mit dem AWS SDK für JavaScript in Node.js

Dokumentation für die AWS IoT Core Dienste, die der AWS SDK für JavaScript unterstützt

- `AWS.Iot reference documentation`
- `AWS.IotData reference documentation`
- `AWS.IotJobsDataPlane reference documentation`
- `AWS.IotSecureTunneling reference documentation`

.NET

So installieren Sie AWS SDK für .NET und nutzen es zum Herstellen einer Verbindung mit dem AWS IoT:

1. Folgen Sie den Anweisungen unter AWS SDK für .NET Umgebung einrichten
2. Folgen Sie den Anweisungen unter AWS SDK für .NET Projekt einrichten

   In diesen Anweisungen wird beschrieben, wie Sie:
   - Ein neues Projekt starten
   - Besorgen und konfigurieren Sie AWS Anmeldeinformationen
   - Installieren Sie AWS SDK-Pakete
3. Erstellen Sie eines der Beispielprogramme unter Arbeiten mit AWS Diensten im AWS SDK for .NET und führen Sie es aus
4. Die SDK-API-Referenzdokumentation prüfen

Dokumentation für die AWS IoT Core Dienste, die der AWS SDK für .NET unterstützt

- Referenzdokumentation zu Amazon.IoT.Model
- Amazon. IotData.Referenzdokumentation zum Modell

- Amazon.IO TJobs DataPlane .Modell-Referenzdokumentation
- Amazon.IO Tunneling.Modell-Referenzdokumentation TSecure

PHP

So installieren Sie AWS SDK für PHP und nutzen es zum Herstellen einer Verbindung mit dem AWS IoT:

1. Folgen Sie den Anweisungen unter Erste Schritte mit Version 3 AWS SDK für PHP

   In diesen Anweisungen wird beschrieben, wie Sie:
   - Auf Voraussetzungen prüfen
   - Das SDK installieren
   - Das SDK auf ein PHP-Skript anwenden
2. Eine Beispiel-App mit einem der AWS SDK für PHP Version 3-Codebeispiele erstellen und ausführen

Dokumentation für die AWS IoT Core Dienste, die der AWS SDK für PHP unterstützt

- TClient Io-Referenzdokumentation
- TDataPlaneClient Io-Referenzdokumentation
- TJobsDataPlaneClient Io-Referenzdokumentation
- TSecureTunnelingClient Io-Referenzdokumentation

Python

So installieren Sie AWS SDK für Python (Boto3) und nutzen es zum Herstellen einer Verbindung mit dem AWS IoT:

1. Folgen Sie den Anweisungen unter AWS SDK für Python (Boto3) Schnellstart

   In diesen Anweisungen wird beschrieben, wie Sie:
   - Das SDK installieren
   - Das SDKs konfigurieren
   - Das SDK in Ihrem Code verwenden
2. Ein Beispielprogramm, das AWS SDK für Python (Boto3) nutzt, erstellen und ausführen

Dieses Programm zeigt die derzeit konfigurierten Protokollierungsoptionen des Kontos an. Nachdem Sie das SDK installiert und für Ihr Konto konfiguriert haben, sollten Sie dieses Programm ausführen können.

```
import boto3
import json

# initialize client
iot = boto3.client('iot')

# get current logging levels, format them as JSON, and write them to stdout
response = iot.get_v2_logging_options()
print(json.dumps(response, indent=4))
```

Weitere Informationen zu der in diesem Beispiel verwendeten Funktion finden Sie unter the section called “Konfigurieren Sie die AWS IoT Protokollierung”.

Dokumentation für die AWS IoT Core Dienste, die der AWS SDK für Python (Boto3) unterstützt

- Referenzdokumentation zu IoT
- Referenzdokumentation zu Io TData Plane
- Io TJobs DataPlane Referenzdokumentation
- Referenzdokumentation zu Io TSecure Tunneling

Ruby

So installieren Sie AWS SDK für Ruby und nutzen es zum Herstellen einer Verbindung mit dem AWS IoT:

- Folgen Sie den Anweisungen unter Erste Schritte mit dem AWS SDK für Ruby

  In diesen Anweisungen wird beschrieben, wie Sie:

  - Das SDK installieren
  - Das SDKs konfigurieren
- Das Hello World Tutorial erstellen und ausführen

Dokumentation für die AWS IoT Core Dienste, die das AWS SDK for Ruby unterstützt

- Referenzdokumentation zu Aws::IoT::Client
- Aws: :Io TData Plane: :Client-Referenzdokumentation
- Aws: :Io TJobsDataPlane: :Client-Referenzdokumentation
- Aws: :Io TSecure Tunneling: :Client-Referenzdokumentation

## AWS Mobil SDKs

The AWS Mobile SDKs bietet Entwicklern mobiler Apps plattformspezifischen Support für die APIs AWS IoT Core Dienste, die IoT-Gerätekommunikation mit MQTT und andere Dienste. APIs AWS

Android

AWS Mobile SDK for Android

Das AWS Mobile SDK for Android enthält eine Bibliothek, Beispiele und Dokumentation, mit denen Entwickler vernetzte mobile Anwendungen erstellen können. AWS Dieses SDK bietet auch Unterstützung für die MQTT-Gerätekommunikation und das Aufrufen APIs der AWS IoT Core Dienste. Weitere Informationen finden Sie hier:

- AWS Mobiles SDK for Android auf GitHub
- AWS Readme zum mobilen SDK for Android
- AWS Beispiele für Mobile-SDK SDK for Android
- AWS API-Referenz zum SDK for Android
- AWSIoTClient Dokumentation zur Klassenreferenz

iOS

AWS Mobile SDK for iOS

Das AWS Mobile SDK for iOS ist ein Open-Source-Software-Entwicklungskit, das unter einer Apache Open Source-Lizenz vertrieben wird. Das SDK for iOS bietet eine Bibliothek, Codebeispiele und Dokumentation, mit deren Hilfe Entwickler verbundene mobile Anwendungen erstellen können AWS. Dieses SDK bietet auch Unterstützung für die Kommunikation mit MQTT-Geräten und das Aufrufen APIs der AWS IoT Core Dienste. Weitere Informationen finden Sie hier:

- AWS Mobile SDK for iOS auf GitHub

- AWS Readme zum SDK for iOS
- AWS SDK for iOS iOS-Beispiele
- AWS IoT Referenzdokumente zu Klassen im AWS SDK for iOS

## REST APIs der AWS IoT Core Dienste

Der REST APIs der AWS IoT Core Dienste kann direkt mithilfe von HTTP-Anfragen aufgerufen werden.

- Endpunkt-URL

  Die Dienstendpunkte, die den REST APIs der AWS IoT Core Dienste verfügbar machen, variieren je nach Region und sind unter AWS IoT Core Endpunkte und Kontingente aufgeführt. Sie müssen den Endpunkt für die Region verwenden, in der sich die AWS IoT Ressourcen befinden, auf die Sie zugreifen möchten, da AWS IoT Ressourcen regionsspezifisch sind.
- Authentifizierung

  Die APIs RESTLICHEN AWS IoT Core Dienste verwenden AWS IAM-Anmeldeinformationen für die Authentifizierung. Weitere Informationen finden Sie unter AWS API-Anfragen signieren in der AWS Allgemeinen Referenz.
- API-Referenz

  Informationen zu den spezifischen Funktionen, die vom REST APIs der AWS IoT Core Dienste bereitgestellt werden, finden Sie unter:
  - API-Referenz für das IoT.
  - API-Referenz für IoT-Daten.
  - API-Referenz für IoT–Jobdaten.
  - API-Referenz für IoT Secure Tunneling

# Geräte Connect mit AWS IoT

Geräte stellen eine Verbindung AWS IoT zu anderen Diensten her AWS IoT Core. Über AWS IoT Core: Geräte senden und empfangen Nachrichten über Geräteendpunkte, die für Ihr Konto spezifisch sind. Die the section called “AWS IoT Gerät SDKs” unterstützen die Gerätekommunikation mithilfe der MQTT- und WSS-Protokolle. Weitere Informationen zu von Geräten unterstützten Protokollen finden Sie unter the section called “Gerätekommunikationsprotokolle”.

Der Message Broker

AWS IoT verwaltet die Gerätekommunikation über einen Nachrichtenbroker. Geräte und Kunden veröffentlichen Nachrichten im Message Broker und abonnieren auch Nachrichten, die der Message Broker veröffentlicht. Nachrichten werden durch ein anwendungsdefiniertes Thema identifiziert. Wenn der Message Broker eine Nachricht empfängt, die von einem Gerät oder Kunden veröffentlicht wurde, veröffentlicht er diese Nachricht an die Geräte und Kunden, die das Nachrichtenthema abonniert haben. Der Message Broker leitet Nachrichten auch an die AWS IoT Rules Engine weiter, die auf den Inhalt der Nachricht reagieren kann.

AWS IoT Nachrichtensicherheit

Zu AWS IoT verwendende Geräteverbindungen the section called “X.509-Clientzertifikate” und AWS Signatur V4 für die Authentifizierung. Die Gerätekommunikation ist durch TLS Version 1.3 gesichert und AWS IoT erfordert, dass Geräte bei der Verbindung die Server Name Indication (SNI) - Erweiterung senden. Weitere Informationen finden Sie unter Transportsicherheit in AWS IoT.

## AWS IoT Gerätedaten und Dienstendpunkte

> **Important**
>
> Sie können die Endpunkte auf Ihrem Gerät zwischenspeichern oder speichern. Das bedeutet, dass Sie die `DescribeEndpoint` API nicht jedes Mal abfragen müssen, wenn ein neues Gerät angeschlossen wird. Die Endpunkte ändern sich nicht, nachdem sie für Ihr Konto AWS IoT Core erstellt wurden.

Jedes Konto hat mehrere Geräteendpunkte, die für das Konto einzigartig sind und bestimmte IoT-Funktionen unterstützen. Die AWS IoT Gerätedatenendpunkte unterstützen ein Veröffentlichungs-/Abonnementprotokoll, das für die Kommunikationsanforderungen von IoT-Geräten konzipiert ist. Andere Clients, wie Apps und Dienste, können diese Schnittstelle jedoch auch verwenden, wenn ihre Anwendung die speziellen Funktionen erfordert, die diese Endpunkte bieten. Die AWS IoT Gerätedienst-Endpunkte unterstützen den geräteorientierten Zugriff auf Sicherheits- und Verwaltungsdienste.

Den Gerätedaten-Endpunkt Ihres Accounts finden Sie auf der Einstellungsseite Ihrer Konsole. AWS IoT Core

Um den Geräteendpunkt Ihres Kontos für einen bestimmten Zweck zu ermitteln, einschließlich des Gerätedatenendpunkts, verwenden Sie den hier gezeigten CLI-Befehl describe-endpoint oder

die REST-API `DescribeEndpoint` und geben Sie den Parameterwert *`endpointType`* aus der folgenden Tabelle an.

```
aws iot describe-endpoint --endpoint-type endpointType
```

Dieser Befehl gibt ein *`iot-endpoint`* im folgenden Format zurück:*`account-specific-prefix`*`.iot.`*`aws-region`*`.amazonaws.com`.

Jeder Kunde verfügt über einen `iot:Data-ATS` und einen `iot:Data`-Endpunkt. Jeder Endpunkt verwendet ein X.509-Zertifikat, um den Client zu authentifizieren. Wir empfehlen dringend, dass Kunden den neueren `iot:Data-ATS`-Endpunkttyp verwenden, um Probleme im Zusammenhang mit dem weit verbreiteten Misstrauen gegenüber Symantec-Zertifizierungsstellen zu vermeiden. Wir stellen den `iot:Data` Endpunkt für Geräte bereit, um Daten von alten Endpunkten abzurufen, die VeriSign Zertifikate aus Gründen der Abwärtskompatibilität verwenden. Weitere Informationen finden Sie unter Server-Authentifizierung.

AWS IoT Endpunkte für Geräte

| Zweck des Endpunkts | ***`endpointType`*** Wert | Beschreibung |
|---|---|---|
| AWS IoT Core – Operationen auf Datenebene | `iot:Data-ATS` | Wird zum Senden und Empfangen von Daten an und von den Message Broker-, Geräteschatten- und Regel-Engine-Komponenten von AWS IoT verwendet.<br><br>`iot:Data-ATS` gibt einen ATS-signierten Datenendpunkt zurück |
| AWS IoT Core – Operationen auf Datenebene (veraltet) | `iot:Data` | `iot:Data`gibt einen VeriSign signierten Datenendpunkt zurück, der aus Gründen der Abwärtskompatibilität bereitgestellt wird. MQTT 5 wird auf Symantec (`iot:Data`)-Endpunkten nicht unterstützt. |

| Zweck des Endpunkts | *endpointType* Wert | Beschreibung |
| --- | --- | --- |
| AWS IoT Core Zugriff auf Anmeldeinformationen | `iot:CredentialProvider` | Wird verwendet, um das integrierte X.509-Zertifikat eines Geräts gegen temporäre Anmeldeinformationen auszutauschen, um eine direkte Verbindung mit anderen AWS -Diensten herzustellen. Weitere Informationen zum Herstellen einer Verbindung mit anderen AWS Diensten finden Sie unter Autorisieren von direkten Aufrufen von Diensten. AWS |
| AWS IoT Device Management – Jobdaten-Operationen | `iot:Jobs` | Wird verwendet, um Geräten die Interaktion mit dem AWS IoT Jobs-Dienst über das Jobs-Gerät HTTPS APIs zu ermöglichen. |
| AWS IoT Device Advisor-Operationen | `iot:DeviceAdvisor` | Ein Testendpunkttyp, der zum Testen von Geräten mit Device Advisor verwendet wird. Weitere Informationen finden Sie unter ???. |
| AWS IoT Core Daten-Beta (Vorschau) | `iot:Data-Beta` | Ein Endpunkttyp, der Betaversionen vorbehalten ist. Informationen zu seiner aktuellen Verwendung finden Sie unter ???. |

Sie können auch Ihren eigenen vollqualifizierten Domainnamen (FQDN), z. B.*example.com*, und das zugehörige Serverzertifikat verwenden, mit dem Sie Geräte verbinden AWS IoT . the section called “Domänenkonfigurationen”

# AWS IoT Gerät SDKs

Das AWS IoT Gerät SDKs hilft Ihnen dabei, Ihre IoT-Geräte mit den AWS IoT Core Protokollen MQTT und MQTT über WSS zu verbinden.

Das AWS IoT Gerät SDKs unterscheidet sich von dem AWS SDKs darin, dass das AWS IoT Gerät die speziellen Kommunikationsanforderungen von IoT-Geräten SDKs unterstützt, aber nicht alle von dem unterstützten Dienste unterstützt AWS SDKs. Die AWS IoT Geräte SDKs sind mit denen kompatibel AWS SDKs , die alle AWS Dienste unterstützen. Sie verwenden jedoch unterschiedliche Authentifizierungsmethoden und stellen eine Verbindung zu verschiedenen Endpunkten her, was die Verwendung auf einem IoT-Gerät AWS SDKs unpraktisch machen könnte.

Mobilgeräte

Sie the section called “AWS Mobil SDKs” unterstützen sowohl die MQTT-Gerätekommunikation, einen Teil des AWS IoT Dienstes APIs als auch die APIs anderer Dienste. AWS Wenn Sie auf einem unterstützten Mobilgerät entwickeln, überprüfen Sie dieses SDK, um festzustellen, ob es die beste Option für die Entwicklung Ihrer IoT-Lösung ist.

C++

AWS IoT C++-Geräte-SDK

Das AWS IoT C++-Geräte-SDK ermöglicht es Entwicklern, verbundene Anwendungen mithilfe AWS und APIs der AWS IoT Core Dienste zu erstellen. Dieses SDK wurde speziell für Geräte entwickelt, die nicht ressourcenbeschränkt sind und die erweiterte Funktionen benötigen, wie beispielsweise Nachrichtenwarteschlangen, Multithreading-Support und die aktuellen Sprachfunktionen. Weitere Informationen finden Sie hier:

- AWS IoT Geräte-SDK C++ v2 aktiviert GitHub
- AWS IoT Readme für das Geräte-SDK C++ v2
- AWS IoT C++ v2-Beispiele für das Geräte-SDK
- AWS IoT C++ v2-API-Dokumentation für das Geräte-SDK

Python

AWS IoT Geräte-SDK für Python

Das AWS IoT Device SDK für Python ermöglicht es Entwicklern, Python-Skripte zu schreiben, um ihre Geräte für den Zugriff auf die AWS IoT Plattform über MQTT oder MQTT über das

WebSocket Secure (WSS) -Protokoll zu verwenden. Durch die Verbindung ihrer Geräte mit den APIs AWS IoT Core Diensten können Benutzer sicher mit dem Message Broker, den Regeln und dem Device Shadow-Service arbeiten, AWS IoT Core der sie bereitstellen AWS Lambda, und mit anderen AWS Diensten wie Amazon Kinesis und Amazon S3 und mehr.

- AWS IoT Geräte-SDK für Python v2 auf GitHub
- AWS IoT Readme zum Geräte-SDK für Python v2
- AWS IoT Geräte-SDK für Python v2-Beispiele
- AWS IoT API-Dokumentation zum Geräte-SDK für Python v2

JavaScript

AWS IoT Geräte-SDK für JavaScript

Das AWS IoT Geräte-SDK für JavaScript ermöglicht es Entwicklern, JavaScript Anwendungen zu schreiben, die über das APIs Protokoll auf MQTT oder MQTT zugreifen. AWS IoT Core WebSocket Das Paket kann in Node.js-Umgebungen und Browser-Anwendungen verwendet werden. Weitere Informationen finden Sie hier:

- AWS IoT Geräte-SDK für Version 2 aktiviert JavaScript GitHub
- AWS IoT Readme für das Geräte-SDK JavaScript für Version 2
- AWS IoT Geräte-SDK für JavaScript v2-Beispiele
- AWS IoT Geräte-SDK für JavaScript v2-API-Dokumentation

Java

AWS IoT Geräte-SDK SDK for Java

Das AWS IoT Device SDK for Java ermöglicht es Java-Entwicklern, AWS IoT Core über MQTT oder MQTT über das Protokoll auf das APIs WebSocket of zuzugreifen. Das SDK unterstützt den Geräteschatten-Dienst. Sie können über die HTTP-Methoden wie ABRUFEN, AKTUALISIEREN und LÖSCHEN auf Schattengeräte zugreifen. Das SDK unterstützt auch ein vereinfachtes Zugangsmodell für Schattengeräte, sodass Entwickler mithilfe der Methoden „Getter” und „Setter” Daten mit den Schattengeräten austauschen können, ohne JSON-Dokumente serialisieren oder deserialisieren zu müssen. Weitere Informationen finden Sie hier:

- AWS IoT Geräte-SDK SDK for Java v2 auf GitHub

- AWS IoT Readme zum Geräte-SDK für Java v2
- AWS IoT Geräte-SDK SDK for Java v2-Beispiele
- AWS IoT API-Dokumentation zum Geräte-SDK für Java v2

Embedded C

AWS IoT Geräte-SDK für Embedded C

> **Important**
>
> Dieses SDK ist für die Verwendung durch erfahrene Entwickler eingebetteter Software vorgesehen.

Das AWS IoT Device SDK for Embedded C (C-SDK) ist eine Sammlung von C-Quelldateien unter der MIT-Open-Source-Lizenz, die in eingebetteten Anwendungen verwendet werden können, um IoT-Geräte sicher mit AWS IoT Core zu verbinden. Es umfasst MQTT-, JSON Parser- und AWS IoT Device Shadow-Bibliotheken und andere. Es wird als Quellcode verteilt und soll zusammen mit einem Anwendungscode, anderen Bibliotheken und optional einem RTOS (Real Time Operating System) in die Kunden-Firmware integriert werden.

Das AWS IoT Device SDK for Embedded C richtet sich im Allgemeinen an Geräte mit eingeschränkten Ressourcen, die eine optimierte Laufzeit in C-Sprache benötigen. Sie können das SDK auf jedem Betriebssystem verwenden und es auf jedem Prozessortyp hosten (z. B. MCUs und MPUs). Wenn auf Ihrem Gerät genügend Speicher- und Verarbeitungsressourcen verfügbar sind, empfehlen wir Ihnen, eines der anderen AWS IoT Geräte- und Mobilgeräte zu verwenden SDKs, z. B. das AWS IoT Geräte-SDK SDK for C++ JavaScript, Java oder Python.

Weitere Informationen finden Sie hier:

- AWS IoT Geräte-SDK für Embedded C auf GitHub
- AWS IoT Readme-Datei zum Geräte-SDK für Embedded C
- AWS IoT Geräte-SDK für eingebettete C-Beispiele

## Gerätekommunikationsprotokolle

AWS IoT Core unterstützt Geräte und Clients, die die Protokolle MQTT und MQTT over WebSocket Secure (WSS) verwenden, um Nachrichten zu veröffentlichen und zu abonnieren, sowie Geräte und Clients, die das HTTPS-Protokoll zum Veröffentlichen von Nachrichten verwenden. Alle Protokolle unterstützen IPv4 und. IPv6 In diesem Abschnitt werden die verschiedenen Verbindungsoptionen für Geräte und Kunden beschrieben.

## Versionen des TLS-Protokolls

AWS IoT Core verwendet TLS Version 1.2 und TLS Version 1.3, um die gesamte Kommunikation zu verschlüsseln. Sie können zusätzliche TLS-Richtlinienversionen für Ihren Endpunkt konfigurieren, indem Sie die TLS-Einstellungen in den Domänenkonfigurationen konfigurieren. Beim Verbinden von Geräten mit können Clients die Server Name Indication (SNI) -Erweiterung senden, die für Funktionen wie die Registrierung mehrerer Konten, konfigurierbare Endpunkte, benutzerdefinierte Domänen und VPC-Endpunkte erforderlich ist. AWS IoT Core Weitere Informationen finden Sie unter Transportsicherheit in AWS IoT.

AWS IoT Gerät SDKs unterstützen MQTT und MQTT over WSS und unterstützen die Sicherheitsanforderungen von Client-Verbindungen. Wir empfehlen die Verwendung von AWS IoT Gerät SDKs, um Clients mit dem AWS IoT zu verbinden.

## Protokolle, Port-Zuweisungen und Authentifizierung

Wie ein Gerät oder ein Client eine Verbindung zum Message Broker herstellt, kann mithilfe eines Authentifizierungstyps konfiguriert werden. Standardmäßig oder wenn keine SNI-Erweiterung gesendet wird, basiert die Authentifizierungsmethode auf dem Anwendungsprotokoll, dem Port und der TLS-Erweiterung Application Layer Protocol Negotiation (ALPN), die Geräte verwenden. In der folgenden Tabelle ist die erwartete Authentifizierung auf der Grundlage von Port, Port und ALPN aufgeführt.

Protokolle, Authentifizierung und Port-Zuweisungen

| Protokoll | Unterstützte Operationen | Authentifizierung | Port | ALPN-Protokollname |
|---|---|---|---|---|
| MQTT über WebSocket | Veröffentlichen, Abonnieren | Signaturversion 4 | 443 | N/A |
| MQTT vorbei WebSocket | Veröffentlichen, Abonnieren | Benutzerdefinierte Authentifizierung | 443 | N/A |

| Protokoll | Unterstützte Operationen | Authentifizierung | Port | ALPN-Protokollname |
|---|---|---|---|---|
| MQTT | Veröffentlichen, Abonnieren | X.509-Clientzertifikat | 443† | `x-amzn-mqtt-ca` |
| MQTT | Veröffentlichen, Abonnieren | X.509-Clientzertifikat | 8883 | N/A |
| MQTT | Veröffentlichen, Abonnieren | Benutzerdefinierte Authentifizierung | 443† | `mqtt` |
| HTTPS | Nur veröffentlichen | Signaturversion 4 | 443 | N/A |
| HTTPS | Nur veröffentlichen | X.509-Clientzertifikat | 443† | `x-amzn-http-ca` |
| HTTPS | Nur veröffentlichen | X.509-Clientzertifikat | 8443 | N/A |
| HTTPS | Nur veröffentlichen | Benutzerdefinierte Authentifizierung | 443 | N/A |

ALPN (Application Layer Protocol Negotiation)

† Bei Verwendung von Standard-Endpunktkonfigurationen müssen Clients, die sich über Port 443 mit X.509-Client-Zertifikatsauthentifizierung verbinden, die TLS-Erweiterung Application Layer Protocol Negotiation (ALPN) implementieren und den ALPN-Protokollnamen verwenden, der in der vom Client ProtocolNameList gesendeten ALPN als Teil der Nachricht aufgeführt ist. `ClientHello`
Auf Port 443 unterstützt der IoT:Data-ATS-Endpunkt x-amzn-http-ca ALPN-HTTP, der IoT:Jobs-Endpunkt jedoch nicht.
Auf Port 8443 HTTPS und Port 443 MQTT mit ALPN kann die benutzerdefinierte Authentifizierung nicht verwendet werden. x-amzn-mqtt-ca

Clients stellen eine Verbindung zu ihren Geräteendpunkten AWS-Konto her. Informationen darüber, wie Sie die Geräteendpunkte Ihres Kontos finden, finden Sie unter the section called “AWS IoT Gerätedaten und Dienstendpunkte”.

> **Note**
>
> AWS SDKs benötigen nicht die gesamte URL. Sie benötigen nur den Endpunkt-Hostnamen, z. B. das `pubsub.py`Beispiel für AWS IoT Device SDK for Python on GitHub. Wenn Sie die gesamte URL wie in der folgenden Tabelle aufgeführt übergeben, kann dies zu einem Fehler wie einem ungültigen Hostnamen führen.

Verbindung herstellen zu AWS IoT Core

| Protokoll | Endpunkt oder URL |
|---|---|
| MQTT | *iot-endpoint* |
| MQTT over WSS | wss://*iot-endpoint* /mqtt |
| HTTPS | https://*iot-endpoint* /topics |

## Wählen Sie ein Anwendungsprotokoll für die Kommunikation mit Ihrem Gerät

Für den Großteil der IoT-Gerätekommunikation über die Geräteendpunkte sollten Sie die Protokolle Secure MQTT oder MQTT over WebSocket Secure (WSS) verwenden. Die Geräteendpunkte unterstützen jedoch auch HTTPS.

In der folgenden Tabelle wird verglichen, wie die beiden High-Level-Protokolle (MQTT und HTTPS) für die Gerätekommunikation AWS IoT Core verwendet werden.

AWS IoT Geräteprotokolle (MQTT und HTTPS) side-by-side

| Funktion | MQTT | HTTPS |
|---|---|---|
| Unterstützung von Veröffentlichen/Abonnieren | Veröffentlichen und Abonnieren | Nur veröffentlichen |

| Funktion | MQTT | HTTPS |
| --- | --- | --- |
| SDK-Unterstützung | AWS Geräte SDKs unterstützen die Protokolle MQTT und WSS | Keine SDK-Unterstützung, aber Sie können sprachspezifische Methoden verwenden, um HTTPS-Anfragen zu stellen |
| Qualität der Service-Unterstützung | MQTT QoS Stufen 0 und 1 | QoS wird durch die Übergabe eines Abfragezeichenfolge-Parameter `?qos=qos` unterstütz, dessen Wert 0 oder 1 sein kann. Sie können diese Abfragezeichenfolge hinzufügen, um eine Nachricht mit dem gewünschten QoS-Wert zu veröffentlichen. |
| Können empfangene Nachrichten verpasst werden, während das Gerät offline war | Ja | Nein |
| Unterstützung von `clientId`-Feldern | Ja | Nein |
| Erkennung von Geräteunterbrechungen | Ja | Nein |
| Sichere Kommunikationen | Ja. Siehe ??? | Ja. Siehe ??? |
| Themendefinitionen | Anwendung definiert | Anwendung definiert |
| Format der Nachrichtendaten | Anwendung definiert | Anwendung definiert |
| Protokoll-Overhead | Niedriger | Höher |
| Stromverbrauch | Niedriger | Höher |

## Wählen Sie einen Authentifizierungstyp für Ihre Gerätekommunikation

Sie können den Authentifizierungstyp für Ihren IoT-Endpunkt mithilfe konfigurierbarer Endpunkte konfigurieren. Verwenden Sie alternativ die Standardkonfiguration und legen Sie fest, wie sich Ihre Geräte mit der Kombination aus Anwendungsprotokoll, Port und ALPN TLS-Erweiterung authentifizieren. Der von Ihnen gewählte Authentifizierungstyp bestimmt, wie sich Ihre Geräte authentifizieren, wenn sie eine Verbindung herstellen. AWS IoT Core Es gibt fünf Authentifizierungstypen:

X.509-Zertifikat enthalten

Authentifizieren Sie Geräte mithilfe von X.509-Client-Zertifikaten, wodurch die Authentifizierung des AWS IoT Core Geräts bestätigt wird. Dieser Authentifizierungstyp funktioniert mit den Protokollen Secure MQTT (MQTT over TLS) und HTTPS.

X.509-Zertifikat mit benutzerdefiniertem Authorizer

Authentifizieren Sie Geräte mithilfe von X.509-Client-Zertifikaten und führen Sie zusätzliche Authentifizierungsaktionen mit einem benutzerdefinierten Authorizer durch, der X.509-Client-Zertifikatsinformationen empfängt. Dieser Authentifizierungstyp funktioniert mit den Protokollen Secure MQTT (MQTT over TLS) und HTTPS. Dieser Authentifizierungstyp ist nur mit konfigurierbaren Endpunkten mit benutzerdefinierter X.509-Authentifizierung möglich. Es gibt keine ALPN-Option.

AWS Signatur Version 4 (SigV4)

Authentifizieren Sie Geräte mit Cognito oder Ihrem Backend-Service und unterstützen Sie so den Verbund von sozialen Netzwerken und Unternehmen. Dieser Authentifizierungstyp funktioniert mit den Protokollen MQTT over WebSocket Secure (WSS) und HTTPS.

Benutzerdefinierter Autorisierer

Authentifizieren Sie Geräte, indem Sie eine Lambda-Funktion konfigurieren, um benutzerdefinierte Authentifizierungsinformationen zu verarbeiten, an die gesendet werden. AWS IoT Core Dieser Authentifizierungstyp funktioniert mit den Protokollen Secure MQTT (MQTT over TLS), HTTPS und MQTT over WebSocket Secure (WSS).

Standard

Authentifizieren Sie Geräte auf der Grundlage der Port- und/oder ALPN-Erweiterung (Application Layer Protocol Negotiation), die die Geräte verwenden. Einige zusätzliche Authentifizierungsoptionen werden nicht unterstützt. Weitere Informationen finden Sie unter ???.

Die folgende Tabelle zeigt alle unterstützten Kombinationen von Authentifizierungstypen und Anwendungsprotokollen.

Unterstützte Kombinationen von Authentifizierungstypen und Anwendungsprotokollen

| Authentifizierungstyp | Sicheres MQTT (MQTT über TLS) | MQTT über WebSocket Secure (WSS) | HTTPS | Standard |
|---|---|---|---|---|
| X.509-Zertifikat enthalten | ✓ | | ✓ | |
| X.509-Zertifikat mit benutzerdefiniertem Authorizer | ✓ | | ✓ | |
| AWS Signatur Version 4 (Sigv4) | | ✓ | ✓ | |
| Benutzerdefinierter Autorisierer | ✓ | ✓ | ✓ | |
| Standard | ✓ | | | ✓ |

## Einschränkungen der Verbindungsdauer

Es kann nicht garantiert werden, dass HTTPS-Verbindungen länger dauern als die Zeit, die für den Empfang und die Beantwortung von Anfragen benötigt wird.

Die Dauer der MQTT-Verbindung ist von der Authentifizierungsfunktion abhängig, die Sie verwenden. In der folgenden Tabelle ist die maximale Verbindungsdauer unter idealen Bedingungen für jede Funktion aufgeführt.

MQTT-Verbindungsdauer nach Authentifizierungsfunktion

| Funktion | Maximale Dauer * |
|---|---|
| X.509-Clientzertifikat | 1 bis 2 Wochen |

| Funktion | Maximale Dauer * |
| --- | --- |
| Benutzerdefinierte Authentifizierung | 1 bis 2 Wochen |
| Signaturversion 4 | Bis zu 24 Stunden |

* Nicht garantiert

Mit X.509-Zertifikaten und benutzerdefinierter Authentifizierung gibt es keine feste Grenze für die Verbindungsdauer, sie kann jedoch auch nur wenige Minuten lang sein. Verbindungsunterbrechungen können aus verschiedenen Gründen auftreten. Die folgende Liste enthält einige der gängigsten Gründe.

- Unterbrechungen der Wi-Fi-Verfügbarkeit
- Verbindungsunterbrechungen des Internetdienstanbieters (ISP)
- Service-Patches
- Dienstbereitstellungen
- Service Auto Scaling
- Nicht verfügbarer Dienst-Host
- Load Balancer-Probleme und -Aktualisierungen
- Client-seitige Fehler

Ihre Geräte müssen Strategien zur Erkennung von Verbindungsabbrüchen und zur Wiederherstellung der Verbindung implementieren. Informationen zu Trennungsereignissen und Anleitungen, wie Sie damit umgehen können, finden Sie in ??? unter ???.

## MQTT

MQTT (Message Queuing Telemetry Transport) ist ein einfaches, weit verbreitetes Messaging-Protokoll, das für eingeschränkte Geräte konzipiert ist. AWS IoT Core Unterstützung für MQTT basiert auf der MQTT-Spezifikation v3.1.1 und v5.0, mit einigen Unterschieden, wie in the section called “AWS IoT Unterschiede zu den MQTT-Spezifikationen” dokumentiert. MQTT 5, die neueste Version des Standards, führt mehrere wichtige Funktionen ein, die ein MQTT-basiertes System robuster machen. Dazu gehören Verbesserungen der Skalierbarkeit, eine verbesserte Fehlerberichterstattung mit Reason-Code-Antworten, Timer für den Ablauf von Meldungen und Sitzungen sowie benutzerdefinierte Header für Benutzermeldungen. Weitere Informationen zu den

Funktionen, die MQTT 5 AWS IoT Core unterstützen, finden Sie unter Von MQTT 5 unterstützte Funktionen. AWS IoT Core unterstützt auch die Kommunikation zwischen MQTT-Versionen (MQTT 3 und MQTT 5). Ein MQTT-3-Publisher kann eine MQTT-3-Meldung an einen MQTT-5-Subscriber senden, der eine MQTT-5-Publish-Meldung erhält, und umgekehrt.

AWS IoT Core unterstützt Geräteverbindungen, die das MQTT-Protokoll und das MQTT-over-WSS-Protokoll verwenden und die durch eine Client-ID identifiziert werden. AWS IoT Gerät SDKs unterstützen beide Protokolle und sind die empfohlenen Verbindungsmethoden für Geräte zu AWS IoT Core Das AWS IoT Gerät SDKs unterstützt die Funktionen, die Geräte und Clients benötigen, um sich mit Diensten zu verbinden und auf sie zuzugreifen AWS IoT . Das Gerät SDKs unterstützt die Authentifizierungsprotokolle, die für die AWS IoT Dienste erforderlich sind, und die Verbindungs-ID-Anforderungen, die für das MQTT-Protokoll und die Protokolle MQTT over WSS erforderlich sind. Informationen darüber, wie Sie AWS IoT mithilfe des AWS Geräts eine Verbindung herstellen können, SDKs sowie Links zu Beispielen AWS IoT in den unterstützten Sprachen finden Sie unter. the section called “Über das Gerät eine Verbindung mit MQTT herstellen AWS IoT SDKs” Weitere Informationen zu Authentifizierung und Portzuordnungen für MQTT-Meldungen unter ???.

Wir empfehlen zwar, das AWS IoT Gerät SDKs für die Verbindung zu verwenden AWS IoT, sie sind jedoch nicht erforderlich. Wenn Sie das AWS IoT Gerät jedoch nicht verwenden SDKs, müssen Sie für die erforderliche Verbindungs- und Kommunikationssicherheit sorgen. Clients müssen auch die Server Name Indication (SNI)-TLS-Erweiterung in der Verbindungsanforderung senden. Verbindungsversuche, die das SNI nicht enthalten, werden abgelehnt. Weitere Informationen finden Sie unter Transportsicherheit in AWS IoT. Clients, die IAM-Benutzer und AWS Anmeldeinformationen zur Authentifizierung von Clients verwenden, müssen die richtige Signature Version 4-Authentifizierung bereitstellen.

In diesem Thema:


- Über das Gerät eine Verbindung mit MQTT herstellen AWS IoT SDKs
- MQTT QoS-(Quality of Service)-Optionen
- Persistente MQTT-Sitzungen
- Beibehaltene MQTT-Meldungen
- MQTT-Meldungen des letzten Willens und Testaments (LWT)
- ConnectAttributes verwenden
- Von MQTT 5 unterstützte Funktionen
- MQTT 5 Eigenschaften
- MQTT-Ursachencodes

- AWS IoT Unterschiede zu den MQTT-Spezifikationen

Über das Gerät eine Verbindung mit MQTT herstellen AWS IoT SDKs

Dieser Abschnitt enthält Links zum AWS IoT Gerät SDKs und zum Quellcode von Beispielprogrammen, die veranschaulichen, wie ein Gerät angeschlossen AWS IoT wird. Die hier verlinkten Beispiel-Apps zeigen, wie Sie AWS IoT mithilfe des MQTT-Protokolls und MQTT über WSS eine Verbindung herstellen können.

> **Note**
>
> Das AWS IoT Gerät SDKs hat einen MQTT 5-Client veröffentlicht.

C++

Verwenden des AWS IoT C++-Geräte-SDK zum Verbinden von Geräten

- Quellcode einer App, als Beispiel für eine MQTT-Verbindung in C++
- AWS IoT Geräte-SDK SDK for C++ v2 auf GitHub

Python

Geräte mit dem AWS IoT Device SDK für Python verbinden

- Quellcode einer App, als Beispiel für eine MQTT-Verbindung in Python
- AWS IoT Geräte-SDK v2 für Python auf GitHub

JavaScript

Verwenden des AWS IoT Geräte-SDK JavaScript zum Verbinden von Geräten

- Quellcode einer Beispiel-App, die ein Beispiel für eine MQTT-Verbindung in zeigt JavaScript
- AWS IoT Geräte-SDK für JavaScript v2 auf GitHub

Java

Geräte mit dem AWS IoT Device SDK for Java verbinden

> **Note**
>
> Das AWS IoT Device SDK for Java v2 unterstützt jetzt die Android-Entwicklung. Weitere Informationen finden Sie unter AWS IoT Geräte-SDK SDK for Android.

- Quellcode einer App, die ein Beispiel für eine MQTT-Verbindung in Java zeigt
- AWS IoT Geräte-SDK SDK for Java v2 auf GitHub

Embedded C

Verwenden Sie das AWS IoT Geräte-SDK für Embedded C, um Geräte zu verbinden

> **Important**
>
> Dieses SDK ist für die Verwendung durch erfahrene Entwickler eingebetteter Software vorgesehen.

- Quellcode einer App, die ein Beispiel für eine MQTT-Verbindung in Embedded C zeigt
- AWS IoT Geräte-SDK für Embedded C aktiviert GitHub

MQTT QoS-(Quality of Service)-Optionen

AWS IoT und das AWS IoT Gerät SDKs unterstützt die MQTT-Qualitätsstufen 0 (QoS) und. 1 Das MQTT-Protokoll definiert eine dritte Ebene von QoS, Ebene2, unterstützt AWS IoT diese jedoch nicht. Nur das MQTT-Protokoll unterstützt die QoS-Funktion. HTTPS unterstützt QoS, indem es einen Abfragezeichenfolge-Parameter `?qos=qos` übergibt, sein Wert kann 0 oder 1 sein.

Die Tabelle beschreibt, wie sich jede QoS-Stufe auf Meldungen auswirkt, die an und von Message Broker veröffentlicht werden.

| Mit einem QoS-Level von ... | Die Meldung ist … | Kommentare |
|---|---|---|
| QoS Stufe 0 | Null oder mehr Mal gesendet | Diese Stufe sollte für Meldungen verwendet |

| Mit einem QoS-Level von ... | Die Meldung ist … | Kommentare |
| --- | --- | --- |
| | | werden, die über zuverlässige Kommunikationsverbindungen gesendet werden oder die problemlos übersehen werden können. |
| QoS Stufe 1 | Mindestens einmal gesendet und dann wiederholt, bis eine PUBACK Antwort eingeht. | Die Meldung gilt erst dann als vollständig, wenn der Absender eine PUBACK Antwort erhält, die auf eine erfolgreiche Zustellung hinweist. |

Persistente MQTT-Sitzungen

Persistente Sitzungen speichern Abonnements und Meldungen eines Kunden mit einer Quality of Service (QoS) von 1, sofern diese nicht vom Kunden bestätigt wurden. Wenn das Gerät wieder eine Verbindung zu einer dauerhaften Sitzung herstellt, wird die Sitzung wieder aufgenommen, Abonnements werden wieder hergestellt und unbestätigte abonnierte Meldungen, die vor der Wiederverbindung empfangen und gespeichert wurden, werden an den Client gesendet.

Die Verarbeitung der gespeicherten Nachrichten wird in CloudWatch Logs aufgezeichnet. CloudWatch Informationen zu den in Logs geschriebenen Einträgen CloudWatch und CloudWatch Logs finden Sie unter Message Broker-Metriken undProtokolleintrag in der Warteschlange.

Erstellen einer persistenten Sitzung

Erstellen Sie in MQTT 3 eine persistente MQTT-Sitzung, indem Sie eine `CONNECT`Meldung versenden und das `cleanSession` Flag auf `0` festlegen. Wenn für den Client, der die `CONNECT`-Meldung versendet, keine Sitzung vorhanden ist, wird eine neue persistente Sitzung erstellt. Wenn für den Client bereits eine Sitzung existiert, nimmt der Client die bestehende Sitzung wieder auf. Um eine saubere Sitzung zu erstellen, senden Sie eine `CONNECT` Meldung und setzen das `cleanSession` Flag auf 1. Der Broker speichert dann keinen Sitzungsstatus, wenn der Client die Verbindung trennt.

In MQTT 5 behandeln Sie persistente Sitzungen, indem Sie das `Clean Start` Flag und `Session Expiry Interval` festlegen. Clean Start steuert den Beginn der Verbindungssitzung und das Ende

der vorherigen Sitzung. Wenn Sie `Clean Start` = `1` setzen, wird eine neue Sitzung erstellt und eine vorherige Sitzung wird beendet, falls sie existiert. Wenn Sie `Clean Start` = `0` setzen, nimmt die Verbindungssitzung eine vorherige Sitzung wieder auf, falls sie existiert. Das Sitzungsablaufintervall bestimmt das Ende der Verbindungssitzung. Das Sitzungsablaufintervall gibt die Zeit in Sekunden (4-Byte-Ganzzahl) an, für die eine Sitzung nach der Trennung bestehen bleibt. Einstellung `Session Expiry interval` = `0` bewirkt, dass die Sitzung sofort nach der Trennung beendet wird. Wenn das Sitzungsablaufintervall nicht in der CONNECT-Meldung angegeben ist, ist der Standardwert 0.

MQTT 5 Clean Start und Ablauf der Sitzung

| Eigenschaftenwert | Beschreibung |
|---|---|
| `Clean Start= 1` | Erzeugt eine neue Sitzung und beendet eine vorherige Sitzung, falls eine existiert. |
| `Clean Start= 0` | Nimmt eine Sitzung wieder auf, falls eine vorherige Sitzung existiert . |
| `Session Expiry Interval> 0` | Hält eine Sitzung aufrecht. |
| `Session Expiry interval= 0` | Behält eine Sitzung nicht bei. |

Wenn Sie in MQTT 5 `Clean Start` = `1` und `Session Expiry Interval` = `0` setzen, entspricht dies einer sauberen MQTT-3-Sitzung. Wenn Sie `Clean Start` = `0` und `Session Expiry Interval` >`0` setzen, entspricht dies einer persistenten MQTT-3-Sitzung.

> **Note**
>
> MQTT-übergreifende (MQTT 3 und MQTT 5) persistente Sitzungen werden nicht unterstützt. Eine persistente MQTT 3-Sitzung kann nicht als MQTT 5-Sitzung wieder aufgenommen werden und umgekehrt.

Operationen während einer persistenten Sitzung

Clients müssen das `sessionPresent`-Attribut in der Connection Acknowledged (`CONNACK`)-Meldung nutzen, um festzustellen, ob eine persistente Sitzung vorhanden ist. Wenn

`sessionPresent` auf 1 gesetzt ist, liegt eine persistente Sitzung vor und alle gespeicherten Meldungen für den Client werden an den Client zugestellt, nachdem der Client `CONNACK` empfangen hat, wie unter Meldungsverkehr nach Wiederverbindung mit einer persistenten Sitzung beschrieben. Wenn `sessionPresent` auf 1 gesetzt ist, muss der Client kein erneutes Abonnement abschließen. Wenn `sessionPresent` auf `0` gesetzt ist, ist keine persistente Sitzung vorhanden, und der Client muss die Themenfilter erneut abonnieren.

Nachdem der Client der persistenten Sitzung beigetreten ist, kann er weiterhin Meldungen veröffentlichen und Themenfilter ohne zusätzliche Flags für jede Maßnahme abonnieren.

Meldungsverkehr nach Wiederverbindung zu einer persistenten Sitzung

Eine persistente Sitzung stellt eine fortlaufende Verbindung zwischen einem Client und einem MQTT-Message Broker dar. Wenn ein Client eine Verbindung mit dem Message Broker über eine persistente Sitzung herstellt, speichert der Message Broker alle Abonnements, die der Client während der Verbindung erstellt. Wenn der Client getrennt wird, speichert der Message Broker unbestätigte QoS 1-Meldungen und neue QoS 1-Meldungen, die zu Themen veröffentlicht wurden, die der Client abonniert hat. Meldungen werden gemäß dem Kontolimit gespeichert. Meldungen, die das Limit überschreiten werden gelöscht. Weitere Informationen zu persistenten Nachrichtenlimits finden Sie unter AWS IoT Core Endpunkte und Kontingente. Wenn der Client die Verbindung zur persistenten Sitzung wiederherstellt, werden alle Abonnements reaktiviert und alle gespeicherten Meldungen werden bei einer maximalen Rate von 10 Meldungen pro Sekunde an den Client gesendet. Wenn in MQTT 5 eine ausgehende QoS1-Verbindung mit dem Meldungsablaufintervall abläuft, während ein Client offline ist, empfängt der Client nach der Wiederaufnahme der Verbindung die abgelaufene Meldung nicht.

Nach der Wiederverbindung werden die gespeicherten Meldungen an den Client gesendet, und zwar mit einer Geschwindigkeit, die auf 10 gespeicherte Meldungen pro Sekunde begrenzt ist, zusammen mit dem aktuellen Meldungsverkehr, bis das `Publish requests per second per connection`-Limit erreicht ist. Da die Zustellungsrate der gespeicherten Meldungen begrenzt ist, dauert es mehrere Sekunden, bis alle gespeicherten Meldungen zugestellt werden, wenn in einer Sitzung nach der Wiederverbindung mehr als 10 gespeicherte Meldungen zugestellt werden müssen.

Eine persistente Sitzung wird beendet.

Dauerhafte Sitzungen können wie folgt enden:

- Die Ablaufzeit der persistenten Sitzung ist abgelaufen. Der Timer für den Ablauf einer persistenten Sitzung wird gestartet, wenn der Message Broker feststellt, dass ein Client die Verbindung getrennt

hat, entweder weil der Client die Verbindung getrennt hat oder weil die Verbindung das Timeout überschritten hat.

- Der Client sendet eine `CONNECT` Nachricht, die das `cleanSession` Flag auf 1 setzt.

In MQTT 3 ist der Standardwert für die Ablaufzeit persistenter Sitzungen eine Stunde, und dies gilt für alle Sitzungen im Konto.

In MQTT 5 können Sie das Sitzungsablaufintervall für jede Sitzung in den Paketen CONNECT und DISCONNECT festlegen.

Für das Sitzungsablaufintervall für das DISCONNECT-Paket:

- Wenn die aktuelle Sitzung ein Sitzungsablaufintervall von 0 hat, können Sie das Sitzungsablaufintervall für das DISCONNECT-Paket nicht auf einen Wert über 0 setzen.
- Wenn die aktuelle Sitzung ein Sitzungsablaufintervall von mehr als 0 hat und Sie das Sitzungsablaufintervall im DISCONNECT-Paket auf 0 setzen, wird die Sitzung auf DISCONNECT beendet.
- Andernfalls aktualisiert das Sitzungsablaufintervall für das DISCONNECT-Paket das Sitzungsablaufintervall der aktuellen Sitzung.

> **Note**
>
> Die gespeicherten Meldungen, die darauf warten, am Ende einer Sitzung an den Client gesendet zu werden, werden verworfen. Sie werden jedoch weiterhin zum Standardnachrichtentarif in Rechnung gestellt, obwohl sie nicht gesendet werden konnten. Weitere Informationen zu Preisen erhalten Sie unter AWS IoT Core Preise. Sie können das Ablaufzeitintervall konfigurieren.

Wiederverbindung nach Ablauf einer persistenten Sitzung

Wenn ein Client vor Ablauf nicht wieder eine Verbindung zu seiner persistenten Sitzung herstellt, wird die Sitzung beendet und die gespeicherten Meldungen werden verworfen. Wenn ein Client nach Ablauf der Sitzung wieder eine Verbindung herstellt und das `cleanSession`-Flag auf `0` setzt, erstellt der Dienst eine neue persistente Sitzung. Alle Abonnements oder Meldungen aus der vorherigen Sitzung sind für diese Sitzung nicht verfügbar, da sie beim Ablauf der vorherigen Sitzung verworfen wurden.

Gebühren für Meldungen während einer dauerhaften Sitzung

Nachrichten werden Ihnen in Rechnung gestellt, AWS-Konto wenn der Message Broker eine Nachricht an einen Client oder eine persistente Offline-Sitzung sendet. Wenn ein Offline-Gerät mit einer dauerhaften Sitzung erneut eine Verbindung herstellt und seine Sitzung wieder aufnimmt, werden die gespeicherten Meldungen an das Gerät übermittelt und Ihrem Konto erneut belastet. Weitere Informationen zu den Preisen für Meldungen finden Sie unter AWS IoT Core Preise – Meldungsübermittlung.

Die standardmäßige Ablaufzeit einer persistenten Sitzung von einer Stunde kann erhöht werden, indem das standardmäßige Verfahren zum Erhöhen von Limits verwendet wird. Beachten Sie, dass durch eine Verlängerung der Sitzungsablaufzeit Ihre Meldungsgebühren steigen können, da durch die zusätzliche Zeit mehr Meldungen für das Offline-Gerät gespeichert werden können und diese zusätzlichen Meldungen Ihrem Konto zum Standardnachrichtentarif in Rechnung gestellt würden. Bei der Ablaufzeit der Sitzung handelt es sich um einen ungefähren Wert, und eine Sitzung kann bis zu 30 Minuten länger als das Kontolimit andauern. Eine Sitzung darf das Kontolimit jedoch nicht unterschreiten. Weitere Informationen zu Sitzungslimits finden Sie unter AWS -Service Quotas.

Beibehaltene MQTT-Meldungen

AWS IoT Core unterstützt das im MQTT-Protokoll beschriebene RETAIN-Flag. Wenn ein Client das RETAIN-Flag für eine von ihm veröffentlichte MQTT-Nachricht setzt, wird die Nachricht AWS IoT Core gespeichert. Sie kann dann an neue Abonnenten gesendet, durch Aufrufen des `GetRetainedMessage`Vorgangs abgerufen und in der AWS IoT Konsole angezeigt werden.

Beispiele für die Verwendung von gespeicherten MQTT-Meldungen

- Als erste Konfigurationsnachricht

  In MQTT gespeicherte Meldungen werden an einen Client gesendet, nachdem der Client ein Thema abonniert hat. Wenn Sie möchten, dass alle Clients, die ein Thema abonnieren, die beibehaltene MQTT-Nachricht direkt nach ihrem Abonnement erhalten, können Sie eine Konfigurationsnachricht veröffentlichen, bei der das RETAIN-Flag gesetzt ist. Abonnierende Clients erhalten außerdem Updates für diese Konfiguration, wenn eine neue Konfigurationsnachricht veröffentlicht wird.
- Als letzte bekannte Zustandsmeldung

  Geräte können das RETAIN-Flag für Meldungen mit aktuellem Status setzen, sodass AWS IoT Core sie speichern werden. Wenn Anwendungen eine Verbindung herstellen oder erneut eine Verbindung herstellen, können sie dieses Thema abonnieren und den zuletzt gemeldeten Status

direkt nach dem Abonnieren des beibehaltenen Nachrichtenthemas abrufen. Auf diese Weise können sie vermeiden, dass sie bis zur nächsten Meldung vom Gerät warten müssen, um den aktuellen Status zu sehen.

In diesem Abschnitt:


- Häufige Aufgaben mit MQTT-Aufbewahrungsnachrichten in AWS IoT Core
- Abrechnung und gespeicherte Meldungen
- Vergleich von beibehaltenen MQTT-Meldungen und persistenten MQTT-Sitzungen
- In MQTT gespeicherte Nachrichten und Device Shadows AWS IoT


## Häufige Aufgaben mit MQTT-Aufbewahrungsnachrichten in AWS IoT Core

AWS IoT Core speichert MQTT-Nachrichten mit gesetztem RETAIN-Flag. Diese gespeicherten Meldungen werden als normale MQTT-Meldung an alle Clients gesendet, die das Thema abonniert haben, und sie werden auch gespeichert, um an neue Abonnenten des Themas gesendet zu werden.

Archivierte MQTT-Meldungen erfordern spezifische Richtlinienaktionen, um Clients den Zugriff auf sie zu autorisieren. Beispiele für die Verwendung von Richtlinien für gespeicherte Meldungen finden Sie unter Beispielrichtlinien für beibehaltene Nachrichten.

In diesem Abschnitt werden allgemeine Vorgänge beschrieben, bei denen gespeicherte Meldungen verwendet werden.

- Erstellen einer beibehaltenen Nachricht

  Der Client bestimmt, ob eine Meldung beibehalten wird, wenn er eine MQTT-Meldung veröffentlicht. Clients können das RETAIN-Flag setzen, wenn sie eine Meldung veröffentlichen, indem sie ein Device SDK verwenden. Anwendungen und Dienste können das RETAIN-Flag setzen, wenn sie die `PublishAktion` zum Veröffentlichen einer MQTT-Meldung verwenden.

  Pro Themenname wird nur eine Meldung beibehalten. Eine neue Meldung mit gesetztem RETAIN-Flag, die zu einem Thema veröffentlicht wurde, ersetzt alle vorhandenen beibehaltenen Meldungen, die zuvor an das Thema gesendet wurden.

  HINWEIS: Sie können nicht zu einem reservierten Thema veröffentlichen, wenn das RETAIN-Flag gesetzt ist.

- Abonnieren eines beibehaltenen Meldungsthemas

Kunden abonnieren Themen für beibehaltene Meldungen wie jedes andere MQTT-Meldungsthema. Bei gespeicherten Meldungen, die durch das Abonnieren eines gespeicherten Meldungsthemas empfangen wurden, ist das RETAIN-Flag gesetzt.

Aufbewahrte Nachrichten werden gelöscht, AWS IoT Core sobald ein Client eine beibehaltene Nachricht mit einer 0-Byte-Nachrichtennutzlast im Thema der beibehaltenen Nachricht veröffentlicht. Clients, die das beibehaltene Meldungsthema abonniert haben, erhalten auch die 0-Byte-Nachricht.

Wenn Sie einen Wildcard-Themenfilter abonnieren, der ein aufbewahrtes Meldungsthema enthält, kann der Client nachfolgende Meldungen empfangen, die zum Thema der beibehaltenen Meldung veröffentlicht wurden, aber die beibehaltene Meldung wird beim Abonnement nicht zugestellt.

HINWEIS: Wenn Sie eine aufbewahrte Meldung abonnieren möchten, muss der Themenfilter in der Anforderung genau dem Thema der aufbewahrten Meldung entsprechen.

Bei gespeicherten Meldungen, die beim Abonnieren eines gespeicherten Meldungsthemas empfangen wurden, ist das RETAIN-Flag gesetzt. Bei gespeicherten Meldungen, die nach dem Abonnement von einem abonnierten Client empfangen werden, ist dies nicht der Fall.

- Eine beibehaltene Meldung wird abgerufen.

  Aufbewahrte Meldungen werden automatisch an Clients zugestellt, wenn sie das Thema mit der gespeicherten Meldung abonnieren. Damit ein Kunde die beibehaltene Meldung nach dem Abonnement erhalten kann, muss er den genauen Themennamen der gespeicherten Meldung abonnieren. Wenn Sie einen Wildcard-Themenfilter abonnieren, der ein aufbewahrtes Meldungsthema enthält, kann der Client nachfolgende Meldungen empfangen, die zum Thema der beibehaltenen Meldung veröffentlicht wurden, aber die beibehaltene Meldung wird beim Abonnement nicht zugestellt.

  Dienste und Apps können gespeicherte Meldungen auflisten und abrufen, indem sie `ListRetainedMessages`und `GetRetainedMessage`aufrufen.

  Ein Client kann nicht daran gehindert werden, Meldungen zu einem gespeicherten Meldungsthema zu veröffentlichen, ohne das RETAIN-Flag zu setzen. Dies kann zu unerwarteten Ergebnissen führen, z. B. dass die gespeicherte Meldung nicht mit der Meldung übereinstimmt, die durch das Abonnieren des Themas empfangen wurde.

Wenn bei MQTT 5 für eine beibehaltene Meldung das Meldungsablaufintervall festgelegt ist und die beibehaltene Meldung abläuft, erhält ein neuer Abonnent, der dieses Thema abonniert, die beibehaltene Meldung bei erfolgreichem Abonnement nicht.

- Themen der beibehaltenen Meldungen auflisten

  Sie können die gespeicherten Meldungen auflisten, indem Sie `ListRetainedMessages` telefonisch abrufen, und die gespeicherten Meldungen können in der AWS IoT Konsole eingesehen werden.

- Details zu gespeicherten Meldungen abrufen

  Sie können die gespeicherten Meldungsdetails telefonisch unter `GetRetainedMessage` abrufen, und sie können in der AWS IoT Konsole angezeigt werden.

- Beibehaltung einer Willensnachricht

  MQTT-Will-Meldungen, die erstellt werden, wenn ein Gerät eine Verbindung herstellt, können beibehalten werden, indem das `Will Retain` Flag im `Connect Flag bits` Feld gesetzt wird.

- Löschen einer beibehaltenen Nachricht

  Geräte, Anwendungen und Dienste können eine gespeicherte Meldung löschen, indem sie eine Meldung mit gesetztem RETAIN-Flag und einer leeren Meldungs-Payload (0 Byte) im Themennamen der zu löschenden Meldung veröffentlichen. Solche Nachrichten löschen die gespeicherte Nachricht von und werden an Clients gesendet AWS IoT Core, die das Thema abonniert haben, aber sie werden nicht von gespeichert. AWS IoT Core

  Beibehaltene Meldungen können auch interaktiv gelöscht werden, indem Sie in der AWS IoT Konsole auf die gespeicherte Meldung zugreifen. Archivierte Meldungen, die mithilfe der AWS IoT Konsole gelöscht werden, senden auch eine 0-Byte-Meldung an Clients, die das Thema der gespeicherten Meldung abonniert haben.

  Aufbewahrte Meldungen können nicht wiederhergestellt werden, nachdem sie gelöscht wurden. Ein Client müsste eine neue beibehaltene Meldung veröffentlichen, um die gelöschte Meldung zu ersetzen.

- Debuggen und Problembehandlung bei gespeicherten Meldungen

  Die AWS IoT Konsole bietet mehrere Tools, mit denen Sie Fehler bei gespeicherten Meldungen beheben können:

  - Die Seite „Zurückbehaltene Meldungen“

Die Seite „Zurückbehaltene Meldungen“ in der AWS IoT Konsole enthält eine paginierte Liste der gespeicherten Meldungen, die von Ihrem Konto in der aktuellen Region gespeichert wurden. Auf dieser Seite können Sie:

- Sehen Sie sich die Details jeder gespeicherten Meldung an, z. B. die Meldungsnutzlast, QoS und den Zeitpunkt, zu dem sie empfangen wurde.
- Aktualisieren Sie den Inhalt einer gespeicherten Nachricht.
- Löscht eine beibehaltene Nachricht.

- Der MQTT-Testclient

  Auf der MQTT-Testclient-Seite in der AWS IoT Konsole können MQTT-Themen abonniert und veröffentlicht werden. Mit der Veröffentlichungsoption können Sie das RETAIN-Flag für die von Ihnen veröffentlichten Meldungen setzen, um zu simulieren, wie sich Ihre Geräte verhalten könnten.

Einige unerwartete Ergebnisse können auf diese Aspekte der Implementierung von gespeicherten Nachrichten zurückzuführen sein AWS IoT Core.

- Beibehaltene Meldungslimits

  Wenn ein Konto die maximale Anzahl an gespeicherten Nachrichten gespeichert hat, wird eine gedrosselte Antwort auf Nachrichten AWS IoT Core zurückgegeben, die mit aktiviertem RETAIN und Payloads von mehr als 0 Byte veröffentlicht wurden, bis einige der gespeicherten Nachrichten gelöscht wurden und die Anzahl der gespeicherten Nachrichten unter den Grenzwert fällt.

- Beibehaltene Reihenfolge der Meldungszustellung

  Die Reihenfolge zwischen beibehaltener und abonnierter Meldungszustellung kann nicht garantiert werden.

### Abrechnung und gespeicherte Meldungen

Beim Veröffentlichen von Meldungen, bei denen das RETAIN-Flag gesetzt ist, von einem Client aus, über die AWS IoT Konsole oder per Anruf `Publish` fallen zusätzliche Gebühren für Meldungsübermittlung an, die unter AWS IoT Core Preise – Meldungsübermittlung beschrieben sind.

Beim Abrufen von gespeicherten Nachrichten durch einen Client, über die AWS IoT Konsole oder durch einen Anruf `GetRetainedMessage`fallen zusätzlich zu den normalen API-Nutzungsgebühren

Gebühren für Nachrichtenübermittlung an. Die zusätzlichen Gebühren sind unter AWS IoT Core Preise – Meldungsübermittlung beschrieben.

Für Will-Meldungen, die veröffentlicht werden, wenn die Verbindung zu einem Gerät unerwartet unterbrochen wird, fallen Gebühren für die Meldungsübermittlung an, die unter AWS IoT Core Preise – Meldungsübermittlung beschrieben sind.

Weitere Informationen zu den Messaging-Kosten finden Sie unter AWS IoT Core Preise – Meldungsübermittlung.

Vergleich von beibehaltenen MQTT-Meldungen und persistenten MQTT-Sitzungen

Aufbewahrte Meldungen und persistente Sitzungen sind Standardfunktionen von MQTT, die es Geräten ermöglichen, Meldungen zu empfangen, die veröffentlicht wurden, während sie offline waren. Aufbewahrte Meldungen können aus persistenten Sitzungen heraus veröffentlicht werden. In diesem Abschnitt werden die wichtigsten Aspekte dieser Funktionen und ihr Zusammenspiel beschrieben.

| | Beibehaltene Meldungen | Persistente MQTT-Sitzungen |
|---|---|---|
| Schlüsselfunktionen | Aufbewahrte Meldungen können verwendet werden, um große Gruppen von Geräten zu konfigurieren oder zu benachrichtigen, nachdem sie eine Verbindung hergestellt haben.<br><br>Aufbewahrte Meldungen können auch verwendet werden, wenn Geräte nach einer erneuten Verbindung nur die zuletzt zu einem Thema veröffentlichte Meldung empfangen sollen. | Dauerhafte Sitzungen sind nützlich für Geräte, deren Konnektivität unterbrochen ist und bei denen möglicherweise mehrere wichtige Meldungen übersehen werden.<br><br>Geräte können sich mit einer dauerhaften Sitzung verbinden, um Meldungen zu empfangen, die gesendet werden, während sie offline sind. |
| Beispiele | Gespeicherte Meldungen können Geräten Konfigura tionsinformationen über ihre Umgebung geben, wenn sie | Geräte, die über ein Mobilfunk netz mit intermittierender Konnektivität eine Verbindung herstellen, könnten persisten |

| | Beibehaltene Meldungen | Persistente MQTT-Sitzungen |
|---|---|---|
| | online gehen. Die Erstkonfiguration könnte eine Liste anderer Meldungsthemen enthalten, die das Gerät abonnieren sollte, oder Informationen darüber, wie es seine lokale Zeitzone konfigurieren sollte. | te Sitzungen verwenden, um zu verhindern, dass wichtige Meldungen verpasst werden, die gesendet werden, wenn ein Gerät nicht mit Netzempfang versorgt ist oder sein Mobilfunknetz ausgeschaltet werden muss. |
| Meldungen, die beim ersten Abonnement eines Themas eingegangen sind | Nach dem Abonnieren eines Themas mit einer beibehaltenen Meldung wird die neueste beibehaltene Meldung empfangen. | Nach dem Abonnieren eines Themas ohne beibehaltene Meldung wird keine Meldung empfangen, bis eine Meldung zu dem Thema veröffentlicht wird. |
| Abonnierte Themen nach dem erneuten Verbindungsaufbau | Ohne eine dauerhafte Sitzung muss der Client nach der Wiederverbindung Themen abonnieren. | Abonnierte Themen werden nach der Wiederverbindung wiederhergestellt. |
| Nach der Wiederverbindung empfangene Meldungen | Nach dem Abonnieren eines Themas mit einer beibehaltenen Meldung wird die neueste beibehaltene Meldung empfangen. | Alle Meldungen, die mit QOS = 1 veröffentlicht und mit QOS =1 abonniert wurden, während das Gerät getrennt wurde, werden gesendet, nachdem das Gerät wieder eine Verbindung hergestellt hat. |

| | Beibehaltene Meldungen | Persistente MQTT-Sitzungen |
|---|---|---|
| Sitzungsablauf | In MQTT 3 laufen gespeicherte Meldungen nicht ab. Sie werden gespeichert, bis sie ersetzt oder gelöscht werden. In MQTT 5 laufen gespeicherte Meldungen nach dem von Ihnen festgelegten Meldungsablaufintervall ab. Weitere Informationen finden Sie unter Message templates (Meldungsvorlagen). | Persistente Sitzungen laufen ab, wenn der Client innerhalb des Timeout-Zeitraums keine erneute Verbindung herstellt. Nach Ablauf einer dauerhaften Sitzung werden die Abonnements und gespeicherten Meldungen des Clients gelöscht, die mit einem QOS = 1 veröffentlicht und mit einem QOS =1 abonniert wurden, während das Gerät getrennt wurde. Abgelaufene Meldungen werden nicht zugestellt. Weitere Hinweise zum Ablauf von Sitzungen mit persistenten Sitzungen finden Sie unter the section called “Persistente MQTT-Sitzungen”. |

Informationen zu persistentem Speicher siehe the section called “Persistente MQTT-Sitzungen”.

Bei Retained Messages bestimmt der Publishing-Client, ob eine Meldung aufbewahrt und an ein Gerät gesendet werden soll, nachdem das Gerät eine Verbindung hergestellt hat, unabhängig davon, ob es eine vorherige Sitzung hatte oder nicht. Die Entscheidung, eine Meldung zu speichern, wird vom Herausgeber getroffen, und die gespeicherte Meldung wird an alle aktuellen und zukünftigen Clients zugestellt, die ein Abonnement für QoS 0 oder QoS 1 abgeschlossen haben. Bei gespeicherten Meldungen wird jeweils nur eine Meldung zu einem bestimmten Thema gespeichert.

Wenn ein Konto die maximale Anzahl an gespeicherten Meldungen gespeichert hat, wird AWS IoT Core eine gedrosselte Antwort auf Meldungen zurückgeben, bei denen RETAIN aktiviert war, und Nutzlasten von mehr als 0 Byte, bis einige beibehaltene Meldungen gelöscht wurden und die Anzahl der gespeicherten Meldungen unter den Grenzwert fällt.

## In MQTT gespeicherte Nachrichten und Device Shadows AWS IoT

Sowohl bei gespeicherten Meldungen als auch bei Geräteschatten werden Daten von einem Gerät gespeichert, sie verhalten sich jedoch unterschiedlich und dienen unterschiedlichen Zwecken. In diesem Abschnitt werden ihre Ähnlichkeiten und Unterschiede beschrieben.

| | Beibehaltene Meldungen | Geräteschatten |
|---|---|---|
| Die Meldungsnutzlast hat eine vordefinierte Struktur oder ein vordefiniertes Schema. | Wie in der Implementierung definiert. MQTT spezifiziert keine Struktur oder kein Schema für seine Meldungsnutzlast. | AWS IoT unterstützt eine bestimmte Datenstruktur. |
| Durch die Aktualisierung der Meldungsnutzlast werden Ereignismeldungen generiert. | Durch das Veröffentlichen einer gespeicherten Meldung wird die Meldung an abonnierte Clients gesendet, es werden jedoch keine zusätzlichen Aktualisierungsnachrichten generiert. | Beim Aktualisieren eines Geräteschattens werden Aktualisierungsmeldungen angezeigt, die die Änderung beschreiben. |
| Meldungsaktualisierungen sind nummeriert. | Aufbewahrte Meldungen werden nicht automatisch nummeriert. | Geräteschatten-Dokumente haben automatische Versionsnummern und Zeitstempel. |
| Die Meldungen-Payload ist an eine Ding-Ressource angehängt. | Beibehaltene Meldungen sind nicht an eine Ding-Ressource angehängt. | Geräteschatten sind an eine Ding-Ressource angehängt. |
| Einzelne Elemente der Meldungs-Payload werden aktualisiert. | Einzelne Elemente der Meldung können nicht geändert werden, ohne die gesamte Meldungsnutzlast zu aktualisieren. | Einzelne Elemente eines Geräteschatten-Dokuments können aktualisiert werden, ohne dass das gesamte Geräteschatten-Dokument aktualisiert werden muss. |

| | Beibehaltene Meldungen | Geräteschatten |
|---|---|---|
| Der Kunde erhält Meldungsdaten bei Abschluss des Abonnements. | Der Kunde erhält automatisch eine gespeicherte Nachricht, nachdem er ein Thema mit einer gespeicherten Meldung abonniert hat. | Clients können Geräteschatten-Updates abonnieren, müssen den aktuellen Status jedoch bewusst anfordern. |
| Indizierung und Durchsuchbarkeit | Zurückbehaltene Meldungen werden nicht für die Suche indexiert. | Flottenindizierung indexiert Geräteschatten-Daten für die Suche und Aggregation. |

MQTT-Meldungen des letzten Willens und Testaments (LWT)

Last Will and Testament (LWT) ist ein Feature in MQTT. Mit LWT können Kunden eine Meldung angeben, die der Broker zu einem vom Kunden definierten Thema veröffentlicht und an alle Clients sendet, die das Thema abonniert haben, wenn eine uninitiierte Verbindungsunterbrechung auftritt. Die von den Clients angegebene Meldung wird als LWT-Meldung oder Will-Meldung bezeichnet, und das von den Clients definierte Thema wird Will-Thema genannt. Sie können eine LWT-Meldung angeben, wenn ein Gerät eine Verbindung zum Broker herstellt. Diese Meldungen können beibehalten werden, indem während der Verbindung die `Will Retain` Markierung im `Connect Flag bits` Feld gesetzt wird. Wenn die `Will Retain` Markierung beispielsweise auf 1 gesetzt ist, wird eine Will-Meldung im Broker im zugehörigen Testament-Thema gespeichert. Weitere Informationen finden Sie unter Meldungsvorlagen.

Der Broker speichert die Will-Meldungen, bis es zu einer uninitiierten Verbindungsunterbrechung kommt. In diesem Fall veröffentlicht der Broker die Meldungen an alle Clients, die das Will-Thema abonniert haben, um den Verbindungsabbruch zu melden. Wenn der Client die Verbindung zum Broker mit einer vom Client initiierten Verbindungsunterbrechung mithilfe der MQTT DISCONNECT-Meldung trennt, veröffentlicht der Broker die gespeicherten LWT-Meldungen nicht. In allen anderen Fällen werden die LWT-Meldungen versendet. Eine vollständige Liste der Verbindungsszenarien, in denen der Broker die LWT-Meldungen sendet, finden Sie unter Connect/Disconnect events.

ConnectAttributes verwenden

`ConnectAttributes` ermöglichen es Ihnen, in Ihren IAM-Richtlinien anzugeben, welche Attribute Sie in Ihrer Connect-Meldung verwenden möchten, z. B. `PersistentConnect` und `LastWill` Mit

`ConnectAttributes` können Sie Richtlinien erstellen, die Geräten standardmäßig keinen Zugriff auf neue Funktionen gewähren. Dies kann hilfreich sein, wenn ein Gerät kompromittiert wurde.

`connectAttributes` unterstützt die folgenden Funktionen:

`PersistentConnect`

Verwenden Sie die `PersistentConnect` Funktion, um alle Abonnements zu speichern, die der Client während der Verbindung abschließt, wenn die Verbindung zwischen dem Client und dem Broker unterbrochen wird.

`LastWill`

Verwenden Sie die `LastWill` Funktion, um eine Meldung an `LastWillTopic` zu veröffentlichen, wenn ein Client unerwartet die Verbindung trennt.

Standardmäßig hat Ihre Richtlinie eine nicht persistente Verbindung, und für diese Verbindung werden keine Attribute übergeben. Sie müssen in Ihrer IAM-Richtlinie eine persistente Verbindung angeben, wenn Sie eine haben möchten.

`ConnectAttributes`Beispiele finden Sie unter Beispiele für Connect-Richtlinien.

Von MQTT 5 unterstützte Funktionen

AWS IoT Core Die Unterstützung für MQTT 5 basiert auf der MQTT v5.0-Spezifikation mit einigen Unterschieden, die unter dokumentiert sind. the section called “AWS IoT Unterschiede zu den MQTT-Spezifikationen”

AWS IoT Core unterstützt die folgenden MQTT 5-Funktionen:

- Geteilte Abonnements
- Clean Start und Ablauf der Sitzung
- Ursachencode für alle ACKs
- Themen-Aliase
- Ablauf der Nachricht
- Weitere Funktionen von MQTT 5

## Geteilte Abonnements

AWS IoT Core unterstützt Shared Subscriptions sowohl für MQTT 3 als auch für MQTT 5. Geteilte Abonnements ermöglichen es mehreren Clients, ein Abonnement für ein Thema gemeinsam zu nutzen, und nur ein Client erhält Meldungen, die zu diesem Thema veröffentlicht wurden, nach dem Zufallsprinzip. Mit geteilten Abonnements können MQTT-Meldungen effektiv auf mehrere Abonnenten verteilt werden. Nehmen wir zum Beispiel an, Sie haben 1.000 Geräte, die zum gleichen Thema veröffentlichen, und 10 Backend-Anwendungen, die diese Meldungen verarbeiten. In diesem Fall können die Backend-Anwendungen dasselbe Thema abonnieren und jede Anwendung würde nach dem Zufallsprinzip Meldungen empfangen, die von den Geräten zu dem gemeinsamen Thema veröffentlicht wurden. Auf diese Weise wird die Menge dieser Meldungen quasi „geteilt“. Geteilte Abonnements ermöglichen auch eine bessere Ausfallsicherheit. Wenn eine Back-End-Anwendung die Verbindung trennt, verteilt der Broker die Last auf die verbleibenden Abonnenten in der Gruppe.

Um gemeinsame Abonnements zu verwenden, abonnieren Kunden den Themenfilter eines gemeinsamen Abonnements wie folgt:

```
$share/{ShareName}/{TopicFilter}
```

- `$share` ist eine wörtliche Zeichenfolge, die den Themenfilter eines geteilten Abonnements angibt, der mit `$share` beginnen muss.
- `{ShareName}` ist eine Zeichenfolge zur Angabe des gemeinsamen Namens, der von einer Gruppe von Abonnenten verwendet wird. Der Themenfilter eines geteilten Abonnements muss ein `ShareName` und gefolgt von einem `/` Zeichen enthalten. `{ShareName}` darf die folgenden Zeichen nicht enthalten: `/`,+ oder#. Die maximale Hash-Schlüsselgröße für `{ShareName}` ist 128 Byte.
- `{TopicFilter}` folgt derselben Themenfiltersyntax wie ein Abonnement ohne gemeinsame Nutzung. Die maximale Hash-Schlüsselgröße für `{TopicFilter}` ist 256 Byte.
- Die beiden erforderlichen Schrägstriche (`/`) für `$share/{ShareName}/{TopicFilter}` sind nicht in den Grenzwerten „Maximale Anzahl von Schrägstrichen im Thema“ und „Themenfilter“ enthalten.

Abonnements, die dasselbe `{ShareName}/{TopicFilter}` haben, gehören derselben gemeinsamen Abonnementgruppe an. Sie können mehrere Gruppen gemeinsam genutzter Abonnements erstellen und dabei das Limit für gemeinsame Abonnements pro Gruppe nicht überschreiten. Weitere Informationen finden Sie unter AWS IoT Core -Endpunkte und -Kontingente in der AWS Allgemeinen Referenz.

In den folgenden Tabellen werden nicht gemeinsam genutzte Abonnements und geteilte Abonnements verglichen:

| Abonnement | Beschreibung | Beispiele für Metrikfilter |
| --- | --- | --- |
| Nicht gemeinsam genutzte Abonnements | Jeder Client erstellt ein separates Abonnement für den Empfang der veröffentlichten Meldungen . Wenn eine Meldung zu einem Thema veröffentlicht wird, erhalten alle Abonnenten dieses Themas eine Kopie der Nachricht. | `sports/tennis`<br>`sports/#` |
| Geteilte Abonnements | Mehrere Kunden können sich ein Abonnement für ein Thema teilen, und nur ein Kunde erhält Meldungen, die zu diesem Thema veröffentlicht wurden, nach dem Zufallsprinzip. | `$share/consumer/sports/tennis`<br>`$share/consumer/sports/#` |

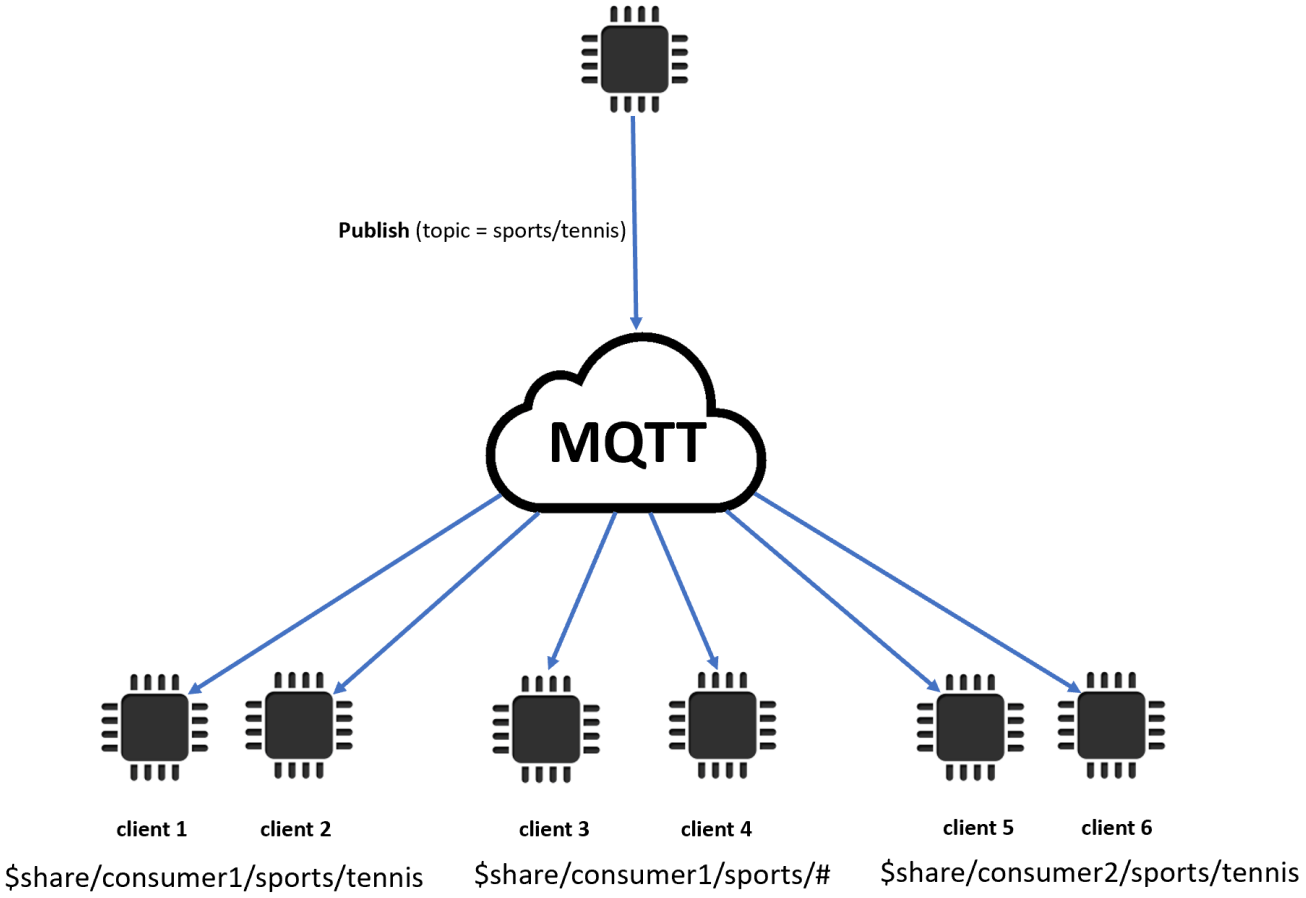
| Es werden nicht gemeinsam genutzte Abonnements angeboten. | Ablauf geteilter Abonnements | | |
| --- | --- | --- | --- |
| | | | |

Wichtige Hinweise zur Verwendung von geteilten Abonnements

- Wenn ein Veröffentlichungsversuch für einen QoS0-Abonnenten fehlschlägt, erfolgt kein erneuter Versuch, und die Meldung wird gelöscht.
- Wenn ein Veröffentlichungsversuch für einen QoS1-Abonnenten mit sauberer Sitzung fehlschlägt, wird die Meldung an einen anderen Abonnenten in der Gruppe für mehrere

Wiederholungsversuche gesendet. Meldungen, die nach allen Wiederholungsversuchen nicht zugestellt werden können, werden verworfen.

- Wenn ein Veröffentlichungsversuch für einen QoS1-Abonnenten mit persistenten Sitzungen fehlschlägt, weil der Abonnent offline ist, werden die Meldungen nicht in die Warteschlange gestellt, sondern an einen anderen Abonnenten in der Gruppe weitergeleitet. Meldungen, die nach allen Wiederholungsversuchen nicht zugestellt werden können, werden verworfen.
- Geteilte Abonnements empfangen keine gespeicherten Meldungen.
- Wenn gemeinsame Abonnements Platzhalterzeichen (# oder +) enthalten, gibt es möglicherweise mehrere übereinstimmende gemeinsame Abonnements zu einem Thema. In diesem Fall kopiert der Message Broker die Veröffentlichungsnachricht und sendet sie in jedem passenden gemeinsamen Abonnement an einen zufälligen Client. Das Platzhalterverhalten von gemeinsamen Abonnements kann in der folgenden Abbildung erklärt werden.



In diesem Beispiel gibt es drei passende gemeinsame Abonnements zum Thema Veröffentlichung von MQTT `sports/tennis`. Der Message Broker kopiert die veröffentlichte Meldung und sendet die Meldung an einen zufälligen Client in jeder passenden Gruppe.

Kunde 1 und Kunde 2 teilen sich das Abonnement: `$share/consumer1/sports/tennis`

Kunde 3 und Kunde 4 teilen sich das Abonnement: `$share/consumer1/sports/#`

Kunde 5 und Kunde 6 teilen sich das Abonnement: `$share/consumer2/sports/tennis`

Weitere Informationen zu den Limits für gemeinsame Abonnements finden Sie unter AWS IoT Core Endpunkte und Kontingente in der AWS Allgemeinen Referenz. Informationen zum Testen von gemeinsamen Abonnements mit dem AWS IoT MQTT-Client in der AWS IoT Konsole finden Sie unter. ??? Weitere Informationen zu gemeinsamen Abonnements finden Sie unter Gemeinsame Abonnements aus der MQTTv5 2.0-Spezifikation.

Clean Start und Ablauf der Sitzung

Sie können Clean Start und Session Expiry verwenden, um Ihre persistenten Sitzungen flexibler zu handhaben. Ein Clean Start-Flag gibt an, ob die Sitzung gestartet werden soll, ohne eine bestehende Sitzung zu verwenden. Ein Sitzungsablaufintervall gibt an, wie lange die Sitzung nach einer Unterbrechung beibehalten werden soll. Das Ablaufintervall für die Sitzung kann bei der Trennung geändert werden. Weitere Informationen finden Sie unter the section called “Persistente MQTT-Sitzungen”.

Ursachencode für alle ACKs

Mithilfe der Ursachencodes können Sie Fehlermeldungen einfacher debuggen oder verarbeiten. Ursachencodes werden vom Message Broker auf der Grundlage der Art der Interaktion mit dem Broker zurückgegeben (Abonnieren, Veröffentlichen, Bestätigen). Weitere Informationen finden Sie unter MQTT. Eine vollständige Liste der MQTT-Ursachencodes finden Sie in der MQTT v5-Spezifikation.

Themen-Aliase

Sie können einen Themennamen durch einen Themenalias ersetzen, bei dem es sich um eine Zwei-Byte-Ganzzahl handelt. Durch die Verwendung von Themenaliasnamen kann die Übertragung von Themennamen optimiert und so potenziell die Datenkosten für Dienste mit Messdaten gesenkt

werden. AWS IoT Core hat ein Standardlimit von 8 Themenaliasnamen. Weitere Informationen finden Sie unter AWS IoT Core -Endpunkte und -Kontingente in der AWS Allgemeinen Referenz.

Ablauf der Nachricht

Sie können veröffentlichten Meldungen Werte für den Ablauf von Meldungen hinzufügen. Diese Werte stellen das Meldungsablaufintervall in Sekunden dar. Wenn die Meldungen innerhalb dieses Intervalls nicht an die Abonnenten gesendet wurden, läuft die Meldung ab und wird entfernt. Wenn Sie den Wert für das Verfallsdatum der Meldung nicht festlegen, läuft die Meldung nicht ab.

Beim ausgehenden Versand erhält der Abonnent eine Meldung mit der verbleibenden Restzeit des Ablaufintervalls. Wenn beispielsweise eine eingehende Veröffentlichungsnachricht einen Meldungsablauf von 30 Sekunden hat und sie nach 20 Sekunden an den Abonnenten weitergeleitet wird, wird das Feld für den Ablauf der Meldung auf 10 aktualisiert. Es ist möglich, dass die vom Abonnenten empfangene Meldung einen aktualisierten MEI von 0 hat. Dies liegt daran, dass sie auf 0 aktualisiert wird, sobald die verbleibende Zeit 999 ms oder weniger beträgt.

In AWS IoT Core, das Mindestablaufintervall für Nachrichten ist 1. Wenn das Intervall auf der Clientseite auf 0 gesetzt ist, wird es auf 1 eingestellt. Das maximale Verfallsintervall für Meldungen beträgt 604800 (7 Tage). Alle Werte, die über diesem Wert liegen, werden an den Maximalwert angepasst.

Bei der versionsübergreifenden Kommunikation wird das Verhalten des Meldungsablaufs durch die MQTT-Version der eingehenden Veröffentlichungsnachricht bestimmt. Beispielsweise MQTT5 kann eine Nachricht mit Ablauf der Nachricht, die von einer Sitzung gesendet wurde, über die eine Verbindung hergestellt wurde, für Geräte ablaufen, die über MQTT3 Sitzungen abonniert wurden. In der folgenden Tabelle ist aufgeführt, wie der Ablauf von Meldungen die folgenden Arten von Veröffentlichungsnachrichten unterstützt:

| Veröffentlichen eines Meldungstyps | Ablaufintervall für Meldungen |
| --- | --- |
| Reguläres Veröffentlichen | Wenn ein Server die Meldung nicht innerhalb der angegebenen Zeit zustellt, wird die abgelaufene Meldung entfernt und der Abonnent erhält sie nicht. Dies schließt Situationen ein, z. B. wenn ein Gerät seine QoS 1-Meldungen nicht veröffentlicht. |

| Veröffentlichen eines Meldungstyps | Ablaufintervall für Meldungen |
|---|---|
| Beibehalten | Wenn eine gespeicherte Meldung abläuft und ein neuer Kunde das Thema abonniert, erhält der Client die Meldung nach Abschluss des Abonnements nicht. |
| Letzter Wille | Das Intervall für Meldungen des letzten Willens beginnt, nachdem der Client die Verbindung getrennt hat und der Server versucht, seinen Abonnenten die letzte Willensnachricht zuzustellen. |
| In die Warteschlange eingestellte Meldungen | Wenn ein ausgehender QoS1-Dienst mit Meldungsablaufintervall abläuft, während ein Client offline ist, empfängt der Client nach der Wiederaufnahme der persistenten Sitzung die abgelaufene Meldung nicht. |

Weitere Funktionen von MQTT 5

Verbindung zum Server trennen

Wenn eine Verbindung unterbrochen wird, kann der Server dem Client proaktiv eine DISCONNECT-Meldung senden, um den Verbindungsabbruch mit einem Ursachencode für die Trennung zu benachrichtigen.

Request Response (Antwort anfordern)

Verlage können verlangen, dass der Empfänger nach Erhalt eine Antwort auf ein vom Verlag spezifiziertes Thema sendet.

Maximale Teilegröße

Client und Server können unabhängig voneinander die maximale Paketgröße angeben, die sie unterstützen.

Payload-Format und Inhaltstyp

Sie können das Payload-Format (Binär, Text) und den Inhaltstyp angeben, wenn eine Meldung veröffentlicht wird. Diese werden an den Empfänger der Meldung weitergeleitet.

## MQTT 5 Eigenschaften

MQTT 5-Eigenschaften sind wichtige Ergänzungen des MQTT-Standards zur Unterstützung neuer MQTT 5-Funktionen wie Session Expiry und das Request/Response-Muster. In können Sie Regeln erstellen AWS IoT Core, die die Eigenschaften ausgehender Nachrichten weiterleiten können, oder HTTP Publish verwenden, um MQTT-Nachrichten mit einigen der neuen Eigenschaften zu veröffentlichen.

In der folgenden Tabelle sind alle MQTT 5-Eigenschaften aufgeführt, die unterstützt werden. AWS IoT Core

| Property (Eigenschaft) | Description (Beschreibung) | Eingab p | packets |
|---|---|---|---|
| Nutzlastformatindikator Nutzlastnutzlast | Ein Zeichenfolgenwert, der angibt, ob die Nutzlast als UTF-8 formatiert ist. | Byte | VERÖFFENTLICHEN, VERBINDEN |
| Inhaltstyp | Eine UTF-8-Zeichenfolge, die den Inhalt der Nutzlast beschreibt. | UTF-8 Zeichenfo | VERÖFFENTLICHEN, VERBINDEN |
| Thema der Antwort | Eine UTF-8-Zeichenfolge, die das Thema beschreibt, zu dem der Empfänger im Rahmen des Anfrage-Antwort-Ablaufs etwas veröffentlichen sollte. Das Thema darf keine Platzhalterzeichen enthalten. | UTF-8 Zeichenfo | VERÖFFENTLICHEN, VERBINDEN |
| Korrelationsdaten | Binärdaten, die vom Absender der Anforderungsnachricht verwendet werden, um zu identifizieren, für welche Anfrage die Antwortnachricht bestimmt ist. | Binär | VERÖFFENTLICHEN, VERBINDEN |
| Benutzereigenschaften | Ein UTF-8-Stringpaar. Diese Eigenschaft kann in einem Paket mehrfach vorkommen. Die Empfänger empfangen die Schlüssel- | UTF-8 String-Paar | VERBINDEN, VERÖFFENTLICHEN, Will-Eigenschaften, ABONNIERE |

| Property (Eigenschaft) | Description (Beschreibung) | Eingab p | packets |
|---|---|---|---|
| | Wert-Paare in derselben Reihenfolge, in der sie gesendet wurden. | | N, TRENNEN, ABBESTELLEN |
| Ablaufintervall für Meldungen | Eine 4-Byte-Ganzzahl, die das Verfallsintervall der Meldung in Sekunden darstellt. Wenn nicht vorhanden, läuft die Meldung nicht ab. | 4-Byte-Ganzzahl | VERÖFFENTLICHEN, VERBINDEN |
| Ablaufintervall der Sitzung | Eine 4-Byte-Ganzzahl, die das Ablaufintervall der Sitzung in Sekunden darstellt. AWS IoT Core unterstützt maximal 7 Tage, mit einem standardmäßigen Maximum von einer Stunde. Wenn der von Ihnen festgelegte Wert das Maximum Ihres Kontos überschreitet, AWS IoT Core wird der angepasste Wert im CONNACK zurückgegeben. | 4-Byte-Ganzzahl | VERBINDEN , VERBINDEN, TRENNEN |
| Zugewiesene Client-ID | Eine zufällige Client-ID, die generiert wird AWS IoT Core , wenn eine Client-ID nicht von Geräten angegeben wird. Bei der zufälligen Client-ID muss es sich um eine neue Client-ID handeln, die von keiner anderen Sitzung verwendet wird, die derzeit vom Broker verwaltet wird. | UTF-8 Zeichenfo | CONNACK |
| Server Keep Alive | Eine 2-Byte-Ganzzahl, die die vom Server zugewiesene Keep-Alive-Zeit darstellt. Der Server trennt die Verbindung zum Client, wenn der Client länger als die Keep-Alive-Zeit inaktiv ist. | 2-Byte-Ganzzahl | CONNACK |
| Problemin formationen anfordern | Ein boolescher Wert, der angibt, ob die Ursachenzeichenfolge oder die Benutzereigenschaften bei Fehlern gesendet werden. | Byte | CONNECT |

| Property (Eigenschaft) | Description (Beschreibung) | Eingab p | packets |
|---|---|---|---|
| Maximal empfangen | Eine 2-Byte-Ganzzahl, die die maximale Anzahl von PUBLISH QOS > 0-Paketen darstellt, die gesendet werden können, ohne dass ein PUBACK empfangen wird. | 2-Byte-Ganzzahl | VERBINDEN, CONNACK |
| Thema Alias Maximum | Dieser Wert gibt den höchsten Wert an, der als Themen-Alias akzeptiert wird. Standard = 0. | 2-Byte-Ganzzahl | VERBINDEN, CONNACK |
| Maximale QoS | Der maximale Wert von QoS, der AWS IoT Core unterstützt wird. Der Standardwert lautet 1. AWS IoT Core unterstützt QoS2 nicht. | Byte | CONNACK |
| Beibehaltung verfügbar | Ein boolescher Wert, der angibt, ob der AWS IoT Core Message Broker gespeicherte Nachrichten unterstützt. Der Standardwert ist 1. | Byte | CONNACK |
| Maximale Teilegröße | Die maximale Paketgröße, die AWS IoT Core akzeptiert und gesendet wird. Kann 128 KB nicht überschreiten. | 4-Byte-Ganzzahl | VERBINDEN, CONNACK |
| Wildcard-Abonnement verfügbar | Ein boolescher Wert, der angibt, ob der AWS IoT Core Message Broker Wildcard Subscription Available unterstützt. Der Standardwert ist 1. | Byte | CONNACK |
| Abonnement-ID verfügbar | Ein boolescher Wert, der angibt, ob der AWS IoT Core Message Broker Subscription Identifier Available unterstützt. Der Standardwert ist 0. | Byte | CONNACK |

MQTT-Ursachencodes

MQTT 5 führt eine verbesserte Fehlerberichterstattung mit Antworten auf Ursachencodes ein. AWS IoT Core kann Ursachencodes zurückgeben, einschließlich, aber nicht beschränkt auf die folgenden, gruppiert nach Paketen. Eine vollständige Liste der von MQTT 5 unterstützten Ursachencodes finden Sie in den MQTT 5-Spezifikationen.

CONNACK-Ursachencodes

| Wert | HEX() | Name des Grundcodes | Beschreibung |
|---|---|---|---|
| 0 | 0x00 | Herzlichen Glückwunsch | Die Verbindung wurde akzeptiert. |
| 128 | 0x80 | Unbekannter Fehler | Der Server möchte den Grund für den Fehler nicht preisgeben, oder keiner der anderen Ursachencodes trifft zu. |
| 133 | 0x85 | Die Client-ID ist nicht gültig. | Die Client-ID ist eine gültige Zeichenfolge, die jedoch vom Server nicht zugelassen wird. |
| 134 | 0x86 | Falscher Benutzername oder falsches Passwort | Der Server akzeptiert den vom Client angegebenen Benutzernamen oder das Passwort nicht. |
| 135 | 0x87 | Nicht autorisiert. | Der Client ist nicht autorisiert, eine Verbindung herzustellen. |
| 144 | 0x90 | Themenname ungültig | Der Name des Will-Themas ist korrekt formatiert, wird aber vom Server nicht akzeptiert. |
| 151 | 0 x 97 | Kontingent überschritten | Ein von der Implementierung oder vom Administrator auferlegtes Limit wurde überschritten. |
| 155 | 0 x 9 B | QoS nicht unterstützt | Der Server unterstützt die in Will QoS eingestellte QoS nicht. |

PUBACK-Ursachencodes

| Wert | HEX() | Name des Grundcodes | Beschreibung |
|---|---|---|---|
| 0 | 0x00 | Herzlichen Glückwunsch | Die Meldung wurde akzeptiert. Die Veröffentlichung der QoS 1-Meldung wird fortgesetzt. |
| 128 | 0x80 | Unbekannter Fehler | Der Empfänger akzeptiert die Veröffentlichung nicht, möchte aber entweder den Grund nicht preisgeben, oder er entspricht keinem der anderen Werte. |
| 135 | 0x87 | Nicht autorisiert. | Die Veröffentlichung ist nicht autorisiert. |
| 144 | 0x90 | Themenname ungültig | Der Themenname ist nicht falsch formatiert, wird aber vom Client oder Server nicht akzeptiert. |
| 145 | 0x91 | Paket-ID wird verwendet. | Die Paket-ID wird bereits verwendet. Dies könnte auf eine Nichtübereinstimmung des Sitzungsstatus zwischen Client und Server hinweisen. |
| 151 | 0 x 97 | Kontingent überschritten | Ein von der Implementierung oder vom Administrator auferlegtes Limit wurde überschritten. |

Disconnect – Ursachencodes

| Wert | HEX() | Name des Grundcodes | Beschreibung |
|---|---|---|---|
| 129 | 0x81 | Fehlerhaftes Paket | Das empfangene Paket entspricht nicht dieser Spezifikation. |
| 130 | 0x82 | Protokollfehler | Ein unerwartetes Paket oder ein Paket, das nicht in der richtigen Reihenfolge ist, wurde empfangen. |
| 135 | 0x87 | Nicht autorisiert. | Die Anfrage ist nicht autorisiert. |

| Wert | HEX() | Name des Grundcodes | Beschreibung |
|---|---|---|---|
| 139 | 0x8B | Server wird heruntergefahren. | Der Server wird heruntergefahren. |
| 141 | 0x8D | Keep Alive Timeout | Die Verbindung wurde geschlossen, weil seit dem 1,5-fachen der Keep-Alive-Zeit kein Paket mehr empfangen wurde. |
| 142 | 0x8E | Sitzung übernommen | Eine andere Verbindung, die dieselbe Client-ID verwendet, hat eine Verbindung hergestellt, wodurch diese Verbindung geschlossen wurde. |
| 143 | 0x8F | Ungültiger Themenfilter | Der Themenfilter ist korrekt formatiert, wird aber vom Server nicht akzeptiert. |
| 144 | 0x90 | Themenname ungültig | Der Themenname ist korrekt formatiert, wird aber von diesem Client oder Server nicht akzeptiert. |
| 147 | 0 x 93 | Empfangsmaximum überschritten | Der Client oder Server hat mehr als die Empfangsmaximum-Publikation erhalten, für die er weder PUBACK noch PUBCOMP gesendet hat. |
| 148 | 0 x 94 | Ungültiges Thema-Alias | Der Client oder Server hat ein PUBLISH-Paket erhalten, das einen Themen-Alias enthält, der größer ist als die maximale Anzahl an Themen-Alias, die er im CONNECT- oder CONNACK-Paket gesendet hat. |
| 151 | 0 x 97 | Kontingent überschritten | Ein von der Implementierung oder vom Administrator auferlegtes Limit wurde überschritten. |
| 152 | 0x98 | Administrative Maßnahmen | Die Verbindung wurde aufgrund einer Verwaltungsmaßnahme geschlossen. |
| 155 | 0 x 9 B | QoS nicht unterstützt | Der Client hat eine QoS angegeben, die höher ist als die QoS, die in einem Maximum QoS im CONNACK angegeben ist. |

| Wert | HEX() | Name des Grundcodes | Beschreibung |
|---|---|---|---|
| 161 | 0 x A1 | Abonnement-Identifikatoren werden nicht unterstützt. | Der Server unterstützt keine Abonnement-IDs. Das Abonnement wird nicht akzeptiert. |

SUBACK-Ursachencodes

| Wert | HEX() | Name des Grundcodes | Beschreibung |
|---|---|---|---|
| 0 | 0x00 | QoS gewährt 0 | Das Abonnement wurde akzeptiert, und die maximale gesendete QoS beträgt QoS 0. Dies könnte eine niedrigere QoS sein als gewünscht. |
| 1 | 0x01 | QoS 1 gewährt 1 | Das Abonnement wurde akzeptiert, und die maximale gesendete QoS beträgt QoS 1. Dies könnte eine niedrigere QoS sein als gewünscht. |
| 128 | 0x80 | Unbekannter Fehler | Das Abonnement wurde nicht akzeptiert, und der Server möchte den Grund entweder nicht preisgeben oder keiner der anderen Ursachencodes trifft zu. |
| 135 | 0x87 | Nicht autorisiert. | Der Kunde ist nicht berechtigt, dieses Abonnement abzuschli eßen. |
| 143 | 0x8F | Ungültiger Themenfilter | Der Themenfilter ist korrekt formatiert, ist aber für diesen Client nicht zulässig. |
| 145 | 0x91 | Paket-ID wird verwendet. | Die angegebene Paket-ID wird bereits verwendet. |
| 151 | 0 x 97 | Kontingent überschritten | Ein von der Implementierung oder vom Administrator auferlegtes Limit wurde überschritten. |

UNSUBACK-Ursachencodes

| Wert | HEX() | Name des Grundcodes | Beschreibung |
|---|---|---|---|
| 0 | 0x00 | Herzlichen Glückwunsch | Das Abonnement wird gelöscht. |
| 128 | 0x80 | Unbekannter Fehler | Die Abmeldung konnte nicht abgeschlossen werden, und der Server möchte den Grund entweder nicht preisgeben oder keiner der anderen Ursachencodes trifft zu. |
| 143 | 0x8F | Ungültiger Themenfilter | Der Themenfilter ist korrekt formatiert, ist aber für diesen Client nicht zulässig. |
| 145 | 0x91 | Paket-ID wird verwendet. | Die angegebene Paket-ID wird bereits verwendet. |

AWS IoT Unterschiede zu den MQTT-Spezifikationen

Die Message-Broker-Implementierung basiert auf der MQTT-Spezifikation v3.1.1 und der MQTT-Spezifikation v5.0, unterscheidet sich jedoch in folgenden Punkten von den Spezifikationen:

- AWS IoT unterstützt die folgenden Pakete für MQTT 3 nicht: PUBREC, PUBREL und PUBCOMP.
- AWS IoT unterstützt die folgenden Pakete für MQTT 5 nicht: PUBREC, PUBREL, PUBCOMP und AUTH.
- AWS IoT unterstützt keine MQTT 5-Serverumleitung.
- AWS IoT unterstützt nur die MQTT Quality of Service (QoS) Stufen 0 und 1. AWS IoT unterstützt das Veröffentlichen oder Abonnieren mit QoS Level 2 nicht. Bei Abfragen über QoS-Ebene 2 sendet der Message Broker kein PUBACK oder SUBACK.
- In AWS IoT bedeutet das Abonnieren eines Themas mit QoS-Stufe 0, dass eine Nachricht null Mal oder öfter zugestellt wird. Meldungen können mehr als einmal übertragen werden. Meldungen, die mehrmals übertragen werden, können mit unterschiedlicher Paket-ID gesendet werden. In diesem Fall wird das DUP-Flag nicht festgelegt.
- Der Message Broker sendet als Antwort auf eine Verbindungsanfrage eine CONNACK-Nachricht. Diese enthält ein Flag, das angibt, ob eine frühere Sitzung wieder aufgenommen wird.

- Bevor der Client zusätzliche Steuerpakete oder eine Anfrage zum Trennen der Verbindung sendet, muss er warten, bis die CONNACK-Meldung vom Message Broker auf seinem Gerät empfangen wird. AWS IoT
- Wenn ein Client ein Thema abonniert, kann es zwischen dem Zeitpunkt, an dem der Message Broker eine SUBACK-Meldung sendet, und den ersten eingehenden passenden Meldungen eine Verzögerung geben.
- Wenn ein Client das Platzhalterzeichen # im Themenfilter verwendet, um ein Thema zu abonnieren, werden alle Zeichenfolgen auf und unter seiner Ebene in der Themenhierarchie abgeglichen. Das übergeordnete Thema stimmt jedoch nicht überein. Wenn Sie beispielsweise das Thema `sensor/#` abonnieren, erhalten Sie Meldungen, die für `sensor/`, `sensor/temperature` oder `sensor/temperature/room1` veröffentlicht werden, nicht jedoch Meldungen, die für `sensor` veröffentlicht werden. Weitere Informationen zu Platzhaltern unter Filter für Themennamen.
- Der Message Broker verwendet die Client-ID, um die einzelnen Clients zu identifizieren. Die Client-ID wird vom Client im Rahmen der MQTT-Nutzlast an den Message Broker übermittelt. Zwei Clients mit identischen Client-IDs können nicht gleichzeitig mit dem Message Broker verbunden sein. Stellt ein Client eine Verbindung zum Message Broker über eine Client-ID her, die bereits von einem anderen Client verwendet wird, wird die neue Client-Verbindung akzeptiert und die Verbindung des früher verbundenen Clients getrennt.
- In seltenen Fällen kann der Message Broker die gleiche logische PUBLISH Meldung mit einer anderen Paket-ID erneut senden.
- Wenn Sie Themenfilter abonnieren, die ein Platzhalterzeichen enthalten, können keine beibehaltenen Meldungen empfangen werden. Um eine gespeicherte Meldung zu erhalten, muss die Anforderung einen Themenfilter enthalten, der genau dem Thema der gespeicherten Meldung entspricht.
- Die Reihenfolge, in der Meldungen und ACK empfangen werden, kann vom Message Broker nicht garantiert werden.
- AWS IoT kann Grenzwerte haben, die von den Spezifikationen abweichen. Weitere Informationen zu den Grenzwerten von AWS IoT Core Message Broker finden Sie im AWS IoT Referenzhandbuch.
- Das MQTT DUP-Flag wird nicht unterstützt.

## HTTPS

Clients können Nachrichten veröffentlichen, indem sie Anforderungen an die REST-API mit den Protokollen HTTP 1.0 oder 1.1 stellen. Informationen zu den Authentifizierungs- und Portzuordnungen, die von HTTP-Anforderungen verwendet werden, finden Sie unter ???.

> **Note**
>
> HTTPS unterstützt keinen `clientId`-Wert wie MQTT. `clientId` ist verfügbar, wenn MQTT verwendet wird, aber es ist nicht verfügbar, wenn HTTPS verwendet wird.

### HTTPS-Nachrichten-URL

Geräte und CLients veröffentlichen ihre Nachrichten, indem sie POST-Anfragen an einen clientspezifischen Endpunkt und eine themenspezifische URL stellen:

```
https://IoT_data_endpoint/topics/url_encoded_topic_name?qos=1
```

- *`IoT_data_endpoint`*ist der Endpunkt der AWS IoT Gerätedaten. Sie finden den Endpunkt in der AWS IoT Konsole auf der Detailseite der Sache oder auf dem Client mit dem AWS CLI folgenden Befehl:

  ```
  aws iot describe-endpoint --endpoint-type iot:Data-ATS
  ```

  Der Endpunkt sollte etwa so aussehen: `a3qjEXAMPLEffp-ats.iot.us-west-2.amazonaws.com`
- *`url_encoded_topic_name`*ist der vollständige Themenname der gesendeten Nachricht.

### Beispiele für HTTPS-Nachrichtencodes

Dies sind einige Beispiele dafür, wie Sie eine HTTPS-Nachricht an AWS IoT senden können.

Python (port 8443)

```
import requests
import argparse
```

```
# define command-line parameters
parser = argparse.ArgumentParser(description="Send messages through an HTTPS
 connection.")
parser.add_argument('--endpoint', required=True, help="Your AWS IoT data custom
 endpoint, not including a port. " +
                                                       "Ex: \"abcdEXAMPLExyz-
ats.iot.us-east-1.amazonaws.com\"")
parser.add_argument('--cert', required=True, help="File path to your client
 certificate, in PEM format.")
parser.add_argument('--key', required=True, help="File path to your private key, in
 PEM format.")
parser.add_argument('--topic', required=True, default="test/topic", help="Topic to
 publish messages to.")
parser.add_argument('--message', default="Hello World!", help="Message to publish. "
 +
                                                       "Specify empty string to
 publish nothing.")

# parse and load command-line parameter values
args = parser.parse_args()

# create and format values for HTTPS request
publish_url = 'https://' + args.endpoint + ':8443/topics/' + args.topic + '?qos=1'
publish_msg = args.message.encode('utf-8')

# make request
publish = requests.request('POST',
            publish_url,
            data=publish_msg,
            cert=[args.cert, args.key])

# print results
print("Response status: ", str(publish.status_code))
if publish.status_code == 200:
        print("Response body:", publish.text)
```

## Python (port 443)

```
import requests
import http.client
import json
import ssl
```

```
ssl_context = ssl.SSLContext(protocol=ssl.PROTOCOL_TLS_CLIENT)
ssl_context.minimum_version = ssl.TLSVersion.TLSv1_2

# note the use of ALPN
ssl_context.set_alpn_protocols(["x-amzn-http-ca"])
ssl_context.load_verify_locations(cafile="./<root_certificate>")

# update the certificate and the AWS endpoint
ssl_context.load_cert_chain("./<certificate_in_PEM_Format>",
 "<private_key_in_PEM_format>")
connection = http.client.HTTPSConnection('<the ats IoT endpoint>', 443,
 context=ssl_context)
message = {'data': 'Hello, I'm using TLS Client authentication!'}
json_data = json.dumps(message)
connection.request('POST', '/topics/device%2Fmessage?qos=1', json_data)

# make request
response = connection.getresponse()

# print results
print(response.read().decode())
```

CURL

So verwenden Sie curl zum Senden einer Nachricht an das AWS IoT.

Um Curl zu verwenden, um eine Nachricht von einem AWS IoT Client-Gerät aus zu senden

1. Überprüfen Sie die curl-Version.

   a. Führen Sie diesen Befehl auf Ihrem Client an einer Eingabeaufforderung aus.

      curl --help

      Suchen Sie im Hilfetext nach den TLS-Optionen. Sie sollten die `--tlsv1.2`-Option sehen.

   b. Wenn die `--tlsv1.2`-Option angezeigt wird, fahren Sie fort.

   c. Wenn die `--tlsv1.2`-Option nicht angezeigt wird oder Sie einen `command not found`-Fehler angezeigt bekommen, müssen Sie vor dem Fortfahren gegebenenfalls curl auf Ihrem Client aktualisieren oder `openssl` installieren.

2. Installieren Sie die Zertifikate auf Ihrem Client.

Kopieren Sie die Zertifikatsdateien, die Sie erstellt haben, als Sie Ihren Client (Ihr Ding) in der AWS IoT Konsole registriert haben. Stellen Sie sicher, dass sich diese drei Zertifikatdateien auf Ihrem Client befinden, bevor Sie fortfahren.

- Die CA-Zertifikatdatei (*Amazon-root-CA-1.pem* in diesem Beispiel).
- Die Zertifikatdatei des Clients (*device.pem.crt* in diesem Beispiel).
- Die private Schlüsseldatei des Clients (*private.pem.key* in diesem Beispiel).

3. Erstellen Sie die curl-Befehlszeile und ersetzen Sie die ersetzbaren Werte gegen die Werte Ihres Kontos und Systems.

```
curl --tlsv1.2 \
    --cacert Amazon-root-CA-1.pem \
    --cert device.pem.crt \
    --key private.pem.key \
    --request POST \
    --data "{ \"message\": \"Hello, world\" }" \
    "https://IoT_data_endpoint:8443/topics/topic?qos=1"
```

--tlsv1.2

Verwenden Sie TLS 1.2 (SSL).

--cacert *Amazon-root-CA-1.pem*

Der Dateiname und Pfad, falls erforderlich, des CA-Zertifikats für die Verifizierung des Peers.

--Zertifikat *device.pem.crt*

Der Dateiname und Pfad der Clientzertifikatdatei, falls erforderlich.

--Schlüssel *private.pem.key*

Der Dateiname und Pfad des privaten Schlüssels des Clients, falls erforderlich.

--request POST

Die Art der HTTP-Anfrage (in diesem Fall POST).

--daten "“ *{ \"message\": \"Hello, world\" }*

Die HTTP POST-Daten, die Sie veröffentlichen möchten. In diesem Fall handelt es sich um eine JSON-Zeichenfolge, wobei die internen Anführungszeichen mit dem umgekehrten Schrägstrich (\) als Escape-Zeichen markiert sind.

„https: //:8443/topics/? *IoT_data_endpoint topic* qos=1"

Die URL des AWS IoT Gerätedatenendpunkts Ihres Clients, gefolgt vom HTTPS-Port`:8443`, gefolgt vom Schlüsselwort `/topics/` und dem Themennamen`topic`, in diesem Fall. Geben Sie die Servicequalität als Abfrageparameter an, `?qos=1`, an.

4. Öffnen Sie den MQTT-Testclient in der AWS IoT Konsole.

   Folgen Sie den Anweisungen unter MQTT-Nachrichten mit dem AWS IoT MQTT-Client anzeigen und konfigurieren Sie die Konsole so, dass sie Nachrichten mit dem Themennamen abonniert, der in Ihrem curl Befehl *topic* verwendet wurde, oder verwenden Sie den Themenfilter mit Platzhaltern für. #

5. Testen Sie den Befehl.

   Während Sie das Thema im Testclient der AWS IoT -Konsole überwachen, rufen Sie im Client die in Schritt 3 erstellte curl-Befehlszeile auf. Sie sollten die Nachrichten Ihres Clients in der Konsole sehen.

## MQTT-Themen

MQTT-Themen identifizieren AWS IoT Nachrichten. AWS IoT Clients identifizieren die Nachrichten, die sie veröffentlichen, indem sie den Nachrichten Themennamen geben. Clients identifizieren die Nachrichten, die sie abonnieren (empfangen) möchten, indem sie einen Themenfilter bei AWS IoT Core registrieren. Der Message Broker verwendet Themennamen und Themenfilter, um Nachrichten von veröffentlichenden Clients an abonnierende Clients zu senden.

Der Message Broker verwendet Topics, um Nachrichten zu identifizieren, die über MQTT und über HTTP an die HTTPS-Nachrichten-URL gesendet wurden.

AWS IoT Unterstützt zwar einige reservierte Systemthemen, die meisten MQTT-Themen werden jedoch von Ihnen, dem Systemdesigner, erstellt und verwaltet. AWS IoT verwendet Themen, um Nachrichten zu identifizieren, die von Publishing-Clients empfangen wurden, und um Nachrichten auszuwählen, die an abonnierte Clients gesendet werden sollen, wie in den folgenden Abschnitten beschrieben. Bevor Sie einen Themen-Namespace für Ihr System erstellen, überprüfen Sie die

Merkmale von MQTT-Themen, um die Hierarchie der Themennamen zu erstellen, die für Ihr IoT-System am besten geeignet ist.

## Themennamen

Themennamen und Themenfilter sind UTF-8-codierte Zeichenfolgen. Sie können eine Hierarchie von Informationen darstellen, indem Sie den Schrägstrich (/) verwenden, um die Ebenen der Hierarchie zu trennen. Dieser Themenname könnte sich beispielsweise auf einen Temperatursensor in Raum 1 beziehen:

- `sensor/temperature/room1`

In diesem Beispiel kann es auch andere Arten von Sensoren in anderen Räumen mit Themennamen geben, z. B.:

- `sensor/temperature/room2`
- `sensor/humidity/room1`
- `sensor/humidity/room2`

> **Note**
>
> Beachten Sie bei der Betrachtung von Themennamen für die Nachrichten in Ihrem System Folgendes:
>
> - Themennamen und Themenfilter berücksichtigen Groß- und Kleinschreibung.
> - Themennamen dürfen keine personenbezogenen Informationen enthalten.
> - Themennamen, die mit einem "$" beginnen, sind reservierte Themen, die nur von AWS IoT Core verwendet werden können.
> - AWS IoT Core kann keine Nachrichten zwischen AWS-Konto s oder Regionen senden oder empfangen.

Weitere Informationen zum Entwurf von Themennamen und Ihres Namespaces finden Sie in unserem Whitepaper Entwerfen von MQTT-Themen für AWS IoT Core.

Beispiele dafür, wie Apps Nachrichten veröffentlichen und abonnieren können, finden Sie am Anfang mit Erste Schritte mit AWS IoT Core Tutorials und AWS IoT Geräte SDKs - SDKs, Mobil- und AWS IoT Geräteclient.

> **Important**
>
> Der Themennamespace ist auf eine Region AWS-Konto und beschränkt. Beispielsweise unterscheidet sich das von einem AWS-Konto in einer Region verwendete `sensor/temp/room1` Thema von dem `sensor/temp/room1` Thema, das von demselben AWS Konto in einer anderen Region oder von einem anderen AWS-Konto in einer anderen Region verwendet wird.

## Thema-ARN

Alle Themen ARNs (Amazon-Ressourcennamen) haben die folgende Form:

```
arn:aws:iot:aws-region:AWS-account-ID:topic/Topic
```

Zum Beispiel ist `arn:aws:iot:us-west-2:123EXAMPLE456:topic/application/topic/device/sensor` ein ARN für das Thema `application/topic/device/sensor`.

## Filter für Themennamen

Abonnierende Clients registrieren Themennamenfilter beim Message Broker, um die Nachrichtenthemen anzugeben, die der Message Broker an sie senden soll. Ein Themennamenfilter kann ein einzelner Themenname sein, um einen einzelnen Themennamen zu abonnieren, oder er kann Platzhalterzeichen enthalten, um mehrere Themennamen gleichzeitig zu abonnieren.

Veröffentlichende Clients können keine Platzhalterzeichen in den von ihnen veröffentlichten Themennamen verwenden.

In der folgenden Tabelle sind die Platzhalterzeichen aufgeführt, die in einem Themenfilter verwendet werden können.

Themenplatzhalter

| Platzhalterzeichen | Übereinstimmungen | Hinweise |
| --- | --- | --- |
| # | Alle Zeichenfolgen auf und unter seiner Ebene in der Themenhierarchie. | Muss das letzte Zeichen im Themenfilter sein.<br><br>Muss das einzige Zeichen auf seiner Ebene der Themenhierarchie sein.<br><br>Kann in einem Themenfilter verwendet werden, der auch das Platzhalterzeichen "+" enthält. |
| + | Jede Zeichenfolge in der Ebene, die das Zeichen enthält. | Muss das einzige Zeichen auf seiner Ebene der Themenhierarchie sein.<br><br>Kann in mehreren Ebenen eines Themenfilters verwendet werden. |

Verwenden von Platzhaltern mit den vorherigen Beispielen der Sensor-Themennamen:

- Ein Abonnement für `sensor/#` empfängt Nachrichten, die für `sensor/`, `sensor/temperature` oder `sensor/temperature/room1` veröffentlicht werden, nicht jedoch Nachrichten, die für `sensor` veröffentlicht werden.
- Ein Abonnement für `sensor/+/room1` empfängt Nachrichten, die für `sensor/temperature/room1` und `sensor/humidity/room1` veröffentlicht wurden, aber keine Nachrichten, die an `sensor/temperature/room2` oder `sensor/humidity/room2` gesendet wurden.

Themenfilter-ARN

Alle Themenfilter ARNs (Amazon-Ressourcennamen) haben die folgende Form:

```
arn:aws:iot:aws-region:AWS-account-ID:topicfilter/TopicFilter
```

`arn:aws:iot:us-west-2:123EXAMPLE456:topicfilter/application/topic/+/sensor` ist beispielsweise ein ARN für den Themenfilter `application/topic/+/sensor`.

## Nutzlast von MQTT-Nachrichten

Die Nachrichten-Payload, die in Ihren MQTT-Nachrichten gesendet wird, ist nicht spezifiziert von AWS IoT, es sei denn, sie bezieht sich auf eine der the section called “Reservierte Themen” Um den Anforderungen Ihrer Anwendung gerecht zu werden, empfehlen wir Ihnen, die Nachrichtennutzlast für Ihre Themen innerhalb der Einschränkungen der AWS IoT Core Service Quotas für Protokolle zu definieren.

Die Verwendung eines JSON-Formats für Ihre Nachrichtennutzdaten ermöglicht es der AWS IoT Regel-Engine, Ihre Nachrichten zu analysieren und SQL-Abfragen darauf anzuwenden. Wenn Ihre Anwendung die Regel-Engine nicht benötigt, um SQL-Abfragen auf Ihre Nachrichtennutzlasten anzuwenden, können Sie jedes Datenformat verwenden, das Ihre Anwendung benötigt. Hinweise zu Einschränkungen und reservierten Zeichen in einem JSON-Dokument, das in SQL-Abfragen verwendet wird, finden Sie unter JSON-Erweiterungen.

Weitere Informationen zum Entwerfen Ihrer MQTT-Themen und der entsprechenden Nachrichtennutzlasten finden Sie unter Entwurf von MQTT-Themen für AWS IoT Core.

Überschreitet eine Nachricht das Größenlimit des Dienstes, führt dies zu einem `CLIENT_ERROR` mit dem Grund `PAYLOAD_LIMIT_EXCEEDED` und "Die Nutzlast der Nachricht überschreitet das Größenlimit für den Nachrichtentyp". Weitere Informationen zur Größenbeschränkung für Nachrichten finden Sie unter AWS IoT Core Grenzwerte und Kontingente für Message Broker.

## Reservierte Themen

Themen, die mit einem Dollarzeichen ($) beginnen, sind für die Nutzung durch reserviert AWS IoT. Sie können diese reservierten Themen abonnieren und veröffentlichen, wenn sie dies zulassen. Sie können jedoch keine neuen Themen erstellen, die mit einem Dollarzeichen beginnen. Nicht unterstützte Veröffentlichungs- oder Abonnementvorgänge für reservierte Themen können zu einer abgebrochenen Verbindung führen.

Komponentenmodell-Themen

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $ aws/sitewise/asset - models/ /assets/ /properties/ | Abonnieren | AWS IoT SiteWise veröffent licht Benachrichtigungen |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| *assetModelId assetId propertyId* | | zu Vermögenswerten zu diesem Thema. Weitere Informationen finden Sie im AWS IoT SiteWise Benutzerhandbuch unter Interaktion mit anderen AWS Diensten. |

AWS IoT Device Defender Themen

Diese Nachrichten unterstützen je nach Thema Antwortpuffer im Format Concise Binary JavaScript Object Representation (CBOR) und Object Notation (JSON). *payload-format* AWS IoT Device Defender Themen unterstützen nur MQTT-Veröffentlichungen.

| ***payload-format*** | Datentyp des Antwortformats |
| --- | --- |
| cbor | Concise Binary Object Representation (CBOR) |
| json | JavaScript Objektnotation (JSON) |

Weitere Informationen finden Sie unter Metriken von Geräten senden.

| Thema | Zulässige Operationen | Beschreibung |
| --- | --- | --- |
| $aws/things/ /defender /metrics/ *thingName payload-format* | Veröffentlichen | AWS IoT Device Defender Agenten veröffentlichen Metriken zu diesem Thema. Weitere Informationen finden Sie unter Metriken von Geräten senden. |
| $aws/things/ /defender /metrics/ /accepted *thingName payload-format* | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, nachdem ein Agent eine erfolgreiche Nachricht in $aws/things/ /defender /metrics/ veröffentlicht hat. AWS IoT Device Defender *thingName* |

| Thema | Zulässige Operationen | Beschreibung |
| --- | --- | --- |
| | | *payload-format* Weitere Informationen finden Sie unter Metriken von Geräten senden. |
| $aws/things/ /defender /metrics/ /rejected *thingName payload-format* | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, nachdem ein Agent eine erfolglose Nachricht auf $aws/things/ / defender/metrics/ veröffentlicht hat. AWS IoT Device Defender *thingName payload-format* Weitere Informationen finden Sie unter Metriken von Geräten senden. |

AWS IoT Core Themen zum Gerätestandort

AWS IoT Core Device Location kann die Messdaten von Ihrem Gerät auflösen und einen geschätzten Standort Ihrer IoT-Geräte angeben. Die Messdaten des Geräts können GNSS-, WLAN-, Mobilfunk- und IP-Adressen umfassen. AWS IoT Core Der Gerätestandort wählt dann den Messtyp aus, der die beste Genauigkeit bietet, und berechnet die Standortinformationen des Geräts. Weitere Informationen erhalten Sie unter AWS IoT Core Standort des Geräts und Auflösen des Gerätestandorts mithilfe von Themen AWS IoT Core zum Gerätestandort MQTT.

| Thema | Zulässige Operationen | Beschreibung |
| --- | --- | --- |
| $aws/device_location/ / get_position_estimate *customer_device_id* | Veröffentlichen | Ein Gerät veröffentlicht zu diesem Thema, um die gescannten Rohmessdaten nach Gerätestandort aufzulösen. AWS IoT Core |
| $aws/device_location/ / get_position_estimate/ accepted *customer_device_id* | Abonnieren | AWS IoT Core Device Location veröffentlicht zu diesem Thema, nachdem der Gerätestandort erfolgreich ermittelt wurde. |

| Thema | Zulässige Operationen | Beschreibung |
| --- | --- | --- |
| $aws/device_location/ / get_position_estimate/ rejected *customer_device_id* | Abonnieren | AWS IoT Core Device Location veröffentlicht zu diesem Thema, wenn der Gerätestandort aufgrund von 4xx-Fehlern nicht erfolgreich ermittelt werden kann. |

Ereignisthemen

Die Ereignismeldungen werden veröffentlicht, wenn bestimmte Ereignisse eintreten. Beispielsweise werden Ereignisse von der Registry generiert, wenn Geräte hinzugefügt, aktualisiert oder gelöscht werden. Die Tabelle zeigt die verschiedenen AWS IoT Ereignisse und ihre reservierten Themen.

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/events/certificates/ registered/*caCertificateId* | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn ein Zertifikat AWS IoT automatisch registriert wird und wenn ein Client ein Zertifikat mit dem `PENDING_ACTIVATION` Status vorlegt. Weitere Informationen finden Sie unter the section called “Konfigurieren der ersten Verbindung durch einen Client für die automatische Registrierung”. |
| $aws/events/job/*jobID*/ storniert | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn ein Job storniert wird. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/job/*jobID*/ cancellation_in_progress | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn ein Job storniert wird. Weitere Informationen finden Sie unter Auftragsereignisse. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/events/job/*jobID*/abgeschlossen | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn ein Job abgeschlossen ist. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/job/*jobID*/gelöscht | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn ein Job gelöscht wird. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/job/*jobID*/deletion_in_progress | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn ein Job gelöscht wird. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/jobExecution/*jobID*/storniert | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn die Ausführung eines Jobs abgebrochen wird. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/jobExecution/*jobID*/gelöscht | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn eine Jobausführung gelöscht wird. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/jobExecution/*jobID*/ist fehlgeschlagen | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn die Ausführung eines Jobs fehlgeschlagen ist. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/jobExecution/*jobID*/abgelehnt | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn eine Jobausführung abgelehnt wurde. Weitere Informationen finden Sie unter Auftragsereignisse. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/events/jobExecution/*jobID*/entfernt | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn eine Jobausführung entfernt wurde. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/jobExecution/*jobID*/war erfolgreich | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn eine Jobausführung erfolgreich war. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/jobExecution/*jobID*/timed_out | Abonnieren | AWS IoT veröffentlicht diese Nachricht, wenn bei der Ausführung eines Jobs das Timeout überschritten wurde. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/presence/connected/*clientId* | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn ein MQTT-Client mit der angegebenen Client-ID eine Verbindung herstellt. AWS IoT Weitere Informationen finden Sie unter „Verbinden/Verbindung trennen“-Ereignisse. |
| $aws/events/presence/disconnected/*clientId* | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn ein MQTT-Client mit der angegebenen Client-ID die Verbindung trennt. AWS IoT Weitere Informationen finden Sie unter „Verbinden/Verbindung trennen“-Ereignisse. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/events/subscriptions/subscribed/*clientId* | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn ein MQTT-Client mit der angegebenen Client-ID ein MQTT-Thema abonniert. Weitere Informationen finden Sie unter „Abonnieren/Abonnement beenden“-Ereignisse. |
| $aws/events/subscriptions/unsubscribed/*clientId* | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn ein MQTT-Client mit der angegebenen Client-ID ein MQTT-Thema abbestellt. Weitere Informationen finden Sie unter „Abonnieren/Abonnement beenden“-Ereignisse. |
| $//erstellt aws/events/thing *thingName* | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn das *thingName* Ding erstellt wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |
| $aws/events/thing/ *thingName* /aktualisiert | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn das *thingName* Ding aktualisiert wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |
| $aws/events/thing/ *thingName* /gelöscht | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn das *thingName* Ding gelöscht wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/events/thingGroup/*thingGroupName*/erstellt | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn die Dinggruppe erstellt *thingGroupName* wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |
| $aws/events/thingGroup/*thingGroupName*/aktualisiert | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn die Dinggruppe aktualisiert *thingGroupName* wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |
| $aws/events/thingGroup/*thingGroupName*/gelöscht | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn die Dinggruppe gelöscht *thingGroupName* wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |
| $aws/events/thingType/*thingTypeName*/erstellt | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn der *thingTypeName* Dingtyp erstellt wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |
| $aws/events/thingType/*thingTypeName*/aktualisiert | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn der *thingTypeName* Dingtyp aktualisiert wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |
| $aws/events/thingType/*thingTypeName*/gelöscht | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn der *thingTypeName* Dingtyp gelöscht wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/events/thingTypeAssociation/thing/*thingName*/*thingTypeName* | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn *thingName* ein Objekt mit einem Dingtyp verknüpft oder vom Dingtyp *thingTypeName* getrennt wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |
| $aws/events/thingGroupMembership/thingGroup/*thingGroupName* /thing/ /hinzugefügt *thingName* | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn ein Objekt zur *thingName* Dinggruppe hinzugefügt wird. *thingGroupName* Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |
| $aws/events/thingGroupMembership/thingGroup/*thingGroupName* /thing/ /removed *thingName* | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn ein Objekt aus der *thingName* Dinggruppe entfernt wird. *thingGroupName* Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |
| $aws/events/thingGroupHierarchy/thingGroup//*parentThingGroupName* childThingGroup/*childThingGroupName* /hinzugefügt | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn die Dinggruppe zur Dinggruppe *parentThingGroupName* hinzugefügt *childThingGroupName* wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/events/thingGroupHierarchy/thingGroup//*parentThingGroupName* childThingGroup/*childThingGroupName* /wurde entfernt | Abonnieren | AWS IoT veröffentlicht zu diesem Thema, wenn die Dinggruppe aus der Dinggruppe *parentThingGroupName* entfernt *childThingGroupName* wird. Weitere Informationen finden Sie unter the section called “Registry-Ereignisse”. |

Flottenbereitstellungsthemen

> **Note**
>
> Die Client-Operationen, die in dieser Tabelle als Empfangen angegeben sind, weisen auf Themen hin, die direkt auf dem Client AWS IoT veröffentlicht werden, der sie angefordert hat, unabhängig davon, ob der Client das Thema abonniert hat oder nicht. Kunden sollten damit rechnen, diese Antwortnachrichten zu erhalten, auch wenn sie sie nicht abonniert haben. Diese Antwortnachrichten werden nicht über den Message Broker weitergeleitet und können auch nicht von anderen Clients oder Regeln abonniert werden.

Diese Nachrichten unterstützen je nach Thema Antwortpuffer im Format Concise Binary Object Representation (CBOR) und JavaScript Object Notation (JSON). *payload-format*

| ***payload-format*** | Datentyp des Antwortformats |
| --- | --- |
| cbor | Concise Binary Object Representation (CBOR) |
| json | JavaScript Objektnotation (JSON) |

Weitere Informationen finden Sie unter MQTT-API für die Gerätebereitstellung.

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/certificates/create/*payload-format* | Veröffentlichen | Veröffentlichen Sie in diesem Thema, um ein Zertifikat über eine Zertifikatssignierungsanforderung (Certificate Signing Request, CSR) zu erstellen. |
| $aws/certificates/create/*payload-format* / akzeptiert | Abonnieren, Empfangen | AWS IoT veröffentlicht nach einem erfolgreichen Aufruf von $aws/certificates/create/*payload-format* zu diesem Thema. |
| $aws/certificates/create/*payload-format* / abgelehnt | Abonnieren, Empfangen | AWS IoT veröffentlicht nach einem erfolglosen Aufruf von $aws/certificates/create/*payload-format* zu diesem Thema. |
| $ aws/certificates/create-from-csr/ *payload-format* | Veröffentlichen | Veröffentlicht in diesem Thema, um ein Zertifikat aus einer CSR zu erstellen. |
| $ aws/certificates/create-from-csr/ /akzeptiert *payload-format* | Abonnieren, Empfangen | AWS IoT veröffentlicht zu diesem Thema einen erfolgreichen Aufruf von $ -from-csr/. aws/certificates/create *payload-format* |
| $ -from-csr/ /abgelehnt aws/certificates/create *payload-format* | Abonnieren, Empfangen | AWS IoT veröffentlicht zu diesem Thema einen erfolglosen Aufruf von $ -from-csr/. aws/certificates/create *payload-format* |
| *templateName* $aws/provisioning-templates/ /provision/ *payload-format* | Veröffentlichen | Veröffentlichen Sie in diesem Thema, um ein Objekt zu registrieren. |
| $aws/provisioning-templates/ *templateN* | Abonnieren, Empfangen | AWS IoT veröffentlicht nach einem erfolgreichen Aufruf von $aws/prov |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| *ame* /provision/ /accepted *payload-format* | | isioning-templates/ /provision/ zu diesem Thema. *templateName payload-format* |
| $aws/provisioning-templates/ /provision/ /rejected *templateName payload-format* | Abonnieren, Empfangen | AWS IoT veröffentlicht nach einem erfolglosen Aufruf von $aws/provisioning-templates/ /provision/ zu diesem Thema. *templateName payload-format* |

Auftragsthemen

> **Note**
>
> Die Client-Operationen, die in dieser Tabelle als Empfangen angegeben sind, weisen auf Themen hin, die direkt auf dem Client AWS IoT veröffentlicht werden, der sie angefordert hat, unabhängig davon, ob der Client das Thema abonniert hat oder nicht. Kunden sollten damit rechnen, diese Antwortnachrichten zu erhalten, auch wenn sie sie nicht abonniert haben. Diese Antwortnachrichten werden nicht über den Message Broker weitergeleitet und können auch nicht von anderen Clients oder Regeln abonniert werden. Verwenden Sie die `notify` und `notify-next` Themen und, um Nachrichten zu Auftragsaktivitäten zu abonnieren.
> Wenn Sie die Auftrags- und `jobExecution` Veranstaltungsthemen für Ihre Flottenüberwachungslösung abonnieren, müssen Sie zunächst die Auftrags- und Auftragsausführungsereignisse aktivieren, um alle Ereignisse auf der Cloud-Seite empfangen zu können.
> Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus.

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/things/ /jobs/get *thingName* | Veröffentlichen | Geräte veröffentlichen eine Nachricht in diesem Topic, um eine `GetPendingJobExecutions` -Anforderung auszugeben. Weitere Informationen |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| | | finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |
| *thingName* $aws/things//jobs/get/accepted | Abonnieren, empfangen | Geräte abonnieren dieses Thema, um Antworten von einer `GetPendingJobExecutions` -Anforderung zu empfangen. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |
| $aws/Dinge/*thingName* /jobs/get/rejected | Abonnieren, Empfangen | Geräte abonnieren dieses Thema, um eine Antwort zu erhalten, wenn eine `GetPendingJobExecutions` Anforderung abgelehnt wird. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |
| $aws/things/ *thingName* /jobs/start-next | Veröffentlichen | Geräte veröffentlichen eine Nachricht in diesem Topic, um eine `StartNextPendingJobExecution` -Anforderung auszugeben. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |
| *thingName* $aws/things/jobs/start-next/accepted | Abonnieren, Empfangen | Geräte abonnieren dieses Topic, um Antworten an eine `StartNextPendingJobExecution` -Anforderung zu empfangen. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/Dinge/*thingName* / jobs/start-next/rejected | Abonnieren, Empfangen | Geräte abonnieren dieses Thema, um eine Antwort zu erhalten, wenn eine `StartNextPendingJobExecution` Anforderung abgelehnt wird. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |
| $aws/things/ /jobs/ /get *thingName* *jobId* | Veröffentlichen | Geräte veröffentlichen eine Nachricht in diesem Topic, um eine `DescribeJobExecution` -Anforderung auszugeben. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |
| $aws/things/ /jobs/ *thingName* /get/accepted *jobId* | Abonnieren, Empfangen | Geräte abonnieren dieses Topic, um Antworten an eine `DescribeJobExecution` -Anforderung zu empfangen. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |
| $aws/things/ /jobs/ *thingName* /get/rejected *jobId* | Abonnieren, Empfangen | Geräte abonnieren dieses Thema, um eine Antwort zu erhalten, wenn eine `DescribeJobExecution` Anforderung abgelehnt wird. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/things/ /jobs/ *thingName* /update *jobId* | Veröffentlichen | Geräte veröffentlichen eine Nachricht in diesem Thema, um eine `UpdateJobExecution` -Anforderung auszugeben. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |
| $aws/things/ /jobs/ *thingName* /update/akzeptiert *jobId* | Abonnieren, Empfangen | Geräte abonnieren dieses Thema, um Erfolgsantworten auf eine `UpdateJobExecution` -Anforderung zu empfangen. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus.<br><br>**Hinweis**<br>Nur das Gerät, das auf $aws/things/ /jobs/ /update veröffentlicht, empfängt Nachrichten zu diesem Thema. *thingName* *jobId* |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/things/ /jobs/ /update/rejected *thingName* *jobId* | Abonnieren, Empfangen | Geräte abonnieren dieses Thema, um eine Antwort zu erhalten, wenn eine `UpdateJobExecution` Anforderung abgelehnt wird. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus.<br><br>**Hinweis**<br>Nur das Gerät, das auf $aws/things/ /jobs/ /update veröffentlicht, empfängt Nachrichten zu diesem Thema. *thingName* *jobId* |
| $aws/things/ /jobs/notify *thingName* | Abonnieren, Empfangen | Geräte abonnieren dieses Thema, um Benachrichtigungen zu empfangen, wenn eine Auftragsausführung der Liste der ausstehenden Ausführungen für ein Objekt hinzugefügt oder aus dieser entfernt wird. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |
| $aws/things/ /jobs/notify-next *thingName* | Abonnieren, Empfangen | Geräte abonnieren dieses Thema, um Benachrichtigungen zu empfangen, wenn die nächste ausstehende Auftragsausführung für das Objekt geändert wird. Weitere Informationen finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $//abgeschlossen aws/events/job *jobId* | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn ein Auftrag abgeschlossen wird. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/job//storniert *jobId* | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn ein Auftrag abgebrochen wird. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/job//gelöscht *jobId* | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn ein Auftrag gelöscht wird. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/job//cancellation_in_progress *jobId* | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn eine Auftragsstornierung beginnt. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/job/*jobId*/deletion_in_progress | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn eine Auftragslöschung beginnt. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/jobExecution/*jobId*/war erfolgreich | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn der Auftrag erfolgreich ausgeführt wurde. Weitere Informationen finden Sie unter Auftragsereignisse. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/events/jobExecution/*jobId*/ist fehlgeschlagen | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn eine Auftragsausführung fehlschlägt. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/jobExecution//abgelehnt *jobId* | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn eine Auftragsausführung abgewiesen wird. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/jobExecution//storniert *jobId* | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn eine Auftragsausführung storniert wird. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/jobExecution//timed_out *jobId* | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn eine Zeitüberschreitung der Auftragsausführung auftritt. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $//wurde entfernt aws/events/jobExecution *jobId* | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn eine Auftragsausführung entfernt wird. Weitere Informationen finden Sie unter Auftragsereignisse. |
| $aws/events/jobExecution//gelöscht *jobId* | Abonnieren | Der Jobs-Service veröffentlicht ein Ereignis in diesem Thema, wenn eine Auftragsausführung gelöscht wird. Weitere Informationen finden Sie unter Auftragsereignisse. |

Themen zu Befehlen

> **Note**
>
> Die in dieser Tabelle als Empfangen vermerkten Client-Operationen beziehen sich auf Themen, die direkt auf dem Client AWS IoT veröffentlicht werden, der sie angefordert hat, unabhängig davon, ob der Client das Thema abonniert hat oder nicht. Kunden sollten damit rechnen, diese Antwortnachrichten zu erhalten, auch wenn sie sie nicht abonniert haben. Diese Antwortnachrichten werden nicht über den Message Broker weitergeleitet und können auch nicht von anderen Clients oder Regeln abonniert werden.

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/commands/// executions/ /request/ *<devices>* *<DeviceID>* *<ExecutionId>* *<PayloadFormat>*<br><br>$aws/commands//*<devices>* *<DeviceID>* /executions/ /request *<ExecutionId>* | Abonnieren, Empfangen | Geräte erhalten eine Nachricht zu diesem Thema, wenn eine Anfrage gestellt wird, eine Befehlsausführung von der Konsole oder über die API zu starten. `StartCommandExecution` In diesem Fall *<devices>* können es sich entweder um IoT-Dings oder MQTT-Clients handeln und es *<DeviceID>* kann sich entweder um den IoT-Dingnamen oder die MQTT-Client-ID handeln. |
| $aws/commands/ / executions/ /response/ *<devices>* *<DeviceID>* *<ExecutionId>* *<PayloadFormat>* | Veröffentlichen | Geräte verwenden die `UpdateCommandExecution` MQTT-API, um zu diesem Thema eine Nachricht über die Befehlsausführung zu veröffentlichen. Die Nachricht wird als Antwort auf die Anfrage veröffentlicht, eine Befehlsausführung über die Konsole oder über die `StartCommandExecution` API zu starten. Die veröffentlichte |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| | | Nachricht verwendet JSON oder CBOR als. *<PayloadFormat>* |
| $aws/commands///executions/ /response/accepted/ *<devices> <DeviceID> <ExecutionId> <PayloadFormat>*<br><br>$aws/commands//*<devices> <DeviceID>* /executions/ /response/accepted *<ExecutionId>* | Abonnieren, Empfangen | Wenn der Cloud-Dienst das Ergebnis der Befehlsausführung erfolgreich verarbeitet hat, veröffentlicht er eine Antwort auf das Thema /accepted. AWS IoT Device Management |
| $aws/commands///executions/ /response/rejected/ *<devices> <DeviceID> <ExecutionId> <PayloadFormat>*<br><br>$aws/commands//*<devices> <DeviceID>* /executions/ /response/rejected *<ExecutionId>* | Veröffentlichen | Wenn der Cloud-Dienst das Ergebnis der Befehlsausführung nicht verarbeiten konnte, veröffentlicht er eine Antwort auf das Thema /rejected. AWS IoT Device Management |

Regelthemen

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/rules/ *ruleName* | Veröffentlichen | Ein Gerät oder eine Anwendung veröffentlicht in diesem Thema, um Regeln direkt auszulösen. Weitere Informationen finden Sie unter Senken der Messaging-Kosten mit Basic Ingest. |

Themen zu Secure Tunneling

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/things/ /tunnels/notify *thing-name* | Abonnieren | AWS IoT veröffentlicht diese Nachricht für einen IoT-Agenten, um einen lokalen Proxy auf dem Remote-Gerät zu starten. Weitere Informationen finden Sie unter the section called “IoT-Agent-Snippet”. |

Schatten-Themen

Die Themen in diesem Abschnitt werden von benannten und unbenannten Schatten verwendet. Die jeweils verwendeten Themen unterscheiden sich nur durch das Themenpräfix. In dieser Tabelle wird das Themenpräfix angezeigt, das von jedem Schattentyp verwendet wird.

| ***ShadowTopicPrefix*** Wert | Schattentyp |
| --- | --- |
| $aws/things/ /shadow *thingName* | Unbenannter (klassischer) Schatten |
| $aws/things/ *thingName* /shadow/name/ *shadowName* | Benannter Schatten |

Um ein vollständiges Thema zu erstellen, wählen Sie *ShadowTopicPrefix* für den Typ des Schattens, auf den Sie sich beziehen möchten, ersetzen *thingName* und, falls zutreffend, durch die entsprechenden Werte*shadowName*, und fügen Sie diesen dann den Themen-Stub hinzu, wie in der folgenden Tabelle dargestellt. Denken Sie daran, dass bei Themen zwischen Groß- und Kleinschreibung unterschieden wird.

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| *ShadowTopicPrefix* / löschen | Veröffentlichen/Abonnieren | Ein Gerät oder eine Anwendung veröffentlicht in diesem Thema, um ein Schattengerät zu löschen. Weitere Informationen finden Sie unter /delete. |
| *ShadowTopicPrefix* / löschen/akzeptiert | Abonnieren | Der Device Shadow-Service sendet Nachrichten an dieses Thema, wenn ein Schattengerät gelöscht wird. Weitere Informationen finden Sie unter /delete/accepted. |
| *ShadowTopicPrefix* / löschen/abgelehnt | Abonnieren | Der Device Shadow-Service sendet Nachrichten an dieses Thema, wenn ein Anfrage zum Löschen eines Schattengeräts abgelehnt wird. Weitere Informationen finden Sie unter /delete/rejected. |
| *ShadowTopicPrefix* / erhalten | Veröffentlichen/Abonnieren | Eine Anwendung oder ein Gerät veröffentlicht eine leere Nachricht für dieses Thema, um ein Schattengerät zugewiesen zu bekommen. Weitere Informationen finden Sie unter MQTT-Themen für Geräteschatten. |
| *ShadowTopicPrefix* / get/akzeptiert | Abonnieren | Der Device Shadow-Service sendet Nachrichten an dieses Thema, wenn ein Anfrage für ein Schattengerät erfolgrei |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| | | ch war. Weitere Informationen finden Sie unter /get/accepted. |
| *ShadowTopicPrefix* / get/abgelehnt | Abonnieren | Der Device Shadow-Service sendet Nachrichten an dieses Thema, wenn ein Anfrage für ein Schattengerät abgelehnt wird. Weitere Informationen finden Sie unter /get/rejected. |
| *ShadowTopicPrefix* / aktualisieren | Veröffentlichen/Abonnieren | Ein Gerät oder eine Anwendung veröffentlicht eine Nachricht in diesem Thema, um ein Schattengerät zu aktualisieren. Weitere Informationen finden Sie unter /update. |
| *ShadowTopicPrefix* / update/akzeptiert | Abonnieren | Der Device Shadow-Service sendet Nachrichten an dieses Thema, wenn ein Schattengerät erfolgreich aktualisiert wurde. Weitere Informationen finden Sie unter /update/accepted. |
| *ShadowTopicPrefix* / update/abgelehnt | Abonnieren | Der Device Shadow-Service sendet Nachrichten an dieses Thema, wenn die Aktualisierung eines Schattengeräts abgelehnt wurde. Weitere Informationen finden Sie unter /update/rejected. |
| *ShadowTopicPrefix* / update/delta | Abonnieren | Der Device Shadow-Service sendet Nachrichten an dieses Thema, wenn zwischen den gemeldeten und gewünschten Abschnitten eines Schattengeräts Abweichungen auftreten. Weitere Informationen finden Sie unter /update/delta. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| *ShadowTopicPrefix* / update/dokumente | Abonnieren | AWS IoT veröffentlicht jedes Mal, wenn eine Aktualisierung des Shadows erfolgreich durchgeführt wurde, ein Statusdokument zu diesem Thema. Weitere Informationen finden Sie unter / update/documents. |

Themen der MQTT-basierten Dateiübertragung

> **Note**
>
> Die Client-Operationen, die in dieser Tabelle als Empfangen angegeben sind, weisen auf Themen hin, die direkt auf dem Client AWS IoT veröffentlicht werden, der sie angefordert hat, unabhängig davon, ob der Client das Thema abonniert hat oder nicht. Kunden sollten damit rechnen, diese Antwortnachrichten zu erhalten, auch wenn sie sie nicht abonniert haben. Diese Antwortnachrichten werden nicht über den Message Broker weitergeleitet und können auch nicht von anderen Clients oder Regeln abonniert werden.

Diese Nachrichten unterstützen je nach Thema Antwortpuffer im Format Concise Binary Object Representation (CBOR) und JavaScript Object Notation (JSON). *payload-format*

| ***payload-format*** | Datentyp des Antwortformats |
| --- | --- |
| cbor | Concise Binary Object Representation (CBOR) |
| json | JavaScript Objektnotation (JSON) |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/things/ /streams/ / data/ *ThingName* | Abonnieren, Empfangen | AWS Bei der MQTT-basierten Dateibereitstellung werden Beiträge |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| *StreamId payload-format* | | zu diesem Thema veröffentlicht, wenn die "" -Anforderung von einem Gerät akzeptiert wird. GetStream Die Nutzlast enthält die Stream-Daten. Weitere Informationen finden Sie unter Verwendung der AWS IoT MQTT basierten Dateibereitstellung auf Geräten. |
| $aws/things/ /streams/ /get/ *ThingName StreamId payload-format* | Veröffentlichen | Ein Gerät veröffentlicht Beiträge zu diesem Thema, um eine "" Anfrage auszuführen. GetStream Weitere Informationen finden Sie unter Verwendung der AWS IoT MQTT basierten Dateibereitstellung auf Geräten. |
| $aws/things/ /streams/ / description/ *ThingName StreamId payload-format* | Abonnieren, Empfangen | AWS Bei der MQTT-basierten Dateibereitstellung wird zu diesem Thema veröffentlicht, wenn die "" -Anforderung von einem Gerät akzeptiert wird. DescribeStream Die Nutzlast enthält die Stream-Beschreibung. Weitere Informationen finden Sie unter Verwendung der AWS IoT MQTT basierten Dateibereitstellung auf Geräten. |

| Thema | Zulässige Client-Operationen | Beschreibung |
| --- | --- | --- |
| $aws/things/ /streams/ / describe/ *ThingName StreamId payload-format* | Veröffentlichen | Ein Gerät veröffentlicht Beiträge zu diesem Thema, um eine "" Anfrage auszuführen. DescribeStream Weitere Informationen finden Sie unter Verwendung der AWS IoT MQTT basierten Dateibereitstellung auf Geräten. |
| $aws/things/ /streams/ / rejected/ *ThingName StreamId payload-format* | Abonnieren, Empfangen | AWS Bei der MQTT-basierten Dateibereitstellung werden Beiträge zu diesem Thema veröffentlicht, wenn eine "" - oder "" Anfrage von einem Gerät abgewiesen wird. DescribeStream GetStream Weitere Informationen finden Sie unter Verwendung der AWS IoT MQTT basierten Dateibereitstellung auf Geräten. |

Reservierte Themen-ARN

Alle reservierten Themen ARNs (Amazon-Ressourcennamen) haben die folgende Form:

```
arn:aws:iot:aws-region:AWS-account-ID:topic/Topic
```

`arn:aws:iot:us-west-2:123EXAMPLE456:topic/$aws/things/thingName/jobs/get/accepted` ist beispielsweise ein ARN für das reservierte Thema `$aws/things/thingName/jobs/get/accepted`.

## Domänenkonfigurationen

In können Sie Domänenkonfigurationen verwenden AWS IoT Core, um das Verhalten Ihrer Datenendpunkte zu konfigurieren und zu verwalten. Mit Domänenkonfigurationen können Sie mehrere AWS IoT Core Datenendpunkte generieren, sie mit Ihren eigenen vollqualifizierten Domainnamen (FQDN) und zugehörigen Serverzertifikaten anpassen und

auch einen benutzerdefinierten Autorisierer zuordnen. Weitere Informationen finden Sie unter Benutzerspezifische Authentifizierung und Autorisierung.

> **Note**
>
> Diese Funktion ist in nicht verfügbar. AWS GovCloud (US) AWS-Regionen

In diesem Kapitel:


- Was ist eine Domain-Konfiguration?
- AWS Verwaltete Domänen erstellen und konfigurieren
- Vom Kunden verwaltete Domains erstellen und konfigurieren
- Verwalten von Domänenkonfigurationen
- Konfiguration von TLS Einstellungen in Domänenkonfigurationen
- Konfiguration des Serverzertifikats für das OCSP Heften


## Was ist eine Domain-Konfiguration?

In bezieht AWS IoT Core sich eine Domänenkonfiguration auf die Einrichtung und Konfiguration einer Domain (entweder AWS verwaltete Domain oder kundenverwaltete Domain) für Ihre AWS IoT Core Datenendpunkte. AWS IoT Core stellt außerdem einen Standardendpunkt für Ihr AWS Konto (`iot:Data-ATS`) bereit, mit AWS IoT Core dem Geräte kommunizieren können.

In diesem Thema:


- Anwendungsfälle
- Die wichtigsten Konzepte
- Wichtige Hinweise


### Anwendungsfälle

Sie können Domänenkonfigurationen verwenden, um Aufgaben wie die folgenden zu vereinfachen.

- Migrieren Sie Geräte zu AWS IoT Core.
- Unterstützung heterogener Geräteflotten durch Beibehaltung separater Domänenkonfigurationen für separate Gerätetypen.

- Behalten Sie die Markenidentität bei (z. B. durch den Domainnamen) und migrieren Sie gleichzeitig die Anwendungsinfrastruktur zu AWS IoT Core.

### Die wichtigsten Konzepte

Die folgenden Konzepte enthalten Einzelheiten zu Domänenkonfigurationen und verwandten Konzepten.

- Konfiguration der Domäne

  Die Einrichtung und Konfiguration einer Domain für Ihre AWS IoT Core Endgeräte.

- Standard-Endpunktdomäne

  Die Domäne, die den Standardendpunkt AWS IoT bereitstellt, `iot:Data-ATS` z. Um den Standardendpunkt zu finden, führen Sie den Befehl describe-endpoint oder describe-domain-configurationCLIaus. Gehen Sie alternativ zur AWS IoT Core Konsole und wählen Sie in der linken Navigationsleiste Domain-Konfigurationen aus Connect aus. Der Standardendpunkt wird zusammen mit dem Namen aufgeführt`iot:Data-ATS`.

- AWS verwaltete Domäne

  Die Domain, die verwaltet AWS werden soll. Wenn Sie sich für eine AWS verwaltete Domain entscheiden, stellen Ihre Geräte eine Verbindung über einen Datenendpunkt her, der von bereitgestellt wird AWS. AWS verwaltet die Domain und die Zertifikate.

- Vom Kunden verwaltete Domain

  Die Domain, die Sie verwalten werden. Wird auch als benutzerdefinierte Domain bezeichnet. Wenn Sie sich für eine vom Kunden verwaltete Domain entscheiden, bedeutet dies, dass Ihre Geräte über einen benutzerdefinierten Domain-Datenendpunkt eine Verbindung herstellen. Sie verwalten die Domain und die Zertifikate. Mit der vom Kunden verwalteten Domain können Sie den Endpunkt URLs an Ihre Bedürfnisse anpassen. Sie können beispielsweise einen benutzerdefinierten Domainnamen (`your-domain-name.com`) verwenden oder bestimmte Zugriffsrichtlinien anwenden.

- Authentifizierungstyp

Der Authentifizierungstyp, mit dem Sie Ihre Geräte authentifizieren möchten, wenn Sie eine Verbindung herstellen AWS IoT Core. Beim Erstellen einer Domänenkonfiguration müssen Sie einen Authentifizierungstyp angeben. Weitere Informationen finden Sie unter ???.

- Anwendungsprotokoll

  Die Protokolle auf Anwendungsebene, mit denen Ihre Geräte eine Verbindung herstellen AWS IoT Core. Beim Erstellen einer Domänenkonfiguration müssen Sie ein Anwendungsprotokoll angeben. Weitere Informationen finden Sie unter ???.

Wichtige Hinweise

AWS IoT Core verwendet die TLSErweiterung „Servername Indication“ (SNI), um Domänenkonfigurationen anzuwenden. Beim Verbinden von Geräten mit können Clients die Erweiterung Server Name Indication (SNI) senden, die für Funktionen wie die Registrierung mehrerer Konten, konfigurierbare Endpunkte, benutzerdefinierte Domänen und VPC Endpunkte erforderlich ist. AWS IoT Core Sie müssen des Weiteren einen Servernamen übergeben, der mit dem Domänennamen identisch ist, den Sie in der Domänenkonfiguration angeben. Um diesen Dienst zu testen, verwenden Sie die Version v2 des AWS IoT Geräts in. SDKs GitHub

Wenn Sie in Ihrem mehrere Datenendpunkte erstellen AWS-Konto, teilen sich diese AWS IoT Core Ressourcen wie MQTT Themen, Geräteschatten und Regeln gemeinsam.

Wenn Sie die Serverzertifikate für die AWS IoT Core benutzerdefinierte Domänenkonfiguration bereitstellen, haben die Zertifikate maximal vier Domainnamen. Weitere Informationen finden Sie unter AWS IoT Core -Endpunkte und -Kontingente.

## AWS Verwaltete Domänen erstellen und konfigurieren

Sie erstellen einen konfigurierbaren Endpunkt in einer AWS verwalteten Domäne mithilfe von CreateDomainConfigurationAPI. Eine Domänenkonfiguration für eine AWS verwaltete Domäne besteht aus folgenden Komponenten:

- `domainConfigurationName`

  Ein benutzerdefinierter Name, der die Domänenkonfiguration identifiziert, und der Wert muss für Sie AWS-Region eindeutig sein. Sie können keine Domänenkonfigurationsnamen verwenden, die mit `IoT:` beginnen, da diese Standardendpunkten vorbehalten sind.

- `defaultAuthorizerName` (optional)

  Der Name des benutzerdefinierten Autorisierers, der am Endpunkt verwendet werden soll.

- `allowAuthorizerOverride` (optional)

  Ein boolescher Wert, der angibt, ob Geräte den Standardautorisierer überschreiben können, indem sie im Header der HTTP Anfrage einen anderen Autorisierer angeben. Dieser Wert ist erforderlich, wenn ein Wert für `defaultAuthorizerName` angegeben wird.

- `serviceType` (optional)

  Der Diensttyp, den der Endpunkt bereitstellt. AWS IoT Core unterstützt nur den `DATA` Diensttyp. Wenn Sie `DATA` angeben, gibt AWS IoT Core einen Endpunkt mit dem Endpunkttyp `iot:Data-ATS` zurück. Sie können keinen konfigurierbaren Endpunkt `iot:Data` (VeriSign) erstellen.

- `TlsConfig` (optional)

  Ein Objekt, das die TLS Konfiguration für eine Domäne angibt. Weitere Informationen finden Sie unter ???.

Der folgende AWS CLI Beispielbefehl erstellt eine Domänenkonfiguration für einen `Data` Endpunkt.

```
aws iot create-domain-configuration --domain-configuration-name
 "myDomainConfigurationName" --service-type "DATA"
```

Die Ausgabe des Befehls kann wie folgt aussehen.

```
{
    "domainConfigurationName": "myDomainConfigurationName",
    "domainConfigurationArn": "arn:aws:iot:us-east-1:123456789012:domainconfiguration/
myDomainConfigurationName/itihw"
}
```

## Vom Kunden verwaltete Domains erstellen und konfigurieren

Mit Domänenkonfigurationen können Sie einen benutzerdefinierten vollqualifizierten Domainnamen (FQDN) angeben, zu dem Sie eine Verbindung herstellen möchten AWS IoT Core. Die Verwendung von kundenverwalteten Domains (auch als benutzerdefinierte Domains bezeichnet) bietet viele Vorteile: Sie können Ihre eigene Domain oder die Ihres Unternehmens Kunden zu Branding-Zwecken zugänglich machen; Sie können Ihre eigene Domain einfach ändern, sodass sie auf einen neuen

Broker verweist; Sie können Multi-Tenancy unterstützen, um Kunden mit unterschiedlichen Domains innerhalb derselben zu bedienen AWS-Konto; und Sie können Ihre eigenen Serverzertifikatsdetails verwalten, z. B. die Root-Zertifizierungsstelle (CA), die zum Signieren des Zertifikats verwendet wurde, den Signaturalgorithmus, Tiefe der Zertifikatskette und der Lebenszyklus des Zertifikat.

Der Workflow zum Einrichten einer Domänenkonfiguration mit einer benutzerdefinierten Domäne besteht aus den folgenden drei Phasen.

1. Registrierung von Serverzertifikaten in AWS Certificate Manager
2. Erstellen einer Domänenkonfiguration
3. DNSDatensätze erstellen

### Registrierung von Serverzertifikaten im AWS Zertifikatsmanager

Bevor Sie eine Domänenkonfiguration mit einer benutzerdefinierten Domäne erstellen, müssen Sie die Serverzertifikatskette in AWS Certificate Manager (ACM) registrieren. Sie können die folgenden drei Serverzertifikattypen verwenden.

- In ACM generierte öffentliche Zertifikate
- Von einer öffentlichen Zertifizierungsstelle signierte externe Zertifikate
- Von einer privaten Zertifizierungsstelle signierte externe Zertifikate

> **Note**
>
> AWS IoT Core betrachtet ein Zertifikat als von einer öffentlichen Zertifizierungsstelle signiert, wenn es in Mozillas vertrauenswürdigem CA-Bundle enthalten ist.

#### Zertifikatanforderungen

Die Anforderungen für den Import von Zertifikaten in finden Sie unter Voraussetzungen für den Import von Zertifikaten inACM. Zusätzlich zu diesen Anforderungen fügt AWS IoT Core folgende Anforderungen hinzu.

- Das Leaf-Zertifikat muss die Erweiterung Extended Key Usage x509 v3 mit dem Wert serverAuth(TLSWeb Server Authentication) enthalten. Wenn Sie das Zertifikat von anfordernACM, wird diese Erweiterung automatisch hinzugefügt.

- Die maximale Tiefe der Zertifikatskette beträgt 5 Zertifikate.
- Die maximale Größe der Zertifikatskette beträgt 16 KB.
- Zu den unterstützten kryptografischen Algorithmen und Schlüsselgrößen gehören RSA 2048 Bit (RSA_2048) und ECDSA 256 Bit (EC_Prime256V1).

Verwenden eines Zertifikats für mehrere Domänen

Wenn Sie beabsichtigen, ein Zertifikat für mehrere Subdomänen zu verwenden, verwenden Sie eine Platzhalterdomäne im Feld Common Name (CN) oder Subject Alternative Names (). SAN Verwenden Sie zum Beispiel **`*.iot.example.com`** dev.iot.example.com, qa.iot.example.com und prod.iot.example.com. FQDNFür jede Domänenkonfiguration ist eine eigene Domänenkonfiguration erforderlich, aber mehrere Domänenkonfigurationen können denselben Platzhalterwert verwenden. Entweder der CN oder der SAN muss die Domäne abdeckenFQDN, die Sie als benutzerdefinierte Domäne verwenden möchten. Falls SANs vorhanden, wird der CN ignoriert und SAN muss die Domain abdeckenFQDN, die Sie als benutzerdefinierte Domain verwenden möchten. Hierbei kann es sich um eine exakte Übereinstimmung oder um eine Platzhalterübereinstimmung handeln. Nachdem ein Wildcard-Zertifikat validiert und für ein Konto registriert wurde, werden andere Konten in der Region daran gehindert, benutzerdefinierte Domänen zu erstellen, die sich mit dem Zertifikat überschneiden.

In den folgenden Abschnitten wird beschrieben, wie Sie die einzelnen Zertifikatstypen erhalten. Für jede Zertifikatsressource ist ein registrierter Amazon-Ressourcenname (ARN) erforderlichACM, den Sie bei der Erstellung Ihrer Domain-Konfiguration verwenden.

ACM-generierte öffentliche Zertifikate

Sie können ein öffentliches Zertifikat für Ihre benutzerdefinierte Domain generieren, indem Sie den RequestCertificateAPIverwenden. Wenn Sie auf diese Weise ein Zertifikat generieren, überprüft ACM Ihr Eigentum an der benutzerdefinierten Domäne. Weitere Informationen finden Sie unter Anfordern eines öffentlichen Zertifikats im AWS Certificate Manager -Benutzerhandbuch.

Von einer öffentlichen Zertifizierungsstelle signierte externe Zertifikate

Wenn Sie bereits über ein Serverzertifikat verfügen, das von einer öffentlichen Zertifizierungsstelle signiert ist (eine Zertifizierungsstelle, die im vertrauenswürdigen CA-Bundle von Mozilla enthalten ist), können Sie die Zertifikatskette direkt importieren, ACM indem Sie den ImportCertificateAPIverwenden. Weitere Informationen zu dieser Aufgabe und den Voraussetzungen und Anforderungen an das Zertifikatformat finden Sie unter Importieren von Zertifikaten.

Von einer privaten Zertifizierungsstelle signierte externe Zertifikate

Wenn Sie bereits über ein Serverzertifikat verfügen, das von einer privaten Zertifizierungsstelle signiert oder selbstsigniert ist, können Sie das Zertifikat zum Erstellen Ihrer Domänenkonfiguration verwenden. Sie müssen jedoch auch ein zusätzliches öffentliches Zertifikat in ACM erstellen, um den Besitz Ihrer Domäne zu überprüfen. Registrieren Sie dazu Ihre Serverzertifikatskette unter ACM Verwendung von. ImportCertificateAPI Weitere Informationen zu dieser Aufgabe und den Voraussetzungen und Anforderungen an das Zertifikatformat finden Sie unter Importieren von Zertifikaten.

Erstellen eines Validierungszertifikats

Nachdem Sie Ihr Zertifikat in importiert habenACM, generieren Sie mithilfe von ein öffentliches Zertifikat für Ihre benutzerdefinierte Domain RequestCertificateAPI. Wenn Sie auf diese Weise ein Zertifikat generieren, überprüft ACM Ihr Eigentum an der benutzerdefinierten Domäne. Weitere Informationen finden Sie unter Anfordern eines öffentlichen Zertifikats. Wenn Sie Ihre Domänenkonfiguration erstellen, verwenden Sie dieses öffentliche Zertifikat als Validierungszertifikat.

Erstellen einer Domänenkonfiguration

Sie erstellen einen konfigurierbaren Endpunkt in einer benutzerdefinierten Domain mithilfe von CreateDomainConfigurationAPI. Eine Domänenkonfiguration für eine benutzerdefinierte Domäne besteht aus folgenden Elementen:

- `domainConfigurationName`

  Ein benutzerdefinierter Name, der die Domänenkonfiguration identifiziert Domänenkonfigurationsnamen, die mit `IoT:` beginnen, sind für Standardendpunkte reserviert und können nicht verwendet werden. Außerdem muss dieser Wert für Sie eindeutig sein AWS-Region.
- `domainName`

  DerFQDN, mit dem Ihre Geräte eine Verbindung herstellen AWS IoT Core. AWS IoT Core nutzt die TLS Erweiterung „Servername Indication“ (SNI), um Domänenkonfigurationen anzuwenden. Geräte müssen diese Erweiterung verwenden, wenn sie eine Verbindung herstellen und einen Servernamen übergeben, der mit dem Domänennamen identisch ist, der in der Domänenkonfiguration angegeben ist.
- `serverCertificateArns`

  Die ARN der Serverzertifikatskette, bei ACM der Sie sich registriert haben. AWS IoT Core unterstützt derzeit nur ein Serverzertifikat.

- `validationCertificateArn`

  Das ARN des öffentlichen Zertifikats, das Sie generiert haben, ACM um die Inhaberschaft Ihrer benutzerdefinierten Domain zu bestätigen. Dieses Argument ist nicht erforderlich, wenn Sie ein öffentlich signiertes oder in ACM generiertes Serverzertifikat verwenden.
- `defaultAuthorizerName (optional)`

  Der Name des benutzerdefinierten Autorisierers, der am Endpunkt verwendet werden soll.
- `allowAuthorizerOverride`

  Ein boolescher Wert, der angibt, ob Geräte den Standardautorisierer überschreiben können, indem sie im HTTP Header der Anfrage einen anderen Autorisierer angeben. Dieser Wert ist erforderlich, wenn ein Wert für `defaultAuthorizerName` angegeben wird.
- `serviceType`

  AWS IoT Core unterstützt derzeit nur den Diensttyp. `DATA` Wenn Sie angeben`DATA`, wird ein Endpunkt mit dem Endpunkttyp AWS IoT zurückgegeben`iot:Data-ATS`.
- `TlsConfig` (optional)

  Ein Objekt, das die TLS Konfiguration für eine Domäne angibt. Weitere Informationen finden Sie unter ???.
- `serverCertificateConfig` (optional)

  Ein Objekt, das die Serverzertifikatkonfiguration für eine Domäne angibt. Weitere Informationen finden Sie unter ???.

Der folgende AWS CLI Befehl erstellt eine Domänenkonfiguration für iot.example.com.

```
aws iot create-domain-configuration --domain-configuration-name
 "myDomainConfigurationName" --service-type "DATA"
--domain-name "iot.example.com" --server-certificate-arns serverCertARN --validation-
certificate-arn validationCertArn
```

> **Note**
>
> Nachdem Sie Ihre Domänenkonfiguration erstellt haben, kann es bis zu 60 Minuten dauern, bis Ihre benutzerdefinierten Serverzertifikate AWS IoT Core bereitgestellt werden.

Weitere Informationen finden Sie unter ???.

DNSDatensätze erstellen

Nachdem Sie Ihre Serverzertifikatskette registriert und Ihre Domainkonfiguration erstellt haben, erstellen Sie einen DNS Datensatz, sodass Ihre benutzerdefinierte Domain auf eine AWS IoT Domain verweist. Dieser Datensatz muss auf einen AWS IoT Endpunkt vom Typ verweisen`iot:Data-ATS`. Sie können Ihren Endpunkt ermitteln, indem Sie den verwenden DescribeEndpointAPI.

Der folgende AWS CLI Befehl zeigt, wie Sie Ihren Endpunkt ermitteln.

```
aws iot describe-endpoint --endpoint-type iot:Data-ATS
```

Nachdem Sie Ihren `iot:Data-ATS` Endpunkt erhalten haben, erstellen Sie einen `CNAME` Datensatz von Ihrer benutzerdefinierten Domain zu diesem AWS IoT Endpunkt. Wenn Sie mehrere benutzerdefinierte Domains in derselben Domain erstellen AWS-Konto, geben Sie ihnen einen Alias für denselben `iot:Data-ATS` Endpunkt.

Fehlerbehebung

Wenn Sie Probleme haben, Geräte mit einer benutzerdefinierten Domain zu verbinden, stellen Sie sicher, dass diese Ihr Serverzertifikat akzeptiert und angewendet AWS IoT Core hat. Sie können überprüfen, ob Ihr Zertifikat akzeptiert AWS IoT Core wurde, indem Sie entweder die AWS IoT Core Konsole oder den verwenden AWS CLI.

Um die AWS IoT Core Konsole zu verwenden, navigieren Sie zur Seite mit den Domänenkonfigurationen und wählen Sie den Namen der Domänenkonfiguration aus. Überprüfen Sie im Abschnitt Serverzertifikatsdetails den Status und die Statusdetails. Wenn das Zertifikat ungültig ist, ersetzen Sie es durch ein Zertifikat, das die im vorherigen Abschnitt aufgeführten Zertifikatsanforderungen erfüllt. ACM Wenn das Zertifikat dasselbe hatARN, AWS IoT Core wird es automatisch abgeholt und beantragt.

Um den Status des Zertifikats mithilfe von zu überprüfen AWS CLI, rufen Sie den an DescribeDomainConfigurationAPIund geben Sie Ihren Domain-Konfigurationsnamen an.

> **Note**
>
> Wenn Ihr Zertifikat ungültig ist, AWS IoT Core wird weiterhin das letzte gültige Zertifikat ausgestellt.

Mit dem folgenden openssl-Befehl können Sie überprüfen, welches Zertifikat auf Ihrem Endpunkt zugestellt wird.

```
openssl s_client -connect custom-domain-name:8883 -showcerts -servername
custom-domain-name
```

## Verwalten von Domänenkonfigurationen

In diesem Thema werden wichtige Operationen behandelt, mit denen Sie Ihre Domänenkonfigurationsressourcen verwalten können. Sie können auch die Lebenszyklen vorhandener Konfigurationen mithilfe der folgenden Methoden verwaltenAPIs: ListDomainConfigurations, DescribeDomainConfigurationUpdateDomainConfiguration, und. DeleteDomainConfiguration

In diesem Thema:

- Anzeigen von Domänenkonfigurationen
- Aktualisieren von Domänenkonfigurationen
- Löschen von Domänenkonfigurationen
- Rotierende Zertifikate in benutzerdefinierten Domänen

### Anzeigen von Domänenkonfigurationen

Um eine paginierte Liste aller Domainkonfigurationen in Ihrem zurückzugeben AWS-Konto, verwenden Sie den. ListDomainConfigurationsAPI Sie können die Details einer bestimmten Domain-Konfiguration mit dem DescribeDomainConfigurationAPIeinsehen. Dies API verwendet einen einzelnen `domainConfigurationName` Parameter und gibt die Details der angegebenen Konfiguration zurück.

Beispiel

### Aktualisieren von Domänenkonfigurationen

Um den Status oder den benutzerdefinierten Authorizer Ihrer Domain-Konfiguration zu aktualisieren, verwenden Sie den UpdateDomainConfigurationAPI. Sie können den Status auf `ENABLED` oder `DISABLED` setzen. Wenn Sie die Domänenkonfiguration deaktivieren, erhalten Geräte, die mit dieser Domäne verbunden sind, einen Authentifizierungsfehler. Derzeit können Sie das Serverzertifikat in Ihrer Domänenkonfiguration nicht aktualisieren. Um das Zertifikat einer Domänenkonfiguration zu ändern, müssen Sie es löschen und neu erstellen.

Beispiel

Löschen von Domänenkonfigurationen

Bevor Sie eine Domainkonfiguration löschen, verwenden Sie den, UpdateDomainConfigurationAPIum den Status auf zu `DISABLED` setzen. Auf diese Weise vermeiden Sie ein versehentliches Löschen des Endpunkts. Nachdem Sie die Domänenkonfiguration deaktiviert haben, löschen Sie sie mit dem DeleteDomainConfigurationAPI. Sie müssen den `DISABLED` Status AWS-managed Domains für 7 Tage aktivieren, bevor Sie sie löschen können. Sie können benutzerdefinierte Domains in `DISABLED` den Status versetzen und sie dann sofort löschen.

Beispiel

Nachdem Sie eine Domänenkonfiguration gelöscht haben, wird das Serverzertifikat, das dieser benutzerdefinierten Domain zugeordnet ist, nicht AWS IoT Core mehr bereitgestellt.

Rotierende Zertifikate in benutzerdefinierten Domänen

Möglicherweise müssen Sie Ihr Serverzertifikat regelmäßig durch ein aktualisiertes Zertifikat ersetzen. Die Häufigkeit, mit der Sie dies tun müssen, ist von der Gültigkeitsdauer Ihres Zertifikats abhängig. Wenn Sie Ihr Serverzertifikat mithilfe von AWS Certificate Manager (ACM) generiert haben, können Sie festlegen, dass das Zertifikat automatisch verlängert wird. Wenn Ihr Zertifikat ACM erneuert AWS IoT Core wird, wird das neue Zertifikat automatisch übernommen. Sie müssen keine weiteren Aktionen ausführen. Wenn Sie Ihr Serverzertifikat aus einer anderen Quelle importiert haben, können Sie es rotieren lassen, indem Sie es erneut importieren. ACM Informationen zum erneuten Importieren von Zertifikaten finden Sie unter Zertifikat erneut importieren.

> **Note**
>
> AWS IoT Core nimmt Zertifikatsaktualisierungen nur unter den folgenden Bedingungen auf.
>
> - Das neue Zertifikat hat dasselbe ARN wie das alte.
> - Das neue Zertifikat hat denselben Signaturalgorithmus, denselben generischen Namen oder denselben alternativen Betreffnamen wie das alte.

## Konfiguration von TLS Einstellungen in Domänenkonfigurationen

AWS IoT Core bietet vordefinierte Sicherheitsrichtlinien, mit denen Sie Ihre Transport Layer Security (TLS) -Einstellungen für TLS1.2 und TLS1.3 in Domänenkonfigurationen anpassen können. Eine

Sicherheitsrichtlinie ist eine Kombination von TLS Protokollen und ihren Verschlüsselungen, die bei TLS Verhandlungen zwischen einem Client und einem Server die unterstützten Protokolle und Verschlüsselungen festlegen. Mit den unterstützten Sicherheitsrichtlinien können Sie die TLS Einstellungen Ihrer Geräte flexibler verwalten, beim Anschließen neuer Geräte die größtmöglichen up-to-date Sicherheitsmaßnahmen anwenden und für bestehende Geräte einheitliche TLS Konfigurationen beibehalten.

In der folgenden Tabelle werden die Sicherheitsrichtlinien, ihre TLS Versionen und die unterstützten Regionen beschrieben:

| Name der Sicherheitsrichtlinie | Unterstützt AWS-Regionen |
|---|---|
| oTSecurityIT-Richtlinie_ _1_3_2022_10 TLS13 | Alles AWS-Regionen |
| oTSecurityIT-Richtlinie_ _1_2_2022_10 TLS13 | Alles AWS-Regionen |
| oTSecurityIT-Richtlinie_ _1_2_2022_10 TLS12 | Alles AWS-Regionen |
| oTSecurityIT-Richtlinie_ _1_0_2016_01 TLS12 | AP-Ost-1, ap-northeast-2, ap-south-1, ap-southeast-2, ca-central-1, CN-Nord-1, CN-Nordwest-1, EU-Nord-1, EU-West-2, EU-West-3, me-south-1, sa-east-1, us-east-2, US-West-1 |
| l oTSecurity TLS12 Policy_ _1_0_2015_01 | ap-northeast-1, ap-southeast-1, eu-central-1, eu-west-1, us-east-1, us-west-2 |

Die Namen der Sicherheitsrichtlinien AWS IoT Core enthalten Versionsinformationen, die auf dem Jahr und dem Monat basieren, in dem sie veröffentlicht wurden. Wenn Sie eine neue Domänenkonfiguration erstellen, lautet die Standardeinstellung für die Sicherheitsrichtlinie `IoTSecurityPolicy_TLS13_1_2_2022_10`. Eine vollständige Tabelle der Sicherheitsrichtlinien mit Einzelheiten zu Protokollen, TCP Ports und Verschlüsselungen finden Sie unter Sicherheitsrichtlinien. AWS IoT Core unterstützt keine benutzerdefinierten Sicherheitsrichtlinien. Weitere Informationen finden Sie unter ???.

Um TLS Einstellungen in Domänenkonfigurationen zu konfigurieren, können Sie die AWS IoT Konsole oder die verwenden AWS CLI.

Inhalt


- Konfigurieren Sie TLS Einstellungen in Domänenkonfigurationen (Konsole)
- Konfigurieren Sie TLS Einstellungen in Domänenkonfigurationen (CLI)


## Konfigurieren Sie TLS Einstellungen in Domänenkonfigurationen (Konsole)

Um TLS Einstellungen mit der AWS IoT Konsole zu konfigurieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS IoT Konsole.
2. Gehen Sie wie folgt vor, um TLS Einstellungen zu konfigurieren, wenn Sie eine neue Domänenkonfiguration erstellen.
    1. Wählen Sie im linken Navigationsbereich Einstellungen und dann im Abschnitt Domänenkonfigurationen die Option Domänenkonfiguration erstellen.
    2. Wählen Sie auf der Seite Domänenkonfiguration erstellen im Abschnitt Benutzerdefinierte Domäneneinstellungen – optional unter Sicherheitsrichtlinie auswählen eine Sicherheitsrichtlinie.
    3. Folgen Sie dem Widget, und führen Sie die restlichen Schritte durch. Wählen Sie Domänenkonfiguration erstellen.
3. Gehen Sie folgendermaßen vor, um die TLS Einstellungen in einer vorhandenen Domänenkonfiguration zu aktualisieren.
    1. Wählen Sie im linken Navigationsbereich Einstellungen und dann unter Domänenkonfigurationen eine Domänenkonfiguration.
    2. Wählen Sie auf der Seite mit den Details zur Domänenkonfiguration die Option Bearbeiten. Wählen Sie dann im Abschnitt Benutzerdefinierte Domäneneinstellungen – optional unter Sicherheitsrichtlinie auswählen eine Sicherheitsrichtlinie.
    3. Wählen Sie Konfiguration aktualisieren.

Weitere Informationen finden Sie unter Eine Domänenkonfiguration erstellen und Domänenkonfigurationen verwalten.

Konfigurieren Sie TLS Einstellungen in Domänenkonfigurationen (CLI)

Sie können die update-domain-configurationCLIBefehle create-domain-configurationund verwenden, um Ihre TLS Einstellungen in Domänenkonfigurationen zu konfigurieren.

1. So geben Sie TLS Einstellungen mit dem create-domain-configurationCLIBefehl an:

```
aws iot create-domain-configuration \
    --domain-configuration-name domainConfigurationName \
    --tls-config securityPolicy=IoTSecurityPolicy_TLS13_1_2_2022_10
```

   Die Ausgabe dieses Befehls kann folgendermaßen aussehen:

```
{
"domainConfigurationName": "test",
"domainConfigurationArn": "arn:aws:iot:us-west-2:123456789012:domainconfiguration/
test/34ga9"
}
```

   Wenn Sie eine neue Domänenkonfiguration erstellen, ohne die Sicherheitsrichtlinie anzugeben, lautet der Standardwert: `IoTSecurityPolicy_TLS13_1_2_2022_10`.

2. Um TLS Einstellungen mit dem describe-domain-configurationCLIBefehl zu beschreiben:

```
aws iot describe-domain-configuration \
    --domain-configuration-name domainConfigurationName
```

   Dieser Befehl kann die Domänenkonfigurationsdetails zurückgeben, die TLS Einstellungen wie die folgenden enthalten:

```
{
 "tlsConfig": {
 "securityPolicy": "IoTSecurityPolicy_TLS13_1_2_2022_10"
 },
 "domainConfigurationStatus": "ENABLED",
 "serviceType": "DATA",
 "domainType": "AWS_MANAGED",
 "domainName": "d1234567890abcdefghij-ats.iot.us-west-2.amazonaws.com",
 "serverCertificates": [],
 "lastStatusChangeDate": 1678750928.997,
 "domainConfigurationName": "test",
```

```
 "domainConfigurationArn": "arn:aws:iot:us-west-2:123456789012:domainconfiguration/
test/34ga9"
}
```

3. So aktualisieren Sie die TLS Einstellungen mit dem update-domain-configurationCLIBefehl:

```
aws iot update-domain-configuration \
    --domain-configuration-name domainConfigurationName \
    --tls-config securityPolicy=IoTSecurityPolicy_TLS13_1_2_2022_10
```

   Die Ausgabe dieses Befehls kann folgendermaßen aussehen:

```
{
"domainConfigurationName": "test",
"domainConfigurationArn": "arn:aws:iot:us-west-2:123456789012:domainconfiguration/
test/34ga9"
}
```

4. Führen Sie den update-domain-configurationCLIBefehl aus, um die TLS Einstellungen für Ihren ATS Endpunkt zu aktualisieren. Der Domänenkonfigurationsname für Ihren ATS Endpunkt lautet`iot:Data-ATS`.

```
aws iot update-domain-configuration \
    --domain-configuration-name "iot:Data-ATS" \
    --tls-config securityPolicy=IoTSecurityPolicy_TLS13_1_2_2022_10
```

   Die Ausgabe dieses Befehls kann folgendermaßen aussehen:

```
{
"domainConfigurationName": "iot:Data-ATS",
"domainConfigurationArn": "arn:aws:iot:us-west-2:123456789012:domainconfiguration/
iot:Data-ATS"
}
```

Weitere Informationen finden Sie unter CreateDomainConfigurationund UpdateDomainConfigurationin der AWS APIReferenz.

# Konfiguration des Serverzertifikats für das OCSP Heften

AWS IoT Core unterstützt das Heften mit dem Online Certificate Status Protocol (OCSP) für Serverzertifikate, auch bekannt als Heften von Serverzertifikaten OCSP oder Heften. OCSP Dabei handelt es sich um einen Sicherheitsmechanismus, der verwendet wird, um den Sperrstatus des Serverzertifikats in einem Transport Layer Security () TLS -Handshake zu überprüfen. OCSPDurch Stapling In AWS IoT Core können Sie die Gültigkeit des Serverzertifikats Ihrer benutzerdefinierten Domain um eine zusätzliche Überprüfungsebene erweitern.

Sie können das OCSP Einheften von Serverzertifikaten aktivieren AWS IoT Core , um die Gültigkeit des Zertifikats zu überprüfen, indem Sie den Responder OCSP regelmäßig abfragen. Die Einstellung zum OCSP Heften ist Teil des Prozesses zum Erstellen oder Aktualisieren einer Domänenkonfiguration mit einer benutzerdefinierten Domäne. OCSPStapling überprüft kontinuierlich den Sperrstatus des Serverzertifikats. Auf diese Weise können Sie überprüfen, ob alle Zertifikate, die von der Zertifizierungsstelle gesperrt wurden, von den Clients, die eine Verbindung zu Ihren benutzerdefinierten Domänen herstellen, nicht mehr als vertrauenswürdig eingestuft werden. Weitere Informationen finden Sie unter ???.

Das OCSP Stapling von Serverzertifikaten ermöglicht die Überprüfung des Sperrstatus in Echtzeit, reduziert die mit der Überprüfung des Sperrstatus verbundene Latenz und verbessert den Datenschutz und die Zuverlässigkeit sicherer Verbindungen. Weitere Informationen zu den Vorteilen der Verwendung von OCSP Heften finden Sie unter. ???

> **Note**
>
> Diese Funktion ist in AWS GovCloud (US) Regions nicht verfügbar.

In diesem Thema:


- Was ist OCSP?
- Wie funktioniert OCSP Heften
- Serverzertifikat wird aktiviert in OCSP AWS IoT Core
- Konfiguration des Serverzertifikats OCSP für private Endpunkte in AWS IoT Core
- Wichtige Hinweise zur Verwendung von OCSP Serverzertifikaten AWS IoT Core
- Problembehandlung beim OCSP Einheften von Serverzertifikaten AWS IoT Core

### Was ist OCSP?

Das Online Certificate Status Protocol (OCSP) hilft bei der Bereitstellung des Sperrstatus eines Serverzertifikats für einen Transport Layer Security (TLS) -Handshake.

### Die wichtigsten Konzepte

Die folgenden Schlüsselkonzepte enthalten Einzelheiten zum Online Certificate Status Protocol (OCSP).

#### OCSP

OCSPwird verwendet, um den Sperrstatus des Zertifikats während des Transport Layer Security (TLS) -Handshakes zu überprüfen. OCSPermöglicht die Validierung von Zertifikaten in Echtzeit. Dadurch wird bestätigt, dass das Zertifikat seit seiner Ausstellung nicht gesperrt wurde oder abgelaufen ist. OCSPist im Vergleich zu herkömmlichen Zertifikatssperrlisten (CRLs) auch besser skalierbar. OCSPDie Antworten sind kleiner und können effizient generiert werden, sodass sie sich besser für große private Schlüsselinfrastrukturen (PKIs) eignen.

#### OCSPResponder

Ein OCSP Responder (auch als OCSP Server bezeichnet) empfängt und beantwortet OCSP Anfragen von Clients, die versuchen, den Sperrstatus von Zertifikaten zu überprüfen.

#### Clientseitig OCSP

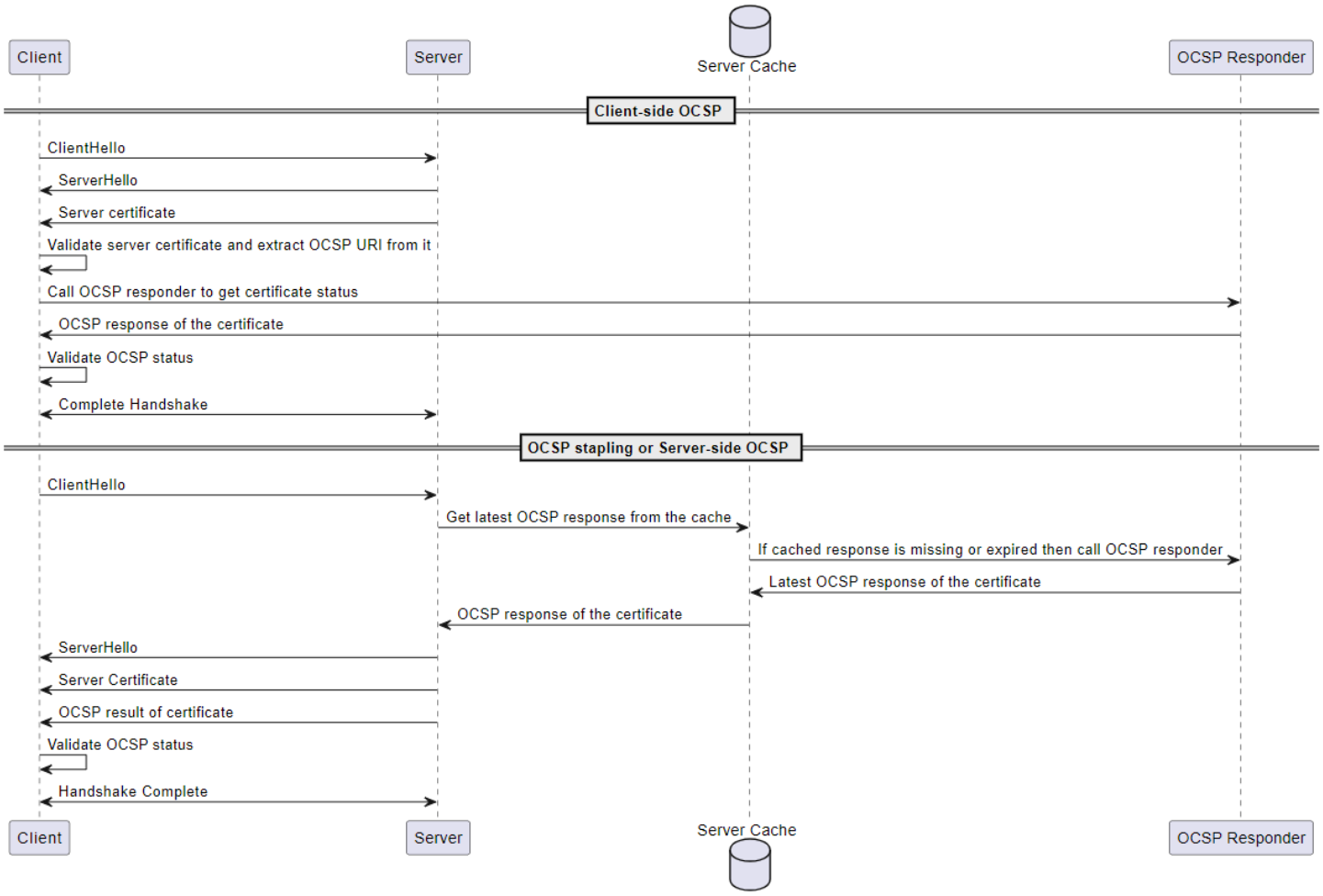
Auf der Clientseite kontaktiert der Client normalerweise einen OCSP ResponderOCSP, OCSP um den Sperrstatus des Zertifikats während des Handshakes zu überprüfen. TLS

#### Serverseitig OCSP

Serverseitig OCSP (auch bekannt als OCSP Stapling) ist der Server (und nicht der Client) in der Lage, die Anfrage an den Responder zu stellen. OCSP Der Server heftet die OCSP Antwort an das Zertifikat und sendet sie während des Handshakes an den Client zurück. TLS

### OCSPDiagramme

Das folgende Diagramm zeigt, wie clientseitig OCSP und OCSP serverseitig funktionieren.




Clientseitige OCSP

1. Der Client sendet eine `ClientHello` Nachricht, um den TLS Handshake mit dem Server zu initiieren.
2. Der Server empfängt die Nachricht und antwortet mit einer `ServerHello` Nachricht. Der Server sendet auch das Serverzertifikat an den Client.
3. Der Client validiert das Serverzertifikat und extrahiert ein Zertifikat OCSP URI daraus.
4. Der Client sendet eine Anfrage zur Überprüfung des Zertifikatswiderrufs an den OCSP Responder.
5. Der OCSP Responder sendet eine OCSP Antwort.
6. Der Client validiert den Zertifikatsstatus anhand der OCSP Antwort.
7. Der TLS Handshake ist abgeschlossen.

Serverseitig OCSP

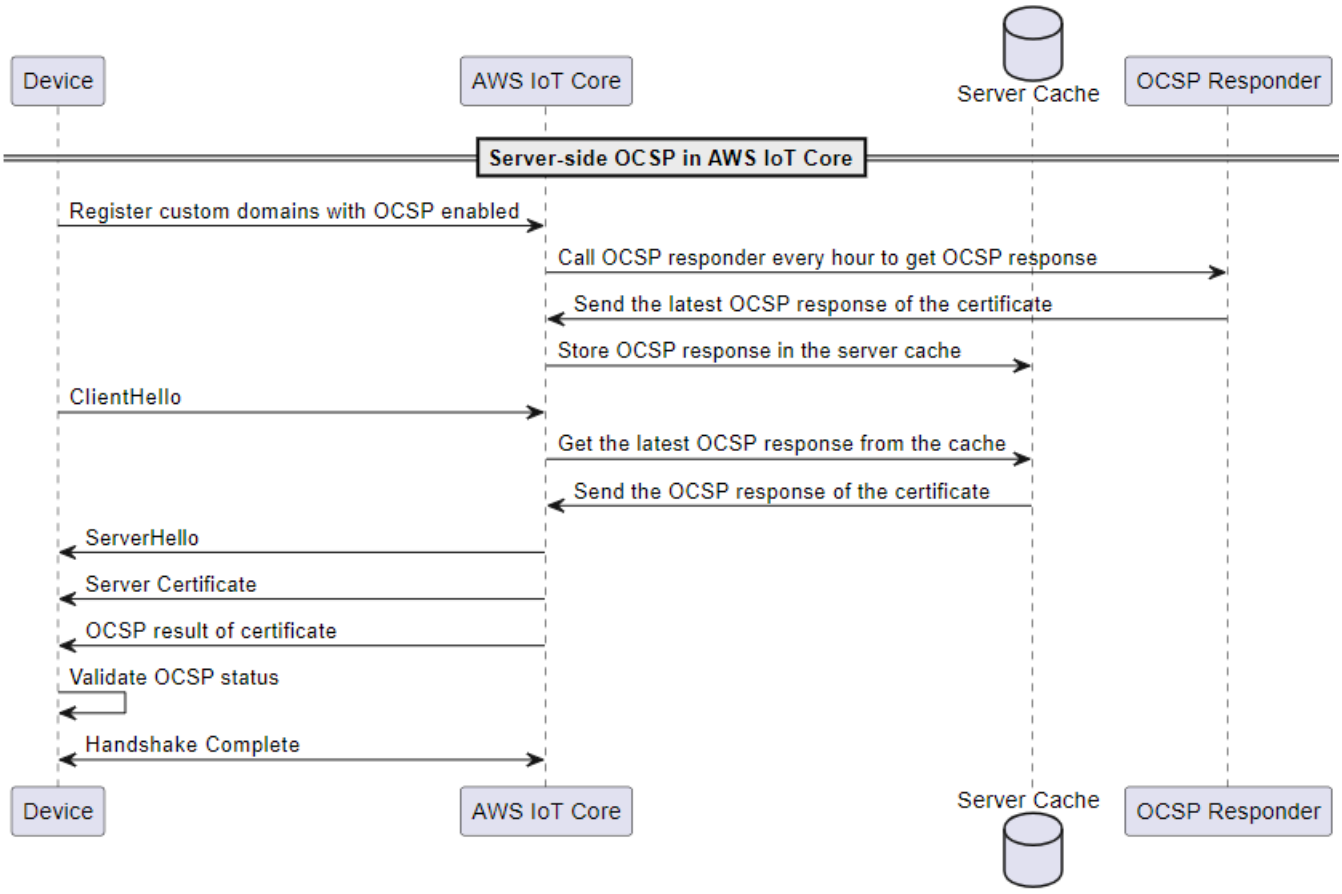
1. Der Client sendet eine `ClientHello` Nachricht, um den TLS Handshake mit dem Server zu initiieren.
2. Der Server empfängt die Nachricht und erhält die letzte zwischengespeicherte AntwortOCSP. Wenn die zwischengespeicherte Antwort fehlt oder abgelaufen ist, ruft der Server den OCSP Responder auf, um den Status des Zertifikats abzufragen.
3. Der OCSP Responder sendet eine OCSP Antwort an den Server.
4. Der Server sendet eine `ServerHello` Nachricht. Der Server sendet auch das Serverzertifikat und den Zertifikatsstatus an den Client.
5. Der Client validiert den OCSP Zertifikatsstatus.
6. Der TLS Handshake ist abgeschlossen.

Wie funktioniert OCSP Heften

OCSPDas Heften wird während des TLS Handshakes zwischen dem Client und dem Server verwendet, um den Sperrstatus des Serverzertifikats zu überprüfen. Der Server stellt die OCSP Anfrage an den OCSP Responder und heftet die OCSP Antworten auf die an den Client zurückgegebenen Zertifikate. Wenn der Server die Anfrage an den OCSP Responder stellt, können die Antworten zwischengespeichert und dann für viele Clients mehrfach verwendet werden.

So funktioniert OCSP Heften in AWS IoT Core

Das folgende Diagramm zeigt, wie serverseitiges OCSP Heften in funktioniert. AWS IoT Core




1. Das Gerät muss bei benutzerdefinierten Domänen registriert sein, wobei OCSP Stapling aktiviert ist.
2. AWS IoT Core ruft jede Stunde den OCSP Responder an, um den Status des Zertifikats abzurufen.
3. Der OCSP Responder empfängt die Anfrage, sendet die neueste OCSP Antwort und speichert die Antwort im CacheOCSP.
4. Das Gerät sendet eine `ClientHello` Nachricht, mit der der TLS Handshake initiiert werden soll. AWS IoT Core
5. AWS IoT Core ruft die neueste OCSP Antwort vom Server-Cache ab, der mit einer OCSP Antwort des Zertifikats antwortet.
6. Der Server sendet eine `ServerHello` Nachricht an das Gerät. Der Server sendet auch das Serverzertifikat und den Zertifikatsstatus an den Client.
7. Das Gerät validiert den OCSP Zertifikatsstatus.
8. Der TLS Handshake ist abgeschlossen.

Vorteile der Verwendung von OCSP Heftklammern im Vergleich zu Schecks auf Kundenseite OCSP

Das OCSP Heften von Serverzertifikaten bietet unter anderem folgende Vorteile:

Verbesserter Datenschutz

Ohne OCSP Heften kann das Gerät des Kunden Informationen an Dritte weitergeben, wodurch möglicherweise OCSP die Privatsphäre der Benutzer gefährdet wird. OCSPStapling behebt dieses Problem, indem der Server die OCSP Antwort erhält und sie direkt an den Client weiterleitet.

Verbesserte Zuverlässigkeit

OCSPDurch Stapling kann die Zuverlässigkeit sicherer Verbindungen verbessert werden, da dadurch das Risiko von OCSP Serverausfällen verringert wird. Wenn OCSP Antworten geheftet werden, fügt der Server dem Zertifikat die neueste Antwort bei. Auf diese Weise haben Clients auch dann Zugriff auf den Sperrstatus, wenn OCSP der Responder vorübergehend nicht verfügbar ist. OCSPStapling trägt dazu bei, diese Probleme zu beheben, da der Server regelmäßig OCSP Antworten abruft und die zwischengespeicherten Antworten in den Handshake aufnimmt. TLS Dadurch wird die Abhängigkeit von der Verfügbarkeit von Respondern in Echtzeit verringert. OCSP

Geringere Serverlast

OCSPStapling entlastet den Server bei der Beantwortung von OCSP Anfragen von OCSP Respondern. Dies kann dazu beitragen, die Last gleichmäßiger zu verteilen, wodurch der Prozess der Zertifikatsvalidierung effizienter und skalierbarer wird.

Reduzierte Latenz

OCSPStapling reduziert die Latenz, die mit der Überprüfung des Sperrstatus eines Zertifikats während des TLS Handshakes verbunden ist. Anstatt dass der Client einen OCSP Server separat abfragen muss, sendet der Server die Anfrage und hängt die OCSP Antwort während des Handshakes mit dem Serverzertifikat an.

Serverzertifikat wird aktiviert in OCSP AWS IoT Core

Um das OCSP Einheften von Serverzertifikaten zu aktivieren AWS IoT Core, erstellen Sie eine Domänenkonfiguration für eine benutzerdefinierte Domäne oder aktualisieren Sie eine bestehende benutzerdefinierte Domänenkonfiguration. Allgemeine Informationen zum Erstellen einer Domänenkonfiguration mit einer benutzerdefinierten Domäne finden Sie unter???.

Verwenden Sie die folgenden Anweisungen, um das OCSP Serverheften mithilfe von AWS Management Console oder AWS CLI zu aktivieren.

Konsole

So aktivieren Sie das OCSP Heften von Serverzertifikaten mithilfe der AWS IoT Konsole:

1. Wählen Sie im Navigationsmenü Einstellungen und dann Domainkonfiguration erstellen aus, oder wählen Sie eine bestehende Domainkonfiguration für eine benutzerdefinierte Domain aus.
2. Wenn Sie sich im vorherigen Schritt dafür entschieden haben, eine neue Domain-Konfiguration zu erstellen, wird die Seite Domain-Konfiguration erstellen angezeigt. Wählen Sie im Abschnitt Eigenschaften der Domänenkonfiguration die Option Benutzerdefinierte Domäne aus. Geben Sie die Informationen ein, um eine Domänenkonfiguration zu erstellen.

   Wenn Sie eine bestehende Domainkonfiguration für eine benutzerdefinierte Domain aktualisieren möchten, wird die Seite mit den Details zur Domain-Konfiguration angezeigt. Wählen Sie Edit (Bearbeiten) aus.
3. Um das OCSP Serverstapling zu aktivieren, wählen Sie im Unterabschnitt Serverzertifikatkonfigurationen die Option OCSP Serverzertifikatstapling aktivieren aus.
4. Wählen Sie Domänenkonfiguration erstellen oder Domänenkonfiguration aktualisieren aus.

AWS CLI

Um das OCSP Heften von Serverzertifikaten zu aktivieren, verwenden Sie AWS CLI:

1. Wenn Sie eine neue Domänenkonfiguration für eine benutzerdefinierte Domäne erstellen, kann der Befehl zum Aktivieren der OCSP Serverstapelung wie folgt aussehen:

```
aws iot create-domain-configuration --domain-configuration-name
 "myDomainConfigurationName" \
        --server-certificate-arns arn:aws:iot:us-
east-1:123456789012:cert/
f8c1e5480266caef0fdb1bf97dc1c82d7ba2d3e2642c5f25f5ba364fc6b79ba3 \
        --server-certificate-config "enableOCSPCheck=true|false"
```

2. Wenn Sie eine bestehende Domänenkonfiguration für eine benutzerdefinierte Domain aktualisieren, kann der Befehl zum Aktivieren des OCSP Serverstaplings wie folgt aussehen:

```
aws iot update-domain-configuration --domain-configuration-name
 "myDomainConfigurationName" \
```

```
        --server-certificate-arns arn:aws:iot:us-
east-1:123456789012:cert/
f8c1e5480266caef0fdb1bf97dc1c82d7ba2d3e2642c5f25f5ba364fc6b79ba3 \
        --server-certificate-config "enableOCSPCheck=true|false"
```

Weitere Informationen finden Sie in CreateDomainConfigurationund UpdateDomainConfigurationaus der AWS IoT API Referenz.

Konfiguration des Serverzertifikats OCSP für private Endpunkte in AWS IoT Core

OCSPMit for private Endpoints können Sie Ihre privaten OCSP Ressourcen innerhalb Ihrer Amazon Virtual Private Cloud (AmazonVPC) für den AWS IoT Core Betrieb nutzen. Der Prozess beinhaltet die Einrichtung einer Lambda-Funktion, die als OCSP Responder fungiert. Die Lambda-Funktion verwendet möglicherweise Ihre privaten OCSP Ressourcen, um OCSP Antworten zu erstellen, die verwendet AWS IoT Core werden.

Lambda-Funktion

Bevor Sie einen Server OCSP für einen privaten Endpunkt konfigurieren, erstellen Sie eine Lambda-Funktion, die als Request for Comments (RFC) -kompatibler 6960-kompatibler Online Certificate Status Protocol (OCSP) -Responder fungiert und grundlegende Antworten unterstützt. OCSP Die Lambda-Funktion akzeptiert eine Base64-Kodierung der OCSP Anfrage im Format Distinguished Encoding Rules ()DER. Die Antwort der Lambda-Funktion ist ebenfalls eine Base64-kodierte OCSP Antwort im Format. DER Die Antwortgröße darf 4 Kilobyte (KiB) nicht überschreiten. Die Lambda-Funktion muss sich in derselben AWS-Konto und AWS-Region wie die Domänenkonfiguration befinden. Im Folgenden finden Sie Beispiele für Lambda-Funktionen.

Beispiele für Lambda-Funktionen

JavaScript

```
import * as pkijs from 'pkijs';
console.log('Loading function');

export const handler = async (event, context) => {
    const requestBytes = decodeBase64(event);
    const ocspRequest = pkijs.OCSPRequest.fromBER(requestBytes);

    console.log("Here is a better look at the OCSP request");
    console.log(ocspRequest.toJSON());
```

```
    const ocspResponse = getOcspResponse();

    console.log("Here is a better look at the OCSP response");
    console.log(ocspResponse.toJSON());

   const responseBytes = ocspResponse.toSchema().toBER();
   return encodeBase64(responseBytes);
};

function getOcspResponse() {
    const responseString = "MIIC/
woBAKCCAvgwggL0BgkrBgEFBQcwAQEEggLlMIIC4TCByqFkMGIxJzAlBgNVBAoMHlJpY2hhcmQncyBEaXNjb3VudCBMY
p5w7WOtPjp3otNtVgIBAYAAGA8yMDI0MDQyMzE4NTMyNVowDQYJKoZIhvcNAQELBQADggIBAJFRyjDAHfazNejo704Ra
+s82R1spDarr3k7Pzkod9jJhwsZ2YgushlS4Npfe4lHCdwFyZR75WXrW55aXFddy03KLz01ZLNYyxkleW3f5dgrUcRU3
DEBiyS7ZsyhKo6igWU/SY7YMSKgwBvFsqSDcOa/hRYQkxWKWJ19gcz8CIkWN7NvfIxCs6VrAdzEJwmE7y3v
+jdfhxW9JmI4xStE4K0tAR9vVOOfKs7NvxXj7oc9pCSG60xl96kaEE6PaY1YsfNTsKQ7pyCJ0s7/2q
+ieZ4AtNyzw1XBadPzPJNv6E0LvI24yQZqN5wACvtut5prMMRxAHbOy
+abLZR58wloFSELtGJ7UD96LFv1GgtC5s
+2QlzPc4bEEof7Lo1EISt3j2ibNch8LxhqTQ4ufrbhsMkpSOTFYEJVMJF6aKj/OGXBUUqgc0Jx6jjJXNQd
+l5KCY9pQFeb/wVUYC6mYqZOkNNMMJxPbHHbFnqb68yO+g5BE9011N44YXoPVJYoXxBLFX+OpRu9cqPkT9/
vlkKd+SYXQknwZ81agKzhf1HsBKabtJwNVMlBKaI8g5UGa7Bxi6ewH3ezdWiERRUK7F56OM53wto/";
    const responseBytes = decodeBase64(responseString);
    return pkijs.OCSPResponse.fromBER(responseBytes);
}

function decodeBase64(input) {
    const binaryString = atob(input);

    const byteArray = new Uint8Array(binaryString.length);
    for (var i = 0; i < binaryString.length; i++) {
        byteArray[i] = binaryString.charCodeAt(i);
    }

    return byteArray.buffer;
}

function encodeBase64(buffer) {
    var binary = '';
    const bytes = new Uint8Array( buffer );
    const len = bytes.byteLength;

    for (var i = 0; i < len; i++) {
        binary += String.fromCharCode( bytes[ i ] );
```

```
    }

    return btoa(binary);
}
```

Java

```
package com.example.ocsp.responder;
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import org.bouncycastle.cert.ocsp.OCSPReq;
import org.bouncycastle.cert.ocsp.OCSPResp;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.util.Base64;

public class LambdaResponderApplication implements RequestHandler<String, String> {
    @Override
    public String handleRequest(final String input, final Context context) {
        LambdaLogger logger = context.getLogger();

        byte[] decodedInput = Base64.getDecoder().decode(input);

        OCSPReq req;
        try {
            req = new OCSPReq(decodedInput);
        } catch (IOException e) {
            logger.log("Got an IOException creating the OCSP request: " +
 e.getMessage());
            throw new RuntimeException(e);
        }

        try {
            OCSPResp response = businessLogic.getMyResponse();
            String toReturn =
 Base64.getEncoder().encodeToString(response.getEncoded());
            return toReturn;
        } catch (Exception e) {
            logger.log("Got an exception creating the response: " + e.getMessage());
            return "";
        }
```

```
    }
}
```

Autorisieren AWS IoT zum Aufrufen Ihrer Lambda-Funktion

Bei der Erstellung der Domänenkonfiguration mit einem OCSP Lambda-Responder müssen Sie die AWS IoT Erlaubnis erteilen, die Lambda-Funktion aufzurufen, nachdem die Funktion erstellt wurde. Um die Berechtigung zu erteilen, können Sie den Befehl add-permission verwenden. CLI

Erteilen Sie Ihrer Lambda-Funktion die Erlaubnis mit dem AWS CLI

1. Geben Sie nach der Eingabe Ihrer Werte den folgenden Befehl ein. Beachten Sie, dass der Wert `statement-id` eindeutig sein muss. *Id-1234*Ersetzen Sie es durch den exakten Wert, den Sie haben, andernfalls wird möglicherweise eine `ResourceConflictException` Fehlermeldung angezeigt.

   ```
   aws lambda add-permission  \
   --function-name "ocsp-function" \
   --principal "iot.amazonaws.com" \
   --action "lambda:InvokeFunction" \
   --statement-id "Id-1234" \
   --source-arn arn:aws:iot:us-east-1:123456789012:domainconfiguration/<domain-config-name>/*
   --source-account 123456789012
   ```

   Die IoT-Domänenkonfiguration ARNs folgt dem folgenden Muster. Das vom Dienst generierte Suffix wird vor der Erstellung nicht bekannt sein, daher müssen Sie das Suffix durch ein ersetzen. * Sie können die Berechtigung aktualisieren, sobald die Domänenkonfiguration erstellt wurde und die genaue ARN Konfiguration bekannt ist.

   `arn:`*`aws`*`:iot:`*`use-east-1:123456789012`*`:domainconfiguration/`*`domain-config-name/service-generated-suffix`*

2. Wenn der Befehl erfolgreich ist, gibt er eine Berechtigungsanweisung zurück, wie in diesem Beispiel. Sie können mit dem nächsten Abschnitt fortfahren, um OCSP Stapling für private Endgeräte zu konfigurieren.

   ```
   {
       "Statement": "{\"Sid\":\"Id-1234\",\"Effect\":\"Allow\",\"Principal
   \":{\"Service\":\"iot.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction
   ```

```
\",\"Resource\":\"arn:aws:lambda:us-east-1:123456789012:function:ocsp-
function\",\"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":\"arn:aws:iot:us-
east-1:123456789012:domainconfiguration/domain-config-name/*\"}}}"
}
```

Wenn der Befehl nicht erfolgreich ist, wird ein Fehler zurückgegeben, wie in diesem Beispiel. Sie müssen den Fehler überprüfen und korrigieren, bevor Sie fortfahren können.

```
An error occurred (AccessDeniedException) when calling the AddPermission operation:
 User: arn:aws:iam::57EXAMPLE833:user/EXAMPLE-1 is not authorized to perform:
 lambda:AddPer
mission on resource: arn:aws:lambda:us-east-1:123456789012:function:ocsp-function
```

### OCSPServerstapling für private Endgeräte konfigurieren

#### Konsole

So konfigurieren Sie das OCSP Stapling von Serverzertifikaten mithilfe der Konsole: AWS IoT

1. Wählen Sie im Navigationsmenü Einstellungen und dann Domainkonfiguration erstellen aus, oder wählen Sie eine bestehende Domainkonfiguration für eine benutzerdefinierte Domain aus.
2. Wenn Sie sich im vorherigen Schritt dafür entschieden haben, eine neue Domain-Konfiguration zu erstellen, wird die Seite Domain-Konfiguration erstellen angezeigt. Wählen Sie im Abschnitt Eigenschaften der Domänenkonfiguration die Option Benutzerdefinierte Domäne aus. Geben Sie die Informationen ein, um eine Domänenkonfiguration zu erstellen.

   Wenn Sie eine bestehende Domainkonfiguration für eine benutzerdefinierte Domain aktualisieren möchten, wird die Seite mit den Details zur Domain-Konfiguration angezeigt. Wählen Sie Edit (Bearbeiten) aus.
3. Um das OCSP Serverstapling zu aktivieren, wählen Sie im Unterabschnitt Serverzertifikatkonfigurationen die Option OCSP Serverzertifikatstapling aktivieren aus.
4. Wählen Sie Domänenkonfiguration erstellen oder Domänenkonfiguration aktualisieren aus.

AWS CLI

So konfigurieren Sie das OCSP Stapling von Serverzertifikaten mit AWS CLI:

1. Wenn Sie eine neue Domänenkonfiguration für eine benutzerdefinierte Domäne erstellen, kann der Befehl zur Konfiguration des Serverzertifikats OCSP für private Endpunkte wie folgt aussehen:

```
aws iot create-domain-configuration --domain-configuration-name
 "myDomainConfigurationName" \
        --server-certificate-arns arn:aws:iot:us-
east-1:123456789012:cert/
f8c1e5480266caef0fdb1bf97dc1c82d7ba2d3e2642c5f25f5ba364fc6b79ba3 \
        --server-certificate-config "enableOCSPCheck=true,
 ocspAuthorizedResponderArn=arn:aws:acm:us-
east-1:123456789012:certificate/certificate_ID, ocspLambdaArn=arn:aws:lambda:us-
east-1:123456789012:function:my-function"
```

2. Wenn Sie eine bestehende Domänenkonfiguration für eine benutzerdefinierte Domain aktualisieren, kann der Befehl zum Konfigurieren des Serverzertifikats OCSP für private Endpunkte wie folgt aussehen:

```
aws iot update-domain-configuration --domain-configuration-name
 "myDomainConfigurationName" \
        --server-certificate-arns arn:aws:iot:us-
east-1:123456789012:cert/
f8c1e5480266caef0fdb1bf97dc1c82d7ba2d3e2642c5f25f5ba364fc6b79ba3 \
        --server-certificate-config "enableOCSPCheck=true,
 ocspAuthorizedResponderArn=arn:aws:acm:us-
east-1:123456789012:certificate/certificate_ID, ocspLambdaArn=arn:aws:lambda:us-
east-1:123456789012:function:my-function"
```

enableOCSPCheck

Dies ist ein boolescher Wert, der angibt, ob die OCSP Server-Stapling-Prüfung aktiviert ist oder nicht. Um das OCSP Heften von Serverzertifikaten zu aktivieren, muss dieser Wert wahr sein.

ocspAuthorizedResponderArn

Dies ist ein Zeichenkettenwert des Amazon-Ressourcennamens (ARN) für ein in AWS Certificate Manager (ACM) gespeichertes X.509-Zertifikat. Falls angegeben, AWS IoT Core wird dieses

Zertifikat verwendet, um die Signatur der erhaltenen OCSP Antwort zu validieren. Falls nicht angegeben, AWS IoT Core wird das ausstellende Zertifikat verwendet, um die Antworten zu validieren. Das Zertifikat muss sich in derselben AWS-Konto und AWS-Region wie die Domänenkonfiguration befinden. Weitere Informationen zur Registrierung Ihres autorisierten Responder-Zertifikats finden Sie unter Zertifikate importieren in AWS Certificate Manager.

ocspLambdaArn

Dies ist ein Zeichenkettenwert des Amazon-Ressourcennamens (ARN) für eine Lambda-Funktion, die als 6960-kompatibler () -Responder mit Request for Comments (RFCOCSP) fungiert und grundlegende Antworten unterstützt. OCSP Die Lambda-Funktion akzeptiert eine Base64-Kodierung der OCSP Anfrage, die mit dem Format codiert ist. DER Die Antwort der Lambda-Funktion ist ebenfalls eine Base64-kodierte OCSP Antwort im Format. DER Die Antwortgröße darf 4 Kilobyte (KiB) nicht überschreiten. Die Lambda-Funktion muss sich in derselben AWS-Konto und AWS-Region wie die Domänenkonfiguration befinden.

Weitere Informationen finden Sie in CreateDomainConfigurationund UpdateDomainConfigurationaus der AWS IoT API Referenz.

Wichtige Hinweise zur Verwendung von OCSP Serverzertifikaten AWS IoT Core

Beachten Sie bei der Verwendung von Serverzertifikaten OCSP in AWS IoT Core Folgendes:

1. AWS IoT Core unterstützt nur die OCSP Responder, die über öffentliche IPv4 Adressen erreichbar sind.
2. Die OCSP Heftfunktion in unterstützt AWS IoT Core keine autorisierten Responder. Alle OCSP Antworten müssen von der Zertifizierungsstelle signiert werden, die das Zertifikat signiert hat, und die Zertifizierungsstelle muss Teil der Zertifikatskette der benutzerdefinierten Domäne sein.
3. Die OCSP Heftfunktion in unterstützt AWS IoT Core keine benutzerdefinierten Domänen, die mit selbstsignierten Zertifikaten erstellt wurden.
4. AWS IoT Core ruft jede Stunde einen OCSP Responder an und speichert die Antwort im Cache. Schlägt der Anruf beim Responder fehl, AWS IoT Core wird die letzte gültige Antwort gespeichert.
5. Wenn sie nicht mehr gültig `nextUpdateTime` ist, AWS IoT Core wird die Antwort aus dem Cache entfernt, und TLS Handshake enthält die OCSP Antwortdaten erst beim nächsten erfolgreichen Anruf an den Responder. OCSP Dies kann passieren, wenn die zwischengespeicherte Antwort abgelaufen ist, bevor der Server eine gültige Antwort vom Responder erhält. OCSP Der Wert von `nextUpdateTime` deutet darauf hin, dass die OCSP Antwort bis zu diesem Zeitpunkt gültig sein wird. Mehr über `nextUpdateTime` erfahren Sie unter ???.

6. Manchmal kann die OCSP Antwort AWS IoT Core nicht empfangen werden oder die vorhandene OCSP Antwort wird entfernt, weil sie abgelaufen ist. In solchen Situationen AWS IoT Core wird weiterhin das von der benutzerdefinierten Domäne bereitgestellte Serverzertifikat ohne OCSP Antwort verwendet.
7. Die Größe der OCSP Antwort darf 4 KiB nicht überschreiten.

Problembehandlung beim OCSP Einheften von Serverzertifikaten AWS IoT Core

AWS IoT Core gibt die `RetrieveOCSPStapleData.Success` Metrik und die `RetrieveOCSPStapleData` Protokolleinträge an aus. CloudWatch Die Metrik und die Protokolleinträge können dabei helfen, Probleme im Zusammenhang mit dem Abrufen von OCSP Antworten zu erkennen. Weitere Informationen erhalten Sie unter ??? und ???.

# Connect zu AWS IoT FIPS-Endpunkten her

AWS IoT stellt Endgeräte bereit, die den Federal Information Processing Standard (FIPS) 140-2 unterstützen. FIPS-konforme Endgeräte unterscheiden sich von Standardendpunkten. AWS Für eine FIPS-konforme Interaktion mit dem AWS IoT müssen Sie die nachstehend beschriebenen Endpunkte mit Ihrem FIPS-kompatiblen Client verwenden. Die AWS IoT Konsole ist nicht FIPS-konform.

In den folgenden Abschnitten wird beschrieben, wie Sie mithilfe der REST-API, eines SDK oder der auf die FIPS-kompatiblen AWS IoT Endpunkte zugreifen. AWS CLI

Themen

- Endpunkte von AWS IoT Core – Steuerebene
- Endpunkte von AWS IoT Core – Datenebene
- AWS IoT Core- Endpunkte des Anmeldeinformationsanbieters
- Endpunkte von AWS IoT Device Management – Auftragsdaten
- Endpunkte von AWS IoT Device Management – Fleet Hub
- Endpunkte AWS IoT Device Management – Secure Tunneling

## Endpunkte von AWS IoT Core – Steuerebene

Die FIPS-konformen AWS IoT Core – Steuerebene-Endpunkte, die die AWS IoT-Operationen unterstützen und ihre zugehörigen CLI-Befehle sind unter FIPS-Endpunkte nach Dienst aufgeführt.

Suchen Sie unter FIPS-Endpunkte nach Dienst nach dem Dienst AWS IoT Core –Steuerebene und suchen Sie nach dem Endpunkt für Ihre AWS-Region.

Um den FIPS-konformen Endpunkt beim Zugriff auf die AWS IoTOperationen zu verwenden, verwenden Sie das AWS SDK oder die REST-API mit dem Endpunkt, der für Sie geeignet ist. AWS-Region

Um den FIPS-konformen Endpunkt bei der Ausführung von --endpoint CLI-Befehlen zu verwenden, fügen Sie dem Befehl den Parameter aws iot mit dem entsprechenden Endpunkt für Ihre AWS-Region hinzu.

## Endpunkte von AWS IoT Core – Datenebene

Die FIPS-konformen Endpunkte von AWS IoT Core – Datenebene sind unter FIPS-Endpunkte nach Dienst aufgeführt. Suchen Sie unter FIPS-Endpunkte nach Dienst nach dem Dienst AWS IoT Core – Datenebene und suchen Sie nach dem Endpunkt für Ihre AWS-Region.

Sie können den FIPS-kompatiblen Endpunkt für Ihre Verbindung AWS-Region mit einem FIPS-kompatiblen Client verwenden, indem Sie das AWS IoT Geräte-SDK verwenden und den Endpunkt für die Verbindungsfunktion des SDK anstelle des Standardendpunkts Ihres Kontos — der Datenebene AWS IoT Core— angeben. Die Verbindungsfunktion ist spezifisch für das AWS IoT Geräte-SDK. Ein Beispiel für eine Verbindungsfunktion finden Sie unter der Verbindungsfunktion im AWS IoT Geräte-SDK für Python.

> **Note**
>
> AWS IoT unterstützt keine AWS-Konto spezifischen AWS IoT Core Datenebenen-Endpunkte, die FIPS-konform sind. Servicefunktionen, die einen AWS-Konto spezifischen Endpunkt in der Server Name Indication (SNI) erfordern, können nicht verwendet werden. FIPS-konforme Endpunkte von AWS IoT Core – Datenebene können keine Registrierungszertifikate für mehrere Konten, benutzerdefinierte Domänen, benutzerdefinierte Autorisierer und konfigurierbare Endpunkte (einschließlich unterstützter TLS-Richtlinien) unterstützen.

## AWS IoT Core- Endpunkte des Anmeldeinformationsanbieters

Die FIPS-konformen Endpunkte des AWS IoT Core Anmeldeinformationsanbieters sind unter FIPS-Endpunkte nach Dienst aufgeführt. Suchen Sie in FIPS Endpoints by Service nach dem Dienst AWS IoT Core - Credential Provider und suchen Sie den Endpunkt für Ihren. AWS-Region

> **Note**
>
> AWS IoT unterstützt keine AWS-Konto FIPS-konformen Endpunkte eines bestimmten AWS IoT Core Anmeldeinformationsanbieters. Dienstfunktionen, die einen AWS-Konto spezifischen Endpunkt im Server Name Indication (SNI) erfordern, können nicht verwendet werden. FIPS-konform AWS IoT Core— Endpunkte von Anmeldeinformationsanbietern können keine Registrierungszertifikate für mehrere Konten, benutzerdefinierte Domänen, benutzerdefinierteAutorisierer und konfigurierbare Endpunkte (einschließlich unterstützter TLS-Richtlinien) unterstützen.

## Endpunkte von AWS IoT Device Management – Auftragsdaten

Die FIPS-konformen Endpunkte von AWS IoT Device Management – Auftragsdaten sind unter FIPS-Endpunkte nach Dienst aufgeführt. Suchen Sie unter FIPS-Endpunkte nach Dienst nach dem Dienst AWS IoT Device Management –Auftragsdaten und suchen Sie nach dem Endpunkt für Ihre AWS-Region.

Um den FIPS-konformen AWS IoT Device Management – Auftragsdaten-Endpunkt zu verwenden, wenn Sie aws iot-jobs-data CLI-Befehle ausführen, fügen Sie dem Befehl den Parameter --endpoint mit dem entsprechenden Endpunkt für Ihre AWS-Region hinzu. Sie können mit diesem Endpunkt auch die REST-API verwenden.

Sie können den FIPS-konformen Endpunkt für Ihre Verbindung AWS-Region mit einem FIPS-kompatiblen Client verwenden, indem Sie das AWS IoT Geräte-SDK verwenden und den Endpunkt für die Verbindungsfunktion des SDK anstelle des Standardendpunkts für Jobdaten Ihres Kontos angeben.AWS IoT Device Management Die Verbindungsfunktion ist spezifisch für das AWS IoT Geräte-SDK. Ein Beispiel für eine Verbindungsfunktion finden Sie unter der Verbindungsfunktion im AWS IoT Geräte-SDK für Python.

## Endpunkte von AWS IoT Device Management – Fleet Hub

Die FIPS-konformen AWS IoT Device Management Fleet Hub-Endpunkte, die mit den CLI-Befehlen von Fleet Hub for AWS IoT Device Management verwendet werden sollen, sind unter FIPS-Endpunkte nach Service aufgeführt. Suchen Sie unter FIPS-Endpunkte nach Dienst nach dem AWS IoT Device Management – Fleet Hub-Dienst und suchen Sie nach dem Endpunkt für Ihre AWS-Region.

Um den FIPS-konformen AWS IoT Device Management Fleet Hub-Endpunkt zu verwenden, wenn Sie aws iotfleethubCLI-Befehle ausführen, fügen Sie dem Befehl den --endpoint Parameter mit dem entsprechenden Endpunkt für Sie AWS-Region hinzu. Sie können mit diesem Endpunkt auch die REST-API verwenden.

## Endpunkte AWS IoT Device Management – Secure Tunneling

Die FIPS-konformen AWS IoT Device Management – Secure Tunneling-Endpunkte für die AWS IoT Secure Tunneling API und die entsprechenden CLI-Befehle sind unter FIPS-Endpunkte nach Dienst aufgeführt. Suchen Sie unter FIPS-Endpunkte nach Dienst nach dem Dienst AWS IoT Device Management –Secure Tunneling und suchen Sie nach dem Endpunkt für Ihre AWS-Region.

Um den FIPS-konformen AWS IoT Device Management – Secure Tunneling-Endpunkt zu verwenden, wenn Sie aws iotsecuretunneling CLI-Befehle ausführen, fügen Sie dem Befehl den Parameter --endpoint mit dem entsprechenden Endpunkt für Ihre AWS-Region hinzu. Sie können mit diesem Endpunkt auch die REST-API verwenden.

# Geräte verwalten mit AWS IoT

AWS IoT bietet eine Registrierung, mit der Sie Dinge verwalten können. Ein Objekt ist eine Darstellung eines bestimmten Geräts oder einer logischen Entität. Es kann ein physisches Gerät oder ein Sensor sein (beispielsweise eine Glühbirne oder ein Wandschalter). Es kann sich auch um eine logische Einheit wie eine Instanz einer Anwendung oder um eine physische Entität handeln, die keine Verbindung zu AWS IoT anderen Geräten herstellt, die dies tun (z. B. ein Auto mit Motorsensoren oder einem Bedienfeld).

Informationen zu einem Objekt werden in der Registry als JSON-Daten gespeichert. Hier sehen Sie ein Beispiel für ein Objekt:

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

Objekte werden anhand eines Namens identifiziert. Objekte können auch Attribute in Form von Name-Wert-Paaren haben, die Sie verwenden können, um Informationen zu einem Objekt, z. B. Seriennummer oder Hersteller, zu speichern.

Ein typischer Anwendungsfall für ein Gerät involviert die Verwendung des Objektnamens als Standard-MQTT-Client-ID. Obwohl wir keine Zuordnung zwischen dem Registrierungsnamen einer Sache und ihrer Verwendung von MQTT-Client IDs, Zertifikaten oder Schattenstatus erzwingen, empfehlen wir Ihnen, einen Ding-Namen zu wählen und ihn als MQTT-Client-ID sowohl für die Registrierung als auch für den Device Shadow-Dienst zu verwenden. Dies sorgt für Ordnung und bequeme Verwaltung Ihrer IoT-Flotte, ohne dass Sie auf die Flexibilität des zugrunde liegenden Gerätezertifikatmodells oder Shadows verzichten müssen.

Sie müssen kein Objekt in der Registry erstellen, um ein Gerät mit AWS IoT zu verbinden. Durch das Hinzufügen Ihrer Objekte zur Registry können Sie Geräte einfacher verwalten und finden.

# Dinge mit der Registrierung verwalten

Sie verwenden die AWS IoT Konsole, die AWS IoT API oder die, AWS CLI um mit der Registrierung zu interagieren. Das folgenden Abschnitte zeigen, wie Sie die CLI zur Arbeit mit dem Registry verwenden.

Wenn du deine Objekt-Objekte benennst:

- Verwenden Sie keine persönlich identifizierbaren Informationen in Ihrem Dingnamen. Der Name des Objekts kann in unverschlüsselten Mitteilungen und Berichten vorkommen.

Themen


- Ein Objekt erstellen
- Objekte auflisten
- Objekte beschreiben
- Ein Objekt aktualisieren
- Ein Objekt löschen
- Ein Prinzipal an ein Objekt anfügen
- Listet Dinge auf, die mit einem Principal verknüpft sind
- Listet die mit einer Sache verknüpften Prinzipale auf
- Listet Dinge auf, die mit einem Prinzipal V2 verknüpft sind
- Listet die mit einer Sache verknüpften Prinzipale auf V2
- Ein Prinzipal von einem Objekt trennen


## Ein Objekt erstellen

Der folgende Befehl zeigt, wie Sie den AWS IoT CreateThing Befehl aus der CLI verwenden, um ein Ding zu erstellen. Sie können den Namen eines Objekts nicht ändern, nachdem Sie es erstellt haben. Um den Namen einer Sache zu ändern, erstellen Sie eine neue Sache, geben Sie ihr den neuen Namen und löschen Sie dann die alte Sache.

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

Der Befehl CreateThing zeigt den Namen und den Amazon-Ressourcennamen (ARN) des neuen Objekts an:

```
{
    "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/MyLightBulb",
    "thingName": "MyLightBulb",
    "thingId": "12345678abcdefgh12345678ijklmnop12345678"
}
```

> **Note**
>
> Es wird nicht empfohlen, für Objektnamen personenbezogene Informationen zu verwenden.

Weitere Informationen finden Sie unter create-thing in der AWS CLI -Befehlsreferenz.

## Objekte auflisten

Mit dem Befehl ListThings können Sie alle Objekte in Ihrem Konto auflisten:

```
$ aws iot list-things
```

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

Sie können den Befehl ListThings verwenden, um nach allen Objekten eines bestimmten Objekttyps zu suchen:

```
$  aws iot list-things --thing-type-name "LightBulb"
```

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

Mit dem Befehl ListThings können Sie nach allen Objekten suchen, die über ein Attribut mit einem bestimmten Wert verfügen. Mit diesem Befehl werden bis zu drei Attribute durchsucht.

```
$  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"
        }
    ]
}
```

Weitere Informationen finden Sie unter list-things in der AWS CLI Befehlsreferenz.

## Objekte beschreiben

Mit dem Befehl DescribeThing können Sie detailliertere Informationen zu einem Objekt anzeigen:

```
$ 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"
    }
```

```
}
```

Weitere Informationen finden Sie in der AWS CLI Befehlsreferenz unter describe-thing.

## Ein Objekt aktualisieren

Mit dem Befehl UpdateThing können Sie ein Objekt aktualisieren. Dieser Befehl aktualisiert nur die Attribute des Dings. Sie können den Namen eines Objekts nicht ändern. Um den Namen eines Dings zu ändern, erstellen Sie ein neues Ding, geben ihm den neuen Namen und löschen Sie dann das alte Ding.

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

Der Befehl UpdateThing erzeugt keine Ausgabe. Mit dem Befehl DescribeThing können Sie das Ergebnis anzeigen:

```
$ aws iot describe-thing --thing-name "MyLightBulb"
{
    "attributes": {
        "model": "456",
        "wattage": "150"
    },
    "version": 2,
    "thingName": "MyLightBulb"
}
```

Weitere Informationen finden Sie unter update-thing in der AWS CLI Befehlsreferenz.

## Ein Objekt löschen

Mit dem Befehl DeleteThing können Sie ein Objekt löschen:

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

Dieser Befehl wird erfolgreich und ohne Fehler zurückgegeben, wenn der Löschvorgang erfolgreich ist oder Sie ein Objekt angeben, das nicht vorhanden ist.

Weitere Informationen finden Sie unter delete-thing in der AWS CLI Befehlsreferenz.

# Ein Prinzipal an ein Objekt anfügen

Ein physisches Gerät kann einen Principal für die Kommunikation verwenden AWS IoT. Ein Principal kann ein X.509-Zertifikat oder eine Amazon Cognito Cognito-ID sein. Sie können dem Ding in der Registrierung, das Ihr Gerät repräsentiert, ein Zertifikat oder eine Amazon Cognito Cognito-ID zuordnen, indem Sie den attach-thing-principalBefehl ausführen.

Verwenden Sie den attach-thing-principalfolgenden Befehl, um ein Zertifikat oder eine Amazon Cognito Cognito-ID an Ihr Ding anzuhängen:

```
$ aws iot attach-thing-principal \
    --thing-name "MyLightBulb1" \
    --principal "arn:aws:iot:us-
east-1:123456789012:cert/
a0c01f5835079de0a7514643d68ef8414ab739a1e94ee4162977b02b12842847"
```

Um Ihrem Ding ein Zertifikat mit einem Anhangstyp (exklusiver Anhang oder nicht exklusiver Anhang) anzuhängen, verwenden Sie den attach-thing-principalBefehl und geben Sie einen Typ in das `--thing-principal-type` Feld ein. Ein exklusiver Anhang bedeutet, dass Ihr IoT-Ding das einzige ist, was an das Zertifikat angehängt ist, und dieses Zertifikat kann nicht mit anderen Dingen verknüpft werden. Ein nicht exklusiver Anhang bedeutet, dass Ihr IoT-Ding an das Zertifikat angehängt ist und dieses Zertifikat mit anderen Dingen verknüpft werden kann. Weitere Informationen finden Sie unter ???.

> **Note**
>
> Für ??? diese Funktion können Sie nur das X.509-Zertifikat als Prinzipal verwenden.

```
$ aws iot attach-thing-principal \
    --thing-name "MyLightBulb2" \
    --principal "arn:aws:iot:us-
east-1:123456789012:cert/
a0c01f5835079de0a7514643d68ef8414ab739a1e94ee4162977b02b12842847" \
    --thing-principal-type "EXCLUSIVE_THING"
```

Wenn der Anhang erfolgreich ist, erzeugt der AttachThingPrincipal Befehl keine Ausgabe. Verwenden Sie den CLI-Befehl list-thing-principals-v 2, um den Anhang zu beschreiben.

Weitere Informationen finden Sie in AttachThingPrincipalder AWS IoT Core API-Referenz.

## Listet Dinge auf, die mit einem Principal verknüpft sind

Um die Dinge aufzulisten, die dem angegebenen Prinzipal zugeordnet sind, führen Sie den `list-principal-things`Befehl aus. Beachten Sie, dass dieser Befehl den Anhangstyp zwischen dem Ding und dem Zertifikat nicht auflistet. Verwenden Sie den `list-principal-things-v2`Befehl, um den Anhangstyp aufzulisten. Weitere Informationen finden Sie unter ???.

```
$ aws iot list-principal-things \
    --principal "arn:aws:iot:us-
east-1:123456789012:cert/
2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a35159767055278e8"
```

Die Ausgabe kann wie folgt aussehen.

```
{
    "things": [
        "MyLightBulb1",
        "MyLightBulb2"
    ]
}
```

Weitere Informationen finden Sie in ListPrincipalThingsder AWS IoT Core API-Referenz.

## Listet die mit einer Sache verknüpften Prinzipale auf

Führen Sie den Befehl aus, um die mit dem angegebenen Ding verknüpften Prinzipale aufzulisten. `list-thing-principals` Beachten Sie, dass dieser Befehl den Anhangstyp zwischen dem Ding und dem Zertifikat nicht auflistet. Verwenden Sie den `list-thing-principals-v2`Befehl, um den Anhangstyp aufzulisten. Weitere Informationen finden Sie unter ???.

```
$ aws iot list-thing-principals \
    --thing-name "MyLightBulb1"
```

Die Ausgabe kann wie folgt aussehen.

```
{
    "principals": [
         "arn:aws:iot:us-
east-1:123456789012:cert/
2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a35159767055278e8",
```

```
        "arn:aws:iot:us-
east-1:123456789012:cert/
1a234b39b4b68278f2e9d84bf97eac2cbf4a1c28b23ea29a44559b9bcf8d395b"
    ]
}
```

Weitere Informationen finden Sie in ListThingPrincipalsder AWS IoT Core API-Referenz.

## Listet Dinge auf, die mit einem Prinzipal V2 verknüpft sind

Führen Sie den `list-principal-things-v2`Befehl aus, um die mit dem angegebenen Zertifikat verknüpften Dinge zusammen mit dem Anhangstyp aufzulisten. Der Anhangstyp bezieht sich darauf, wie das Zertifikat an die Sache angehängt ist.

```
$ aws iot list-principal-things-v2 \
    --principal "arn:aws:iot:us-
east-1:123456789012:cert/
2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a35159767055278e8"
```

Die Ausgabe kann wie folgt aussehen.

```
{
    "PrincipalThingObjects": [
        {
            "thingPrincipalType": "NON_EXCLUSIVE_THING",
            "thing": "arn:aws:iot:us-east-1:123456789012:thing/thing_1"
        },
        {
            "thingPrincipalType": "NON_EXCLUSIVE_THING",
            "thing": "arn:aws:iot:us-east-1:123456789012:thing/thing_2"
        }

    ]
}
```

Weitere Informationen finden Sie in der AWS IoT Core API-Referenz unter ListPrincipalThingsV2.

## Listet die mit einer Sache verknüpften Prinzipale auf V2

Führen Sie den `list-thing-principals-V2`Befehl aus, um die mit der angegebenen Sache verknüpften Zertifikate zusammen mit dem Anlagentyp aufzulisten. Der Anhangstyp bezieht sich darauf, wie das Zertifikat an die Sache angehängt ist.

```
$ aws iot list-thing-principals-v2 \
    --thing-name "thing_1"
```

Die Ausgabe kann wie folgt aussehen.

```
{
    "ThingPrincipalObjects": [
        {
            "thingPrincipalType": "NON_EXCLUSIVE_THING",
            "principal": "arn:aws:iot:us-
east-1:123456789012:cert/
2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a35159767055278e8"
        },
        {
            "thingPrincipalType": "NON_EXCLUSIVE_THING",
            "principal": "arn:aws:iot:us-
east-1:123456789012:cert/
1a234b39b4b68278f2e9d84bf97eac2cbf4a1c28b23ea29a44559b9bcf8d395b"
        }
    ]
}
```

Weitere Informationen finden Sie in der AWS IoT Core API-Referenz unter ListThingsPrincipalV2.

## Ein Prinzipal von einem Objekt trennen

Mit dem Befehl `DetachThingPrincipal` können Sie ein Zertifikat von einem Objekt trennen:

```
$ aws iot detach-thing-principal \
    --thing-name "MyLightBulb" \
    --principal "arn:aws:iot:us-
east-1:123456789012:cert/
2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a35159767055278e8"
```

Der Befehl DetachThingPrincipal erzeugt keine Ausgabe.

Weitere Informationen finden Sie in detach-thing-principalder AWS IoT Core API-Referenz.

# Objekttypen

Mit Objekttypen können Sie Informationen zur Beschreibung und Konfiguration speichern, die auf alle Objekte desselben Objekttyps zutreffen. Dadurch wird die Verwaltung der Objekte im Registry vereinfacht. Sie können beispielsweise einen LightBulb Dingtyp definieren. Alle Dinge, die mit dem LightBulb Ding-Typ verknüpft sind, haben eine Reihe von Attributen gemeinsam: Seriennummer, Hersteller und Wattleistung. Wenn Sie ein Objekt vom Typ erstellen LightBulb (oder den Typ eines vorhandenen Objekts ändern LightBulb), können Sie Werte für jedes der LightBulb im Dingtyp definierten Attribute angeben.

Auch wenn Objekttypen optional sind, sind sie hilfreich, um Objekte leichter zu erkennen.

- Objekte mit Objekttyp können bis zu 50 Attribute haben.
- Objekte ohne Objekttyp können bis zu drei Attribute haben.
- Ein Objekt kann nur mit einem Objekttyp verknüpft werden.
- Für die Anzahl der Objekttypen in Ihrem Konto ist keine Einschränkung vorhanden.

Es ist nicht möglich, einen Objekttyp nach dem Erstellen umzubenennen. Sie können einen Objekttyp jederzeit als veraltet einstufen, um zu verhindern, dass neue Objekte mit diesem verknüpft werden. Außerdem können Sie Objekttypen, mit denen keine Objekte verknüpft sind, löschen.

Themen:


- Objekttyp erstellen
- Objekttypen auflisten
- Einen Objekttyp beschreiben
- Einen Objekttyp mit einem Objekt verknüpfen
- Aktualisiere einen Dingtyp
- Einen Objekttyp als veraltet einstufen
- Einen Objekttyp löschen


## Objekttyp erstellen

Mit dem Befehl CreateThingType können Sie einen Objekttyp erstellen:

```
$ aws iot create-thing-type
```

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

Der Befehl CreateThingType gibt eine Reaktion zurück, die Objekttyp und ARN enthält:

```
{
    "thingTypeName": "LightBulb",
    "thingTypeId": "df9c2d8c-894d-46a9-8192-9068d01b2886",
    "thingTypeArn": "arn:aws:iot:us-west-2:123456789012:thingtype/LightBulb"
}
```

## Objekttypen auflisten

Mit dem Befehl ListThingTypes können Sie Objekttypen auflisten:

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

Der ListThingTypes Befehl gibt eine Liste der Dingtypen zurück, die in Ihrem definiert sind AWS-Konto:

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

## Einen Objekttyp beschreiben

Mit dem Befehl DescribeThingType können Sie Informationen zu einem Objekttyp abrufen:

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

Der Befehl DescribeThingType gibt Informationen zum angegebenen Typ zurück:

```
{
    "thingTypeProperties": {
        "searchableAttributes": [
            "model",
            "wattage"
        ],
        "thingTypeDescription": "light bulb type"
    },
    "thingTypeId": "df9c2d8c-894d-46a9-8192-9068d01b2886",
    "thingTypeArn": "arn:aws:iot:us-west-2:123456789012:thingtype/LightBulb",
    "thingTypeName": "LightBulb",
    "thingTypeMetadata": {
        "deprecated": false,
        "creationDate": 1544466338.399
    }
}
```

## Einen Objekttyp mit einem Objekt verknüpfen

Mit dem Befehl CreateThing können Sie beim Erstellen eines Objekts einen Objekttyp festlegen:

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

Mit dem Befehl UpdateThing können Sie den mit einem Objekt verknüpften Objekttyp jederzeit ändern:

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

Mit dem Befehl UpdateThing können Sie außerdem die Verknüpfung eines Objekts mit einem Objekttyp aufheben.

## Aktualisiere einen Dingtyp

Sie können den UpdateThingType Befehl verwenden, um einen Dingtyp zu aktualisieren, wenn Sie ein Ding erstellen:

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

Mit dem Befehl UpdateThing können Sie den mit einem Objekt verknüpften Objekttyp jederzeit ändern:

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

Mit dem Befehl UpdateThing können Sie außerdem die Verknüpfung eines Objekts mit einem Objekttyp aufheben.

## Einen Objekttyp als veraltet einstufen

Objekttypen sind unveränderlich. Nach ihrer Definition können sie nicht geändert werden. Sie können einen Objekttyp jedoch als veraltet einstufen, um zu verhindern, dass Benutzer neue Objekte mit diesem verknüpfen. Alle bestehenden Objekte, die mit diesem Objekttyp verknüpft sind, bleiben unverändert.

Mit dem Befehl DeprecateThingType können Sie einen Objekttyp als veraltet einstufen:

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

Mit dem Befehl DescribeThingType können Sie das Ergebnis anzeigen:

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

```
{
    "thingTypeName": "StopLight",
    "thingTypeProperties": {
        "searchableAttributes": [
            "wattage",
```

```
            "numOfLights",
            "model"
        ],
        "thingTypeDescription": "traffic light type",
    },
    "thingTypeMetadata": {
        "deprecated": true,
        "creationDate": 1468425854308,
        "deprecationDate": 1468446026349
    }
}
```

Einen Objekttyp als veraltet einzustufen kann rückgängig gemacht werden. Mit der Markierung `--undo-deprecate` mit dem CLI-Befehl DeprecateThingType können Sie die Einstufung als veraltet rückgängig machen:

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

Mit dem CLI-Befehl DescribeThingType können Sie das Ergebnis anzeigen:

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

```
{
    "thingTypeName": "StopLight",
    "thingTypeArn": "arn:aws:iot:us-east-1:123456789012:thingtype/StopLight",
    "thingTypeId": "12345678abcdefgh12345678ijklmnop12345678"
    "thingTypeProperties": {
        "searchableAttributes": [
            "wattage",
            "numOfLights",
            "model"
        ],
        "thingTypeDescription": "traffic light type"
    },
    "thingTypeMetadata": {
        "deprecated": false,
        "creationDate": 1468425854308,
    }
}
```

## Einen Objekttyp löschen

Sie können Objekttypen erst löschen, nachdem sie als veraltet eingestuft wurden. Mit dem Befehl DeleteThingType können Sie einen Objekttyp löschen:

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

> **Note**
>
> Bevor Sie einen Dingtyp löschen können, warten Sie fünf Minuten, nachdem Sie ihn als veraltet markiert haben.

# Statische Objektgruppen

Mithilfe von statischen Objektgruppen können Sie verschiedene Objekte gleichzeitig verwalten, indem Sie sie in Gruppen zusammenfassen. Statische Objektgruppen enthalten eine Gruppe von Objekten, die über die Konsole, die CLI oder die API verwaltet werden. Dynamische Objektgruppen dagegen enthalten Objekte, die mit einer angegebenen Abfrage übereinstimmen. Statische Objektgruppen können auch andere statische Objektgruppen enthalten - Sie können eine Gruppenhierarchie aufbauen. Sie können eine Richtlinie mit einer übergeordneten Gruppe verbinden, die von den dieser untergeordneten Gruppen und von allen Objekten in der Gruppe sowie allen untergeordneten Gruppen übernommen wird. Dies vereinfacht die Steuerung von Berechtigungen für große Zahlen von Objekten.

> **Note**
>
> Richtlinien für Dinggruppen erlauben keinen Zugriff auf AWS IoT Greengrass Datenebenenoperationen. Um einer Sache den Zugriff auf einen Vorgang auf der AWS IoT Greengrass Datenebene zu gewähren, fügen Sie die Berechtigung zu einer AWS IoT Richtlinie hinzu, die Sie dem Zertifikat der Sache hinzufügen. Weitere Informationen finden Sie unter Geräteauthentifizierung und -autorisierung im AWS IoT Greengrass Entwicklerhandbuch.

Folgende Aktionen sind mit statischen Objektgruppen möglich:

- Eine Gruppe erstellen, beschreiben oder löschen.

- Ein Objekt zu einer Gruppe oder zu mehreren Gruppen hinzufügen.
- Ein Objekt aus einer Gruppe entfernen.
- Die erstellten Gruppen auflisten.
- Alle (direkt oder indirekt) untergeordneten Gruppen einer Gruppe auflisten.
- Die Objekte in einer Gruppe, einschließlich aller Objekte in dieser untergeordneten Gruppen, auflisten.
- Alle (direkt oder indirekt) übergeordneten Gruppen einer Gruppe auflisten.
- Die Attribute einer Gruppe hinzufügen, löschen oder aktualisieren. (Attribute sind Name/Wert-Paare, mit denen Sie Informationen zu einer Gruppe speichern können.)
- Eine Richtlinie mit einer Gruppe verbinden oder von dieser entfernen.
- Die mit einer Gruppe verbundenen Richtlinien auflisten.
- Die von einem Objekt (aufgrund der mit seiner Gruppe oder einer der dieser übergeordneten Gruppen verbundenen Richtlinie) übernommenen Richtlinien auflisten.
- Konfiguration von Protokollierungsoptionen für Objekte in einer Gruppe. Siehe Konfigurieren Sie die AWS IoT Protokollierung.
- Erstellen von Aufträgen, die an jedes Objekt in einer Gruppe und in dieser untergeordneten Gruppen gesendet und dort ausgeführt werden. Siehe AWS IoT Jobs.

> **Note**
>
> Wenn ein Ding an eine statische Dinggruppe angehängt ist, an die eine AWS IoT Core Richtlinie angehängt ist, muss der Name des Dings mit der Client-ID übereinstimmen.

Hier sind Sie einige Einschränkungen für statische Objektgruppen:

- Eine Gruppe kann höchstens eine direkt übergeordnete Gruppe haben.
- Wenn eine Gruppe einer anderen Gruppe untergeordnet ist, geben Sie dies bei der Erstellung an.
- Sie können das übergeordnete Element einer Gruppe nicht später ändern. Planen Sie daher die Gruppenhierarchie, und erstellen Sie eine übergeordnete Gruppe, bevor Sie untergeordnete Gruppen erstellen.
- Die Anzahl der Gruppen, zu denen ein Objekt gehören kann, ist begrenzt.

- Ein Objekt kann nicht mehr als einer Gruppe in derselben Hierarchie hinzugefügt werden. (Anders ausgedrückt: Sie können ein Objekt nicht zwei Gruppen mit derselben übergeordneten Gruppe hinzufügen).
- Gruppen können nicht umbenannt werden.
- Namen der Objektgruppen dürfen keine internationale Zeichen enthalten, z. B. û, é und ñ.
- Verwenden Sie keine persönlich identifizierbaren Informationen in Ihrem Ding-Gruppennamen. Der Name der Objektgruppe kann in unverschlüsselten Mitteilungen und Berichten vorkommen.

Das Anfügen bzw. Entfernen von Richtlinien zu/von Gruppen kann die Sicherheit Ihrer AWS IoT -Operationen unter verschiedenen Aspekten verbessern. Das Anfügen einer Richtlinie pro Gerät zu einem Zertifikat, das wiederum mit einem Objekt verbunden wird, ist zeitaufwändig und erschwert die schnelle Aktualisierung oder Änderung von Richtlinien für eine ganze Geräteflotte. Das Anhängen einer Richtlinie an die Gruppe des Objekts erspart Schritte, wenn die Zertifikate auf einem Objekt rotiert werden müssen. Dazu werden Richtlinien dynamisch auf Objekte angewendet, wenn sich deren Gruppenmitgliedschaft ändert, Sie müssen daher nicht jedes Mal, wenn ein Gerät Mitglied einer anderen Gruppe wird, einen komplexen Satz von Berechtigungen neu erstellen.

## Erstellen einer statischen Objektgruppe

Mit dem Befehl CreateThingGroup können Sie eine statische Objektgruppe erstellen:

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

Der Befehl CreateThingGroup gibt eine Antwort zurück, die den Namen, die ID und den ARN der statischen Objektgruppe enthält:

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

> **Note**
>
> Es wird nicht empfohlen, für Objektgruppennamen personenbezogene Informationen zu verwenden.

Hier ist ein Beispiel, bei dem bei der Erstellung eine der statischen Objektgruppe übergeordnete Gruppe angegeben wird:

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

Wie zuvor gibt der Befehl CreateThingGroup eine Antwort zurück, die den Namen, die ID und den ARN der statischen Objektgruppe enthält:

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

**Important**

Beachten Sie beim Erstellen von Objektgruppenhierarchien die folgenden Einschränkungen:

- Zu einer Objektgruppe kann es nur eine direkte übergeordnete Gruppe geben.
- Die Anzahl der direkten untergeordneten Gruppen, die eine Objektgruppe haben kann, ist begrenzt.
- Die maximale Tiefe einer Gruppenhierarchie ist begrenzt.
- Die Anzahl der Attribute, die eine Objektgruppe haben kann, ist begrenzt. (Attribute sind Name/Wert-Paare, mit denen Sie Informationen zu einer Gruppe speichern können.) Die Längen der einzelnen Attributnamen und Werte sind ebenfalls begrenzt.

## Beschreiben einer Objektgruppe

Mit dem Befehl DescribeThingGroup können Sie Informationen zu einer Objektgruppe abrufen:

```
$ aws iot describe-thing-group --thing-group-name RedLights
```

Der Befehl DescribeThingGroup gibt Informationen zur angegebenen Gruppe zurück:

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

## Hinzufügen eines Objekts zu einer statischen Objektgruppe

Mit dem Befehl AddThingToThingGroup können Sie einer statischen Objektgruppe ein Objekt hinzufügen:

```
$ aws iot add-thing-to-thing-group --thing-name MyLightBulb --thing-group-name
 RedLights
```

Der Befehl AddThingToThingGroup erzeugt keine Ausgabe.

> **Important**
>
> Sie können ein Objekt maximal 10 Gruppen hinzufügen. Ein Objekt kann jedoch nicht mehr als einer Gruppe in derselben Hierarchie hinzugefügt werden. (Anders ausgedrückt: Sie können ein Objekt nicht zwei Gruppen mit derselben übergeordneten Gruppe hinzufügen).

Wenn ein Objekt zu der maximalen Anzahl an Objektgruppen gehört und es sich bei einer oder mehreren dieser Gruppen um (eine) dynamische Objektgruppe(n) handelt, können Sie mit der Markierung overrideDynamicGroups statischen Gruppen den Vorrang vor dynamischen Gruppen geben.

## Entfernen eines Objekts aus einer statischen Objektgruppe

Mit dem Befehl RemoveThingFromThingGroup können Sie ein Objekt aus einer Objektgruppe entfernen:

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

Der Befehl RemoveThingFromThingGroup erzeugt keine Ausgabe.

## Auflisten von Objekten in einer Objektgruppe

Mit dem Befehl ListThingsInThingGroup können Sie die Objekte einer Gruppe auflisten:

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

Der Befehl ListThingsInThingGroup gibt eine Liste der Objekte in der betreffenden Gruppe aus:

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

Mit dem Parameter `--recursive` können Sie die Objekte einer Gruppe und in allen dieser untergeordneten Gruppen auflisten:

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

```
{
    "things":[
        "TestThingA",
```

```
        "MyLightBulb"
    ]
}
```

> **Note**
>
> Diese Operation ist letztlich konsistent. Mit anderen Worten, Änderungen an der Dinggruppe werden möglicherweise nicht sofort übernommen.

## Auflisten von Objektgruppen

Mit dem Befehl ListThingGroups können Sie die Objektgruppen Ihres Kontos auflisten:

```
$ aws iot list-thing-groups
```

Der ListThingGroups Befehl gibt eine Liste der Dinggruppen in Ihrem zurück AWS-Konto:

```
{
    "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"
```

```
        }
    ]
}
```

Verwenden Sie die optionalen Filter, um die Gruppen aufzulisten, die eine bestimmte Gruppe als übergeordnete Gruppe haben (`--parent-group`), oder deren Namen mit einem bestimmten Präfix beginnen (`--name-prefix-filter`). Mit dem Parameter `--recursive` können Sie alle untergeordneten Gruppen auflisten, nicht nur die direkt untergeordneten Gruppen einer Objektgruppe:

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

In diesem Fall gibt der ListThingGroups Befehl eine Liste der direkten untergeordneten Gruppen der Dinggruppe zurück, die in Ihrem definiert ist AWS-Konto:

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

Verwenden Sie den Parameter `--recursive` mit dem Befehl ListThingGroups, um alle (und nicht nur die direkt) untergeordneten Gruppen einer Objektgruppe aufzulisten:

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

Der Befehl ListThingGroups gibt eine Liste aller untergeordneten Gruppen einer Objektgruppe zurück:

```
{
    "childGroups":[
        {
            "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"
        }
    ]
}
```

> **Note**
>
> Diese Operation ist letztlich konsistent. Mit anderen Worten, Änderungen an der Dinggruppe werden möglicherweise nicht sofort übernommen.

## Auflisten von Gruppen für ein Objekt

Mit dem Befehl ListThingGroupsForThing können Sie die Objekte einer Gruppe auflisten, zu denen ein Objekt gehört:

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

Der Befehl ListThingGroupsForThing gibt eine Liste aller Objektgruppen aus, zu denen dieses Objekt gehört:

```
{
    "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"
        }
    ]
```

```
}
```

## Aktualisieren einer statischen Objektgruppe

Mit dem Befehl UpdateThingGroup können Sie die Attribute einer statischen Objektgruppe aktualisieren:

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

Der UpdateThingGroup Befehl gibt eine Antwort zurück, die die Versionsnummer der Gruppe nach der Aktualisierung enthält:

```
{
    "version": 4
}
```

> **Note**
>
> Die Anzahl der Attribute, die ein Objekt haben kann, ist begrenzt.

## Löschen einer Objektgruppe

Mit dem Befehl DeleteThingGroup können Sie eine Objektgruppe löschen:

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

Der Befehl DeleteThingGroup erzeugt keine Ausgabe.

> **Important**
>
> Wenn Sie versuchen, eine Objektgruppe zu löschen, zu der untergeordnete Gruppen gehören, führt dies zu einem Fehler:
>
> ```
> A client error (InvalidRequestException) occurred when calling the
>  DeleteThingGroup
> ```

```
operation: Cannot delete thing group : RedLights when there are still child
 groups attached to it.
```

Bevor Sie die Gruppe löschen, löschen Sie zunächst alle untergeordneten Gruppen.

Sie können eine Gruppe löschen, die untergeordnete Objekte hat, Berechtigungen, die aufgrund der Mitgliedschaft des Objekts in dieser Gruppe bestehen, gelten dann jedoch nicht mehr. Prüfen Sie vor dem Löschen einer Gruppe, der eine Richtlinie zugeordnet ist, sorgfältig, dass das Entfernen dieser Berechtigungen nicht dazu führt, dass die Objekte in der Gruppe ihre Funktionen nicht mehr korrekt ausführen können. Außerdem kann es sein, dass Befehle, die angeben, zu welchen Gruppen ein Objekt gehört (z. B.ListGroupsForThing), die Gruppe weiterhin anzeigen, während Datensätze in der Cloud aktualisiert werden.

## Anfügen einer Richtlinie an eine statische Objektgruppe

Mit dem Befehl AttachPolicy können Sie eine Richtlinie an eine statische Objektgruppe und damit auch an alle Objekte in dieser Gruppe und in allen ihren untergeordneten Gruppen anfügen:

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

Der Befehl AttachPolicy erzeugt keine Ausgabe

**Important**

Sie können maximal zwei Richtlinien an eine Gruppe anhängen.

**Note**

Es wird nicht empfohlen, für Richtliniennamen personenbezogene Informationen zu verwenden.

Der Parameter `--target` kann ein Objektsgruppen-ARN (wie oben), ein Zertifikat-ARN oder eine Amazon Cognito-Identität sein. Weitere Informationen zu Richtlinien, Zertifikaten und Authentifizierung finden Sie unter Authentifizierung.

Weitere Informationen finden Sie unter AWS IoT Core Richtlinien.

## Trennen einer Richtlinie von einer statischen Objektgruppe

Mit dem Befehl DetachPolicy können Sie eine Richtlinie von einer Gruppe und damit von alle Objekten in dieser Gruppe und in allen ihren untergeordneten Gruppen trennen:

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

Der Befehl DetachPolicy erzeugt keine Ausgabe.

## Auflisten der an eine statische Objektgruppe angefügten Richtlinien

Mit dem Befehl ListAttachedPolicies können Sie die an eine statische Objektgruppe angefügten Richtlinien auflisten:

```
$ aws iot list-attached-policies --target "arn:aws:iot:us-
west-2:123456789012:thinggroup/RedLights"
```

Der Parameter `--target` kann ein Objektsgruppen-ARN (wie oben), ein Zertifikat-ARN oder eine Amazon Cognito -Identität sein.

Fügen Sie den optionalen Parameter `--recursive` hinzu, um alle den übergeordneten Gruppen der Gruppe angehängten Richtlinien einzuschließen.

Der Befehl ListAttachedPolicies gibt eine Liste von Richtlinien zurück:

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

## Auflisten der Gruppen für eine Richtlinie

Mit dem Befehl ListTargetsForPolicy können Sie die Ziele auflisten, einschließlich aller Gruppen, an die eine Richtlinie angehängt ist:

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

Fügen Sie den optionalen Parameter `--page-size` *`number`* hinzu, um die maximale Anzahl der für jede Abfrage anzuzeigenden Ergebnisse anzugeben, sowie den Parameter `--marker` *`string`* auf allen folgenden Aufrufen, um den eventuell vorhandenen nächsten Ergebnissatz abzurufen.

Der Befehl ListTargetsForPolicy gibt eine Liste von Zielen und das Token für den Abruf weiterer Ergebnisse zurück:

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

## Abrufen gültiger Richtlinien für ein Objekt

Mit dem Befehl GetEffectivePolicies können Sie die für ein Objekt geltenden Richtlinien auflisten, einschließlich der Richtlinien, die an Gruppen angehängt sind, zu denen das Objekt gehört (unabhängig davon, ob es sich um direkt oder indirekt übergeordnete Gruppen handelt):

```
$ aws iot get-effective-policies \
  --thing-name "MyLightBulb" \
  --principal "arn:aws:iot:us-east-1:123456789012:cert/
a0c01f5835079de0a7514643d68ef8414ab739a1e94ee4162977b02b12842847"
```

Mit dem Parameter `--principal` geben Sie den ARN des an das Objekt angehängten Zertifikats an. Wenn Sie die Amazon Cognito-Identitätsauthentifizierung verwenden, verwenden Sie den Parameter `--cognito-identity-pool-id`, und fügen Sie optional den Parameter `--principal` hinzu, um eine Amazon Cognito-Identität anzugeben. Wenn Sie nur die `--cognito-identity-pool-id` angeben, werden die mit der Rolle des Identitätspools verbundenen Richtlinien für nicht authentifizierte Benutzer zurückgegeben. Wenn Sie beide verwenden, werden die mit der Rolle des Identitätspools verbundenen Richtlinien für authentifizierte Benutzer zurückgegeben.

Der Parameter `--thing-name` ist optional und kann anstelle des Parameters `--principal` verwendet werden. Wenn er verwendet wird, werden die mit einer Gruppe, zu der das Objekt gehört, verbundenen Richtlinien, sowie die Richtlinien, die eventuellen dieser Gruppe übergeordneten Gruppen angefügt sind (bis zur Root-Gruppe in dieser Hierarchie) zurückgegeben.

Der Befehl GetEffectivePolicies gibt eine Liste von Richtlinien zurück:

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

## Test-Autorisierung für MQTT-Aktionen

Mit dem Befehl TestAuthorization können Sie testen, ob eine MQTT-Aktion (`Publish`, `Subscribe`) für ein Objekt zulässig ist:

```
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/my/topic\"]}"
```

Mit dem Parameter `--principal` geben Sie den ARN des an das Objekt angehängten Zertifikats an. Wenn Sie die Amazon Cognito-Identitätsauthentifizierung verwenden, geben Sie eine Cognito-Identität als `--principal` an, oder verwenden Sie den Parameter `--cognito-identity-pool-id` oder beides. (Wenn Sie nur die `--cognito-identity-pool-id` angeben, werden die mit der Rolle des Identitätspools verbundenen Richtlinien für nicht authentifizierte Benutzer berücksichtigt. Wenn Sie beide verwenden, werden die mit der Rolle des Identitätspools verbundenen Richtlinien für authentifizierte Benutzer berücksichtigt.

Geben Sie eine oder mehrere MQTT-Aktionen an, die Sie testen möchten, indem Sie Sätze von Ressourcen und Aktionstypen nach dem Parameter `--auth-infos` auflisten. Das Feld `actionType` sollte „PUBLISH“, „SUBSCRIBE“, „RECEIVE” oder „CONNECT“ enthalten. Das `resources` Feld sollte eine Liste von Ressourcen enthalten ARNs. Weitere Informationen finden Sie unter AWS IoT Core Richtlinien.

Sie können die Auswirkungen des Hinzufügens von Richtlinien testen, indem Sie sie mit dem Parameter `--policy-names-to-add` angeben. Sie können auch die Auswirkungen des Entfernens von Richtlinien testen, indem Sie den Parameter `--policy-names-to-skip` verwenden.

Mit dem optionalen Parameter `--client-id` können Sie Ihre Ergebnisse weiter verfeinern.

Der Befehl TestAuthorization gibt Details zu Aktionen aus, die für jeden angegebenen Satz von `--auth-infos`-Abfragen zulässig sind oder abgelehnt wurden:

```
{
    "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" ]
        }
    ]
}
```

# Dynamische Objektgruppen

Dynamische Dinggruppen werden aus bestimmten Suchanfragen in der Registrierung erstellt. Suchabfrageparameter wie Gerätekonnektivität, Erstellung von Geräteschatten und Daten zu AWS IoT Device Defender Verstößen unterstützen dies. Für dynamische Dinggruppen muss die Flottenindizierung aktiviert sein, um die Daten Ihrer Geräte zu indizieren, zu durchsuchen und zu aggregieren. Sie können eine Vorschau der Dinge in einer dynamischen Dinggruppe mithilfe einer Suchabfrage zur Flottenindizierung anzeigen, bevor Sie sie erstellen. Weitere Informationen erhalten Sie unter -Flottenindizierung und Abfragesyntax.

> **Note**
>
> Dynamische Objektgruppenvorgänge werden im Rahmen von Registrierungsvorgängen gemessen. Weitere Informationen finden Sie unter AWS IoT Core Zusätzliche Details zur Messung.

Dynamische Objektgruppen unterscheiden sich von statischen Objektgruppen in folgender Hinsicht:

- Die Objektmitgliedschaft ist nicht explizit definiert. Um eine dynamische Dinggruppe zu erstellen, definieren Sie eine Suchabfragezeichenfolge, um die Gruppenmitgliedschaft zu bestimmen.
- Dynamische Objektgruppen können nicht Teil einer Hierarchie sein.
- Auf dynamische Objektgruppen können keine Richtlinien angewendet werden.
- Sie verwenden eine andere Gruppe von Befehlen zum Erstellen, Aktualisieren und Löschen von dynamischen Objektgruppen. Für alle anderen Operationen verwenden Sie dieselben Befehle für beide Arten von Dinggruppen.
- Die Anzahl der dynamischen Gruppen pro AWS-Konto ist begrenzt.

- Verwenden Sie keine persönlich identifizierbaren Informationen in Ihrem Dinggruppennamen. Der Name der Objektgruppe kann in unverschlüsselten Mitteilungen und Berichten vorkommen.

Weitere Informationen über statische Objektgruppen finden Sie unter Statische Objektgruppen.

## Anwendungsfälle dynamischer Dinggruppen

Sie können dynamische Dinggruppen für die folgenden Anwendungsfälle verwenden:

## Geben Sie eine dynamische Dinggruppe als Ziel für einen Job an

Wenn Sie einen kontinuierlichen Job mit einer dynamischen Dinggruppe als Ziel erstellen, können Sie Geräte automatisch als Ziel auswählen, wenn sie die gewünschten Kriterien erfüllen. Bei den Kriterien kann es sich um den Konnektivitätsstatus oder um in der Registrierung oder im Shadow gespeicherte Kriterien wie Softwareversion oder Modell handeln. Wenn ein Ding nicht in der dynamischen Dinggruppe erscheint, erhält es das Auftragsdokument aus dem Job nicht.

Zum Beispiel, wenn Ihre Geräteflotte ein Firmware-Update benötigt, um das Risiko einer Unterbrechung während des Aktualisierungsvorgangs zu minimieren, und Sie die Firmware nur auf Geräten mit einer Akkulaufzeit von mehr als 80% aktualisieren möchten. Sie können eine dynamische Dinggruppe mit dem Namen 80 erstellenPercentBatteryLife , die nur Geräte mit einer Akkulaufzeit von über 80% umfasst, und diese als Ziel für Ihre Arbeit verwenden. Nur Geräte, die Ihre Kriterien für die Akkulaufzeit erfüllen, erhalten das Firmware-Update. Wenn Geräte die Kriterien für die Akkulaufzeit von 80% erreichen, werden sie automatisch der dynamischen Objektgruppe hinzugefügt und erhalten das Firmware-Update.

Möglicherweise verfügen Sie auch über mehrere Gerätemodelle mit unterschiedlicher Firmware oder unterschiedlichen Betriebssystemen, sodass unterschiedliche Versionen neuer Softwareupdates erforderlich sind. Dies ist der häufigste Anwendungsfall für dynamische Gruppen mit fortlaufenden Aufträgen, bei denen Sie für jede Kombination aus Gerätemodell, Firmware und Betriebssystem eine dynamische Gruppe erstellen können. Anschließend können Sie fortlaufende Aufträge für jede dieser dynamischen Gruppen einrichten, um Softwareupdates zu übertragen, da Geräte anhand der definierten Kriterien automatisch Mitglieder dieser Gruppen werden.

Weitere Informationen zum Angeben von Objektgruppen als Auftragszielen finden Sie unter CreateJob.

## Verwenden Sie dynamische Änderungen der Gruppenmitgliedschaft, um die gewünschten Aktionen durchzuführen

Jedes Mal, wenn ein Gerät zu einer dynamischen Dinggruppe hinzugefügt oder daraus entfernt wird, wird im Rahmen von Registrierungsereignisaktualisierungen eine Benachrichtigung an ein MQTT-Thema gesendet. Sie können AWS IoT Core Regeln für die Interaktion mit AWS Diensten konfigurieren, die auf den Aktualisierungen der dynamischen Gruppenmitgliedschaft basieren, und die gewünschten Aktionen ausführen. Zu den Beispielaktionen gehören das Schreiben in eine Lambda-Funktion Amazon DynamoDB, das Aufrufen einer Lambda-Funktion oder das Senden einer Benachrichtigung an Amazon SNS.

### Fügen Sie Geräte zur automatischen Erkennung von Verstößen zu einer dynamischen Dinggruppe hinzu

AWS IoT Device Defender Detect: Kunden können ein Sicherheitsprofil für eine dynamische Dinggruppe definieren. Geräte der dynamischen Dinggruppe werden anhand des für die Gruppe definierten Sicherheitsprofils automatisch auf Verstöße erkannt.

### Richten Sie Protokollebenen für dynamische Dinggruppen ein, um Geräte mit detaillierter Protokollierung zu beobachten

Sie können eine Protokollebene für eine dynamische Dinggruppe angeben. Dies ist nützlich, wenn Sie die Protokollierungsebene und die Details nur für Geräte anpassen möchten, die bestimmte Kriterien erfüllen. Wenn Sie beispielsweise vermuten, dass Geräte mit einer bestimmten Firmware-Version Fehler im veröffentlichten Thema einer bestimmten Regel verursachen, sollten Sie eine detaillierte Protokollierung einrichten, um diese Probleme zu beheben. In diesem Fall können Sie eine dynamische Gruppe für alle Geräte mit dieser Firmware-Version erstellen, von der wir annehmen, dass sie als Registrierungsattribut oder in einem Geräteshadow gespeichert ist. Sie können dann eine Debug-Ebene festlegen, wobei das Protokollierungsziel als diese dynamische Dinggruppe definiert ist. Weitere Informationen zur detaillierten Protokollierung finden Sie unter Überwachung AWS IoT mithilfe von Protokollen. CloudWatch Weitere Informationen zum Angeben einer Protokollierungsebene für eine bestimmte Dinggruppe finden Sie unter Konfiguration der ressourcenspezifischen Anmeldung. AWS IoT

## Erstellen einer dynamischen Objektgruppe

Mit dem Befehl CreateDynamicThingGroup können Sie eine dynamische Objektgruppe erstellen. Verwenden Sie den create-dynamic-thing-group CLI-Befehl, um eine dynamische Dinggruppe für das PercentBatteryLife 80-Szenario zu erstellen:

```
$ aws iot create-dynamic-thing-group --thing-group-name "80PercentBatteryLife" --query-string "attributes.batterylife80"
```

> **Note**
>
> Verwenden Sie in Ihren dynamischen Dinggruppennamen keine personenbezogenen Daten.

Der CreateDynamicThingGroup Befehl gibt eine Antwort zurück. Die Antwort enthält den Indexnamen, die Abfragezeichenfolge, die Abfrageversion, den Namen der Dinggruppe, die Dinggruppen-ID und den Amazon-Ressourcennamen (ARN) Ihrer Dinggruppe:

```
{
    "indexName": "AWS_Things",
    "queryVersion": "2017-09-30",
    "thingGroupName": "80PercentBatteryLife",
    "thingGroupArn": "arn:aws:iot:us-
west-2:123456789012:thinggroup/80PercentBatteryLife",
    "queryString": "attributes.batterylife80\n",
    "thingGroupId": "abcdefgh12345678ijklmnop12345678qrstuvwx"
}
```

Die Erstellung dynamischer Dinggruppen erfolgt nicht auf einmal. Der Backfillvorgang für die dynamische Objektgruppe nimmt einige Zeit in Anspruch. Wenn Sie eine dynamische Dinggruppe erstellen, wird der Status der Gruppe auf gesetzt`BUILDING`. Wenn der Backfillvorgang abgeschlossen ist, wechselt der Status zu `ACTIVE`. Verwenden Sie den DescribeThingGroupBefehl, um den Status Ihrer dynamischen Dinggruppe zu überprüfen.

## Beschreiben einer dynamischen Objektgruppe

Mit dem Befehl DescribeThingGroup können Sie Informationen zu einer dynamischen Objektgruppe abrufen:

```
$ aws iot describe-thing-group --thing-group-name "80PercentBatteryLife"
```

Der Befehl DescribeThingGroup gibt Informationen zur angegebenen Gruppe zurück:

```
{
    "status": "ACTIVE",
    "indexName": "AWS_Things",
    "thingGroupName": "80PercentBatteryLife",
    "thingGroupArn": "arn:aws:iot:us-
west-2:123456789012:thinggroup/80PercentBatteryLife",
    "queryString": "attributes.batterylife80\n",
    "version": 1,
    "thingGroupMetadata": {
        "creationDate": 1548716921.289
    },
```

```
    "thingGroupProperties": {},
    "queryVersion": "2017-09-30",
    "thingGroupId": "84dd9b5b-2b98-4c65-84e4-be0e1ecf4fd8"
}
```

Wenn die Ausführung DescribeThingGroup auf einer dynamischen Dinggruppe ausgeführt wird, werden Attribute zurückgegeben, die für die dynamischen Dinggruppen spezifisch sind. Beispiele für Rückgabeattribute sind der QueryString und der Status.

Der Status einer dynamischen Objektgruppe kann die folgenden Werte haben:

`ACTIVE`

Die dynamische Objektgruppe ist einsatzbereit.

`BUILDING`

Die dynamische Objektgruppe wird erstellt, und die Mitgliedschaft wird bearbeitet.

`REBUILDING`

Die Mitgliedschaft der dynamischen Objektgruppe wird aktualisiert, nach der Anpassung Suchabfrage der Gruppe.

> **Note**
>
> Nachdem Sie eine dynamische Dinggruppe erstellt haben, verwenden Sie sie unabhängig von ihrem Status. Nur dynamische Objektgruppen mit dem Status `ACTIVE` enthalten alle Objekte, die der Suchabfrage für diese dynamische Objektgruppe entsprechen. Dynamische Objektgruppen mit den Status `BUILDING` und `REBUILDING` enthalten möglicherweise nicht alle Objekte, die der Suchabfrage entsprechen.

## Aktualisieren einer dynamischen Objektgruppe

Verwenden Sie den Befehl UpdateDynamicThingGroup, um die Attribute einer dynamischen Objektgruppe zu aktualisieren, einschließlich der Suchabfrage der Gruppe: Mit dem folgenden Befehl werden zwei Attribute aktualisiert. Eines ist die Beschreibung der Dinggruppe und das andere ist die Abfragezeichenfolge, mit der die Mitgliedschaftskriterien auf Akkulaufzeit > 85 geändert werden:

```
$ aws iot update-dynamic-thing-group --thing-group-name "80PercentBatteryLife" --thing-
group-properties "thingGroupDescription=\"This thing group contains devices with a
 battery life greater than 85 percent.\"" --query-string "attributes.batterylife85"
```

Der UpdateDynamicThingGroup Befehl gibt eine Antwort zurück, die die Versionsnummer der Gruppe nach der Aktualisierung enthält:

```
{
    "version": 2
}
```

Die Aktualisierung einer dynamischen Dinggruppe erfolgt nicht sofort. Der Backfillvorgang für die dynamische Objektgruppe nimmt einige Zeit in Anspruch. Wenn Sie eine dynamische Dinggruppe aktualisieren, ändert sich der Status der Gruppe in, `REBUILDING` während die Gruppe ihre Mitgliedschaft aktualisiert. Wenn der Backfillvorgang abgeschlossen ist, wechselt der Status zu `ACTIVE`. Verwenden Sie den DescribeThingGroupBefehl, um den Status Ihrer dynamischen Dinggruppe zu überprüfen.

## Löschen einer dynamischen Objektgruppe

Mit dem Befehl DeleteDynamicThingGroup können Sie eine dynamische Objektgruppe löschen:

```
$ aws iot delete-dynamic-thing-group --thing-group-name "80PercentBatteryLife"
```

Der Befehl DeleteDynamicThingGroup erzeugt keine Ausgabe.

Befehle, die zeigen, zu welchen Gruppen ein Objekt gehört (z. B. ListGroupsForThing) zeigen möglicherweise weiterhin die Gruppe an, während Datensätze in der Cloud aktualisiert werden.

## Einschränkungen dynamischer und statischer Dinggruppen

Dynamische Dinggruppen und statische Dinggruppen haben die folgenden Einschränkungen:

- Die Anzahl der Attribute, die eine Dinggruppe haben kann, ist begrenzt.
- Die Anzahl der Gruppen, zu denen ein Objekt gehören kann, ist begrenzt.
- Sie können Dinggruppen nicht umbenennen.
- Namen der Objektgruppen dürfen keine internationale Zeichen enthalten, z. B. û, é und ñ.

# Einschränkungen dynamischer Dinggruppen

Für dynamische Dinggruppen gelten die folgenden Einschränkungen:

## -Flottenindizierung

Wenn der Flottenindexdienst aktiviert ist, können Sie Suchanfragen auf Ihrer Geräteflotte durchführen. Sie können dynamische Dinggruppen erstellen und verwalten, nachdem das Auffüllen der Flottenindizierung abgeschlossen ist. Die Fertigstellungszeit für den Backfill-Prozess hängt direkt von der Größe Ihrer Geräteflotte ab, die bei der registriert ist. AWS Cloud Nachdem Sie den Flottenindizierungsservice für dynamische Objektgruppen aktiviert haben, können Sie ihn erst wieder deaktivieren, wenn Sie alle Ihre dynamischen Objektgruppen gelöscht haben.

> **Note**
>
> Wenn Sie über die Berechtigungen verfügen, den Flottenindex abzufragen, können Sie auf Daten zu Objekten über die gesamte Flotte hinweg zugreifen.

## Die Anzahl der dynamischen Objektgruppen ist begrenzt

Die Anzahl der dynamischen Dinggruppen ist begrenzt.

## Erfolgreiche Befehle können Fehler protokollieren

Wenn Sie eine dynamische Dinggruppe erstellen oder aktualisieren, ist es möglich, dass einige Dinge in eine dynamische Dinggruppe aufgenommen werden können, aber sie werden dieser nicht hinzugefügt. In diesem Szenario wird ein erfolgreicher Befehl zum Erstellen oder Aktualisieren ausgeführt, während ein Fehler protokolliert und eine Metrik generiert wird. `AddThingToDynamicThingGroupsFailed` Eine einzelne Metrik kann mehrere Protokolleinträge darstellen.

Ein Fehlerprotokolleintrag im CloudWatch Protokoll wird erstellt, wenn Folgendes eintritt:

- Ein geeignetes Ding kann keiner dynamischen Dinggruppe hinzugefügt werden.
- Ein Ding wird aus einer dynamischen Dinggruppe entfernt, um es einer anderen Gruppe hinzuzufügen.

Wenn ein Ding für das Hinzufügen zu einer dynamischen Dinggruppe in Frage kommt, sollten Sie Folgendes beachten:

- Ist das Objekt schon in der maximalen Anzahl von Gruppen enthalten? (Weitere Informationen finden Sie unter Limits).
  - NEIN: Das Objekt wird der dynamischen Objektgruppe hinzugefügt.
  - JA: Gehört das Objekt dynamischen Objektgruppen an?
    - NEIN: Das Objekt kann nicht zu der dynamischen Objektgruppe hinzugefügt werden, ein Fehler wird protokolliert und eine `AddThingToDynamicThingGroupsFailed` Metrik wird generiert.
    - JA: Ist die dynamische Objektgruppe, in die das Objekt aufgenommen werden soll, älter als jede dynamische Objektgruppe, der das Objekt bereits angehört?
      - NEIN: Das Objekt kann nicht zu der dynamischen Objektgruppe hinzugefügt werden, ein Fehler wird protokolliert und eine `AddThingToDynamicThingGroupsFailed` Metrik wird generiert.
      - JA: Entfernen Sie das Ding aus der neuesten dynamischen Dinggruppe, protokollieren Sie einen Fehler und fügen Sie das Ding der dynamischen Dinggruppe hinzu. Dies erzeugt einen Fehler und es wird eine `AddThingToDynamicThingGroupsFailed` Metrik für die dynamische Objektgruppe generiert, aus der das Objekt entfernt wurde.

Wenn ein Ding in einer dynamischen Dinggruppe die Suchabfrage nicht mehr erfüllt, wird das Ding aus der dynamischen Dinggruppe entfernt. Ebenso wird ein Ding, das aktualisiert wird, um der Suchabfrage einer dynamischen Dinggruppe zu entsprechen, der Gruppe hinzugefügt, wie zuvor beschrieben. Diese Hinzufügungen und Entfernungen sind normal und verursachen keine Fehlerprotokolleinträge.

### Bei Aktivierung von **`overrideDynamicGroups`** haben statische Gruppen Vorrang vor dynamischen Gruppen

Die Anzahl der Gruppen, zu denen ein Objekt gehören kann, ist begrenzt. Wenn Sie die UpdateThingGroupsForThingBefehle AddThingToThingGroupoder verwenden, um die Ding-Mitgliedschaft zu aktualisieren, gibt das Hinzufügen des `--overrideDynamicGroups` Parameters statischen Dinggruppen Vorrang vor dynamischen Dinggruppen.

Beachten Sie Folgendes, wenn Sie einer statischen Dinggruppe ein Ding hinzufügen:

- Gehört das Objekt bereits der maximalen Anzahl von Gruppen an?

- NEIN: Das Objekt wird der statischen Objektgruppe hinzugefügt.
- JA: Ist das Objekt in dynamischen Gruppen enthalten?
  - NEIN: Das Objekt kann nicht zu der Objektgruppe hinzugefügt werden. Der Befehl löst eine Ausnahme aus.
  - JA: Wurde --overrideDynamicGroups aktiviert?
    - NEIN: Das Objekt kann nicht zu der Objektgruppe hinzugefügt werden. Der Befehl löst eine Ausnahme aus.
    - JA: Das Objekt wird aus der zuletzt erstellten dynamischen Objektgruppe entfernt, ein Fehler wird protokolliert und es wird eine `AddThingToDynamicThingGroupsFailed` Metrik für die dynamische Objektgruppe generiert, aus der das Objekt entfernt wurde. Anschließend wird das Objekt der statischen Objektgruppe hinzugefügt.

### Ältere dynamische Objektgruppen haben Vorrang vor neueren.

Die Anzahl der Gruppen, zu denen ein Objekt gehören kann, ist begrenzt. Wenn durch einen Erstellungs- oder Aktualisierungsvorgang zusätzliche Gruppenberechtigungen für ein Ding geschaffen werden und das Ding sein Gruppenlimit erreicht hat, kann es aus einer anderen dynamischen Dinggruppe entfernt werden, um dieses Hinzufügen zu ermöglichen. Wenn Sie mehr Informationen wünschen, wie dies geschieht, beachten Sie die Beispiele unter Erfolgreiche Befehle können Fehler protokollieren und Bei Aktivierung von `overrideDynamicGroups` haben statische Gruppen Vorrang vor dynamischen Gruppen.

Wenn ein Ding aus einer dynamischen Dinggruppe entfernt wird, wird ein Fehler protokolliert und ein Ereignis ausgelöst.

### Sie können keine Richtlinien auf dynamische Objektgruppen anwenden.

Wenn Sie versuchen, eine Richtlinie auf eine dynamische Objektgruppe anzuwenden, wird eine Ausnahme generiert.

### Die Mitgliedschaft in dynamischen Objektgruppen ist letztlich konsistent.

Nur der letzte Status eines Geräts wird für die Registrierung evaluiert. Zwischenzustände können bei schneller Aktualisierung der Zustände übersprungen werden. Vermeiden Sie es, eine Regel oder einen Job einer dynamischen Dinggruppe zuzuordnen, deren Mitgliedschaft von einem Zwischenstatus abhängt.

# Einer AWS IoT MQTT-Clientverbindung ein Ding zuordnen

Eine exklusive Zuordnung von Dingen liegt vor, wenn Sie ein X.509-Zertifikat an eine einzelne AWS IoT Sache anhängen. In diesem Fall kann das Zertifikat nicht mit anderen Dingen verwendet werden. Indem sichergestellt wird, dass ein Zertifikat nur von einem einzigen IoT-Ding verwendet wird, trägt es dazu bei, Sicherheitslücken zu vermeiden.

In AWS IoT ist die Client-ID eine eindeutige Kennung für ein Ding oder ein Gerät, wenn es eine Verbindung zum AWS IoT Core MQTT-Broker herstellt. Wenn Sie eine nicht ausschließliche Zuordnung verwenden, können mehrere Dinge an dasselbe Zertifikat angehängt werden. Wenn eine nicht ausschließliche Zuordnung besteht, müssen Sie, um eine klare Zuordnung aufrechtzuerhalten und mögliche Konflikte zu vermeiden, Ihre Client-ID mit dem Namen des Dings abgleichen.

In diesem Thema


- Anwendungsfälle
- Wie ordne ich eine Sache einer Verbindung zu


## Anwendungsfälle

Das Zuordnen eines Objekts zu einer Verbindung bietet die folgenden Funktionen.

> **Note**
>
> Beachten Sie, dass Sie alle folgenden Funktionen außer der Funktion für Lebenszyklusereignisse verwenden können, wenn Ihr IoT-Ding und Ihre Client-Verbindung eine nicht ausschließliche Zuordnung haben. Um Ihren Dingnamen in die Lebenszyklusereignismeldungen aufzunehmen, müssen Ihr IoT-Ding und Ihre Client-Verbindung eine exklusive Zuordnung haben.

Ding-Richtlinienvariablen — Sie können Ding-Richtlinienvariablen verwenden, um den Gerätezugriff auf AWS IoT API-Operationen zu autorisieren. Mit diesen Variablen können Sie AWS IoT Core Richtlinien schreiben, die Berechtigungen auf der Grundlage von Dingeigenschaften wie Namen, Typen und Attributwerten gewähren oder verweigern. Mithilfe von Ding-Richtlinienvariablen können Sie dieselbe Richtlinie anwenden, um mehrere AWS IoT Core Geräte zu steuern. Auf diese Weise können Sie die Richtlinienverwaltung vereinfachen und die doppelte Nutzung von Ressourcen reduzieren. Weitere Informationen finden Sie unter Ding-Richtlinienvariablen.

Lebenszyklusereignisse — Sie können den Namen des Dings in Lebenszyklusereignissen abrufen (z. B. Verbinden, Trennen und Abonnieren und Abbestellen). Dies ermöglicht die Verarbeitung des in den Nachrichten enthaltenen Dingnamens, z. B. in Regeln. Weitere Informationen finden Sie unter Lebenszyklusereignisse.

Ressourcenspezifische Protokollierung — Sie können die ressourcenspezifische Protokollierung für Dinggruppen konfigurieren und auf einfache Weise die gewünschte Protokollierungskonfiguration für alle Dinge innerhalb der definierten Dinggruppe anwenden. Weitere Informationen finden Sie unter ???.

Kostenzuweisung — Sie können Abrechnungsgruppen mit benutzerdefinierten Tags für die Kostenzuweisung erstellen und die Dinge zu diesen Gruppen hinzufügen. Weitere Informationen finden Sie unter Abrechnungsgruppen.

## Wie ordne ich eine Sache einer Verbindung zu

Wenn Ihre Client-ID mit dem Namen Ihres Dings in der Registrierung übereinstimmt, AWS IoT Core wird die Client-Verbindung dem Ding zugeordnet, nachdem Sie ein X.509-Zertifikat an dieses IoT-Ding angehängt haben. Wenn Ihre Client-ID nicht mit dem Namen des Dings in der Registrierung übereinstimmt, können Sie ausschließlich ein X.509-Zertifikat an das Ding anhängen, um diese Zuordnung herzustellen. Das Ding, das diesen exklusiven Anhang hat, wird als exklusives Ding bezeichnet. Andernfalls wird es als nicht exklusives Ding bezeichnet. Wenn ein Zertifikat mit einer exklusiven Sache verknüpft ist, kann dieses Zertifikat nur dann mit anderen Dingen verknüpft werden, wenn Sie es von der exklusiven Sache trennen. Wählen Sie in diesem Abschnitt entweder AWS Management Console oder, AWS CLI um einer Verbindung eine Sache zuzuordnen.

AWS Management Console

Um ein Zertifikat an eine Sache anzuhängen, verwenden Sie ausschließlich den AWS Management Console.

1. Öffnen Sie die AWS IoT Startseite in der AWS IoT Konsole. Wählen Sie in der linken Navigationsleiste unter Sicherheit die Option Zertifikate aus.
2. Wählen Sie auf der Seite Zertifikate ein Zertifikat aus, an das Sie etwas anhängen möchten. Wählen Sie dann in der oberen rechten Ecke der Seite unter Aktionen die Option An Dinge anhängen aus.

   Wählen Sie alternativ ein Zertifikat aus und navigieren Sie zur Seite mit den Zertifikatsdetails. Wählen Sie den Tab „Dinge“ und anschließend „An Dinge anhängen“.

3. Aktivieren Sie auf der Seite „Zertifikat an Ding (en) anhängen“ das Kontrollkästchen Ding mit Verbindung verknüpfen. Wählen Sie dann aus der Dropdownliste Dinge eine Sache aus, an die dieses Zertifikat angehängt werden soll.
4. Wählen Sie „Ding (e) anhängen“. Wenn die Aktion erfolgreich ist, wird ein Banner mit der Aufschrift „Erfolgreich wurde ein Ding an Ihr Zertifikat angehängt“ angezeigt, und das Ding wird der Registerkarte „Dinge“ hinzugefügt.

Um ein Zertifikat von einem exklusiven Objekt zu trennen, verwenden Sie den AWS Management Console

1. Öffnen Sie die AWS IoT Startseite in der AWS IoT Konsole. Wählen Sie in der linken Navigationsleiste unter Sicherheit die Option Zertifikate aus.
2. Wählen Sie auf der Seite Zertifikate ein Zertifikat aus und navigieren Sie zur Seite mit den Zertifikatsdetails.
3. Wählen Sie auf der Seite mit den Zertifikatsdetails die Registerkarte Dinge aus. Wählen Sie dann eine Sache aus, von der Sie das Zertifikat trennen möchten. Wählen Sie Dinge trennen.
4. Bestätigen Sie im Fenster „Dinge trennen“ Ihre Aktion. Wählen Sie Detach (Trennen) aus. Wenn die Aktion erfolgreich ist, wird ein Banner mit der Aufschrift „Ein Ding wurde erfolgreich von Ihrem Zertifikat getrennt“ angezeigt, und das Ding wird nicht mehr auf der Registerkarte „Dinge“ angezeigt.

AWS CLI

1. Führen Sie den attach-thing-principalBefehl aus, um ein Zertifikat an ein Objekt anzuhängen AWS CLI, indem Sie es verwenden. Um den exklusiven certificate-to-thing Anhang anzugeben, müssen Sie dies `EXCLUSIVE_THING` in dem `--thing-principal-type` Feld angeben. Ein Beispielbefehl kann der folgende sein.

```
aws iot attach-thing-principal \
    --thing-name "thing_1" \
    --principal "arn:aws:iot:us-
east-1:123456789012:cert/
2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a351597670552 78e8" \
    --thing-principal-type "EXCLUSIVE_THING"
```

Dieser Befehl liefert keine Ausgabe. Weitere Informationen finden Sie unter ???.

2. Führen Sie den `list-principal-things-v2` Befehl aus, um die mit dem angegebenen Zertifikat verknüpften Elemente zusammen mit dem Anhangstyp aufzulisten. Der Anhangstyp bezieht sich darauf, wie das Zertifikat an die Sache angehängt ist. Ein Beispielbefehl kann der folgende sein.

```
$ aws iot list-principal-things-v2 \
    --principal "arn:aws:iot:us-
east-1:123456789012:cert/
2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a35159767055278e8"
```

Die Ausgabe kann wie folgt aussehen.

```
{
    "PrincipalThingObjects": [
        {
            "thingPrincipalType": "EXCLUSIVE_THING",
            "thing": "arn:aws:iot:us-east-1:123456789012:thing/thing_1"
        }
    ]
}
```

Weitere Informationen finden Sie unter ???.

3. Führen Sie den `list-thing-principals-v2` Befehl aus, um die mit dem angegebenen Objekt verknüpften Prinzipale zusammen mit dem Anlagentyp aufzulisten. Der Anhangstyp bezieht sich darauf, wie das Zertifikat an die Sache angehängt ist. Ein Beispielbefehl kann der folgende sein.

```
$ aws iot list-thing-principals-v2 \
    --thing-name "thing_1"
```

Die Ausgabe kann wie folgt aussehen.

```
{
    "ThingPrincipalObjects": [
        {
            "thingPrincipalType": "EXCLUSIVE_THING",
            "principal": "arn:aws:iot:us-
east-1:123456789012:cert/
2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a35159767055278e8"
        }
    ]
```

```
}
```

Weitere Informationen finden Sie unter ???.

4. Um ein Zertifikat von einer Sache zu trennen, führen Sie den detach-thing-principalBefehl aus.

```
aws iot detach-thing-principal \
    --principal "arn:aws:iot:us-
east-1:123456789012:cert/
2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a35159767055278e8" \
    --thing-name "thing_1"
```

Dieser Befehl liefert keine Ausgabe. Weitere Informationen finden Sie unter ???.

# Hinzufügen von Übertragungsattributen zur Nachrichtenanreicherung

In können Sie MQTT-Nachrichten von Geräten anreichern AWS IoT Core, indem Sie propagierende Attribute hinzufügen, bei denen es sich um kontextbezogene Metadaten aus Dingattributen oder Verbindungsdetails handelt. Dieser Prozess, bekannt als Nachrichtenanreicherung, kann in verschiedenen Szenarien hilfreich sein. Sie können beispielsweise Nachrichten für jeden eingehenden Veröffentlichungsvorgang anreichern, ohne Änderungen auf der Geräteseite vorzunehmen oder Regeln verwenden zu müssen. Durch die Nutzung von propagierenden Attributen können Sie von einer effizienteren und kostengünstigeren Methode zur Anreicherung Ihrer IoT-Daten profitieren, ohne die Komplexität der Konfiguration von Regeln oder der Verwaltung von Konfigurationen für die Neuveröffentlichung.

Die Funktion zur Nachrichtenanreicherung steht AWS IoT Core Kunden zur Verfügung, die Basic Ingest und Message Broker verwenden. Es ist wichtig zu beachten, dass Publishing-Geräte zwar jede MQTT-Version verwenden können, Abonnenten (Anwendungen oder Dienste, die Nachrichten konsumieren) jedoch MQTT 5 unterstützen müssen, um die angereicherten Nachrichten mit propagierenden Attributen zu empfangen. Die angereicherten Nachrichten werden als MQTT 5-Benutzereigenschaften zu jeder Nachricht hinzugefügt, die von Geräten veröffentlicht wird. Wenn Sie Regeln verwenden, können Sie die Funktion get_user_properties nutzen, um die angereicherten Daten für das Routing oder die Verarbeitung von Nachrichten auf der Grundlage der Daten abzurufen.

In können Sie propagierende Attribute hinzufügen AWS IoT Core, wenn Sie einen Dingtyp erstellen oder aktualisieren, indem Sie den oder den verwenden. AWS Management Console AWS CLI

> **Important**
>
> Wenn Sie Übertragungsattribute hinzufügen, müssen Sie sicherstellen, dass der Client, der die Nachricht veröffentlicht, mit einem Zertifikat authentifiziert wurde. Weitere Informationen finden Sie unter Client-Authentifizierung.

> **Note**
>
> Wenn Sie versuchen, diese Funktion mit dem MQTT-Testclient in der Konsole zu testen, funktioniert es möglicherweise nicht, da für diese Funktion MQTT-Clients erforderlich sind, die mit einem zugehörigen Zertifikat authentifiziert sind.

## AWS Management Console

Um propagierende Attribute für die Nachrichtenanreicherung hinzuzufügen, verwenden Sie den AWS Management Console

1. Öffnen Sie die AWS IoT Startseite in der AWS IoT Konsole. Wählen Sie in der linken Navigationsleiste unter Verwalten die Option Alle Geräte aus. Wählen Sie dann „Dingtypen“.
2. Wählen Sie auf der Seite „Dingtypen“ die Option „Dingtyp erstellen“ aus.

   Um die Nachrichtenanreicherung durch Aktualisierung eines Dingtyps zu konfigurieren, wählen Sie einen Dingtyp aus. Wählen Sie dann auf der Detailseite des Dingtyps die Option Aktualisieren aus.
3. Wählen Sie auf der Seite Dingtyp erstellen unter Eigenschaften des Dingtyps die Informationen zum Dingtyp aus, oder geben Sie sie ein.

   Wenn Sie einen Dingtyp aktualisieren möchten, werden die Eigenschaften des Dingtyps angezeigt, nachdem Sie im vorherigen Schritt „Aktualisieren“ ausgewählt haben.
4. Erweitern Sie unter Zusätzliche Konfiguration den Eintrag Attribute weitergeben. Wählen Sie dann Ding-Attribut und geben Sie das Ding-Attribut ein, das Sie in die veröffentlichten MQTT5 Nachrichten aufnehmen möchten. Mithilfe der Konsole können Sie bis zu drei Ding-Attribute hinzufügen.

Wählen Sie im Abschnitt Attribute weitergeben die Option Verbindungsattribut aus und geben Sie den Attributtyp und optional den Attributnamen ein.

5. Fügen Sie optional Tags hinzu. Wählen Sie dann „Dingtyp erstellen“.

   Wenn Sie einen Dingtyp aktualisieren möchten, wählen Sie Dingtyp aktualisieren.

## AWS CLI

1. Führen Sie den Befehl aus, um Übertragungsattribute für die Nachrichtenanreicherung hinzuzufügen AWS CLI, indem Sie mit dem einen neuen Dingtyp erstellen. create-thing-type Ein Beispielbefehl kann der folgende sein.

```
aws iot create-thing-type \
    --thing-type-name "LightBulb" \
    --thing-type-properties "{\"mqtt5Configuration\":{\"propagatingAttributes\":
[{\"userPropertyKey\":\"iot:ClientId\", \"connectionAttribute\":\"iot:ClientId\"},
 {\"userPropertyKey\":\"test\", \"thingAttribute\":\"A\"}]}}" \
```

   Die Ausgabe des Befehls kann wie folgt aussehen.

```
{
 "thingTypeName": "LightBulb",
 "thingTypeArn": "arn:aws:iot:us-west-2:123456789012:thingtype/LightBulb",
 "thingTypeId": "ce3573b0-0a3c-45a7-ac93-4e0ce14cd190"
}
```

2. Führen Sie den update-thing-typeBefehl aus, um die Nachrichtenanreicherung durch Aktualisierung eines Dingtyps mithilfe AWS CLI zu konfigurieren. Beachten Sie, dass Sie nur aktualisieren können`mqtt5Configuration`, wenn Sie diesen Befehl ausführen. Ein Beispielbefehl kann der folgende sein.

```
aws iot update-thing-type \
    --thing-type-name "MyThingType" \
    --thing-type-properties "{\"mqtt5Configuration\":{\"propagatingAttributes\":
[{\"userPropertyKey\":\"iot:ClientId\", \"connectionAttribute\":\"iot:ClientId\"},
 {\"userPropertyKey\":\"test\", \"thingAttribute\":\"A\"}]}}" \
```

   Dieser Befehl liefert keine Ausgabe.

3. Um einen Ding-Typ zu beschreiben, führen Sie den `describe-thing-type` Befehl aus. Dieser Befehl erzeugt eine Ausgabe mit Konfigurationsinformationen zur Nachrichtenanreicherung im `thing-type-properties` Feld. Ein Beispielbefehl kann der folgende sein.

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

Die Ausgabe kann wie folgt aussehen.

```
{
 "thingTypeName": "LightBulb",
 "thingTypeId": "bdf72512-0116-4392-8d79-bf39b17ef73d",
 "thingTypeArn": "arn:aws:iot:us-east-1:123456789012:thingtype/LightBulb",
 "thingTypeProperties": {
  "mqtt5Configuration": {
   "propagatingAttributes": [
    {
     "userPropertyKey": "iot:ClientId",
     "connectionAttribute": "iot:ClientId"
    },
    {
     "userPropertyKey": "test",
     "thingAttribute": "attribute"
    }
   ]
  }
 },
 "thingTypeMetadata": {
  "deprecated": false,
  "creationDate": "2024-10-18T17:37:46.656000+00:00"
 }
}
```

Weitere Informationen finden Sie unter ???.

# Verschlagworten Sie Ihre Ressourcen AWS IoT

Zur einfacheren Verwaltung und Organisation Ihrer Objektgruppen, Objekttypen, Themenregeln, Aufträge, geplanten Audits und Sicherheitsprofile können Sie diesen Ressourcen optional Ihre eigenen Metadaten in Form von Tags zuweisen. In diesem Abschnitt werden Tags und deren Erstellung beschrieben.

Zur besseren Verwaltung der mit Objekten verbundenen Kosten können Sie Abrechnungsgruppen erstellen, die Objekte enthalten. Anschließend können Sie allen diesen Abrechnungsgruppen Tags mit Ihren Metadaten zuweisen. Dieser Abschnitt erläutert auch die Abrechnungsgruppen und die Befehle für ihre Erstellung und Verwaltung.

## Grundlagen zu Tags (Markierungen)

Sie können Tags verwenden, um Ihre AWS IoT Ressourcen auf unterschiedliche Weise zu kategorisieren (z. B. nach Zweck, Eigentümer oder Umgebung). Dies ist nützlich, wenn Sie viele Ressourcen desselben Typs haben. In diesem Fall können Sie schnell bestimmte Ressourcen basierend auf den zugewiesenen Tags bestimmen. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, die Sie beide selbst definieren können. Sie können zum Beispiel eine Reihe von Tags für Ihre Objekttypen definieren, die Ihnen helfen, Ihre Geräte nach Typ nachzuverfolgen. Wir empfehlen die Erstellung von Tag-Schlüsseln, die die Anforderungen der jeweiligen Ressourcenart erfüllen. Die Verwendung einheitlicher Tag-Schlüssel vereinfacht das Verwalten der -Ressourcen.

Sie können die Ressourcen auf Grundlage der hinzugefügten oder angewendeten Tags durchsuchen und filtern. Sie können Abrechnungsgruppentags auch verwenden, um Ihre Kosten zu kategorisieren und zu verfolgen. Sie können auch Tags verwenden, um den Zugriff auf Ihre Ressourcen zu steuern (in Verwenden von Tags mit IAM-Richtlinien beschrieben).

Aus Gründen der Benutzerfreundlichkeit bietet der Tag-Editor in der AWS Management Console eine zentrale, einheitliche Möglichkeit, Ihre Tags zu erstellen und zu verwalten. Weitere Informationen finden Sie unter Arbeiten mit dem Tag-Editor in Arbeiten mit der AWS Management Console.

Sie können auch mit Tags arbeiten, indem Sie die AWS CLI und die verwenden AWS IoT API. Sie können Tags bei der Erstellung mit Objektgruppen, Objekttypen, Themenregeln, Aufträgen, Sicherheitsprofilen und Abrechnungsgruppen verbinden, indem Sie in den folgenden Befehlen das Feld `Tags` verwenden:

- CreateBillingGroup
- CreateDestination
- CreateDeviceProfile
- CreateDynamicThingGroup
- CreateJob
- CreateOTAUpdate
- CreatePolicy
- CreateScheduledAudit
- CreateSecurityProfile
- CreateServiceProfile
- CreateStream
- CreateThingGroup
- CreateThingType
- CreateTopicRule
- CreateWirelessGateway
- CreateWirelessDevice

Sie können Tags für vorhandene Ressourcen, die das Markieren unterstützen, hinzufügen, ändern oder löschen. Verwenden Sie dazu die folgenden Befehle:

- TagResource
- ListTagsForResource
- UntagResource

Sie können Tag (Markierung)-Schlüssel und -Werte bearbeiten und Tags (Markierungen) jederzeit von einer Ressource entfernen. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht null festlegen. Wenn Sie ein Tag (Markierung) mit demselben Schlüssel wie ein vorhandener Tag (Markierung) für die Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben. Wenn Sie eine Ressource löschen, werden alle der Ressource zugeordneten Tags ebenfalls gelöscht.

## Tag-Beschränkungen und -Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Maximale Anzahl von Tags pro Ressource: 50
- Maximale Schlüssellänge — 127 Unicode-Zeichen in UTF -8
- Maximale Wertlänge — 255 Unicode-Zeichen in UTF -8
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden.
- Verwenden Sie nicht das Präfix `aws:` in Ihren Tag-Namen oder -Werten. Es ist für die AWS Verwendung reserviert. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht zum Limit für Tags pro Ressource gezählt.
- Wenn Ihr Markierungsschema für mehrere Services und Ressourcen verwendet wird, denken Sie daran, dass die zulässigen Zeichen bei anderen Services möglicherweise eingeschränkt sind. Zulässige Zeichen sind Buchstaben, Leerzeichen und Zahlen, die in UTF -8 dargestellt werden können, sowie die folgenden Sonderzeichen: + - =. _:/@.

# Verwenden von Tags mit IAM-Richtlinien

Sie können tagbasierte Berechtigungen auf Ressourcenebene in den IAM Richtlinien anwenden, die Sie für Aktionen verwenden. AWS IoT API Dies ermöglicht Ihnen eine bessere Kontrolle darüber, welche Ressourcen ein Benutzer erstellen, ändern oder verwenden kann. Sie können das `Condition`-Element (auch als `Condition`-Block bezeichnet) mit den folgenden Bedingungskontextschlüsseln und Werten in einer IAM-Richtlinie zum Steuern des Benutzerzugriffs (Berechtigungen) basierend auf den Tags einer Ressource verwenden:

- Verwenden Sie `aws:ResourceTag/`*`tag-key`*`: `*`tag-value`*, um Benutzeraktionen für Ressourcen mit bestimmten Tags zuzulassen oder zu verweigern.
- Verwenden Sie diese Option, `aws:RequestTag/`*`tag-key`*`: `*`tag-value`* um vorzuschreiben, dass ein bestimmtes Tag verwendet (oder nicht verwendet) werden muss, wenn Sie eine API Anfrage zum Erstellen oder Ändern einer Ressource stellen, die Tags zulässt.
- Wird verwendet, `aws:TagKeys: [`*`tag-key`*`, ...]` um zu verlangen, dass ein bestimmter Satz von Tag-Schlüsseln verwendet (oder nicht verwendet) wird, wenn eine API Anfrage zum Erstellen oder Ändern einer Ressource gestellt wird, die Tags zulässt.

> **Note**
>
> Die Bedingungskontextschlüssel und -werte in einer IAM Richtlinie gelten nur für AWS IoT Aktionen, bei denen ein Bezeichner für eine Ressource, die markiert werden kann, ein erforderlicher Parameter ist. Beispielsweise DescribeEndpointist die Verwendung von auf der Grundlage von Bedingungskontextschlüsseln und -werten nicht zulässig oder verweigert, weil in dieser Anforderung auf keine markierbare Ressource (Dinggruppen, Dingtypen, Themenregeln, Jobs oder Sicherheitsprofile) verwiesen wird. Weitere Informationen zu markierbaren AWS IoT Ressourcen und Bedingungsschlüsseln, die sie unterstützen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für. AWS IoT

Weitere Informationen finden Sie unter Zugriffssteuerung mit Tags im AWS Identity and Access Management Benutzerhandbuch. Der Abschnitt IAMJSONRichtlinien-Referenz dieses Handbuchs enthält ausführliche Syntax, Beschreibungen und Beispiele der Elemente, Variablen und Bewertungslogik von JSON Richtlinien in. IAM

Die folgende Beispielrichtlinie wendet zwei auf Tags basierende Einschränkungen für die `ThingGroup`-Aktionen an. Ein IAM Benutzer, der durch diese Richtlinie eingeschränkt ist:

- Es kann keine Objektgruppe mit dem Tag „env=prod“ erstellt werden (im Beispiel siehe Zeile `"aws:RequestTag/env" : "prod"`).
- Kann keine Objektgruppe modifizieren oder darauf zugreifen, die den Tag „env=prod“ aufweist (im Beispiel vgl. die Zeile `"aws:ResourceTag/env" : "prod"`).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "iot:CreateThingGroup",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/env": "prod"
        }
      }
    },
    {
```

```
      "Effect": "Deny",
      "Action": [
        "iot:CreateThingGroup",
        "iot:DeleteThingGroup",
        "iot:DescribeThingGroup",
        "iot:UpdateThingGroup"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/env": "prod"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:CreateThingGroup",
        "iot:DeleteThingGroup",
        "iot:DescribeThingGroup",
        "iot:UpdateThingGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

Sie können auch mehrere Tag-Werte für einen bestimmten Tag-Schlüssel angeben, indem Sie sie wie folgt in einer Liste angeben:

```
          "StringEquals" : {
            "aws:ResourceTag/env" : ["dev", "test"]
          }
```

> **Note**
>
> Wenn Sie Benutzern den Zugriff zu Ressourcen auf der Grundlage von Tags (Markierungen) gewähren oder verweigern, müssen Sie daran denken, Benutzern explizit das Hinzufügen und Entfernen dieser Tags (Markierungen) von den jeweiligen Ressourcen unmöglich zu

machen. Andernfalls können Benutzer möglicherweise Ihre Einschränkungen umgehen und sich Zugriff auf eine Ressource verschaffen, indem sie ihre Tags (Markierungen) modifizieren.

## Fakturierungsgruppen

AWS IoT ermöglicht es Ihnen nicht, Tags direkt auf einzelne Dinge anzuwenden, aber es ermöglicht Ihnen, Dinge in Abrechnungsgruppen zu platzieren und diese mit Tags zu versehen. Denn die AWS IoT Zuordnung von Kosten- und Nutzungsdaten auf der Grundlage von Stichwörtern ist auf Abrechnungsgruppen beschränkt.

AWS IoT Core für LoRa WAN Ressourcen, wie z. B. Mobilfunkgeräte und Gateways, können nicht zu Abrechnungsgruppen hinzugefügt werden. Sie können jedoch mit AWS IoT Dingen verknüpft werden, die zu Abrechnungsgruppen hinzugefügt werden können.

Die folgenden Befehle sind verfügbar:

- AddThingToBillingGroup fügt ein Objekt zu einer Abrechnungsgruppe hinzu.
- CreateBillingGroup erstellt eine Abrechnungsgruppe.
- DeleteBillingGroup löscht die Abrechnungsgruppe.
- DescribeBillingGroup gibt Informationen über eine Abrechnungsgruppe zurück.
- ListBillingGroups listet die von Ihnen erstellen Abrechnungsgruppen auf.
- ListThingsInBillingGroup listet die Objekte auf, die Sie der jeweiligen Abrechnungsgruppe hinzugefügt haben.
- RemoveThingFromBillingGroup entfernt das angegebene Objekt aus der Abrechnungsgruppe.
- UpdateBillingGroup aktualisiert die Informationen zu der Abrechnungsgruppe.
- CreateThing ermöglicht es Ihnen, eine Abrechnungsgruppe für das Objekt anzugeben, wenn Sie es erstellen.
- DescribeThing gibt die Beschreibung eines Objekts zusammen mit der Abrechnungsgruppe, zu der das Objekt gehört (falls vorhanden) zurück.

Das AWS IoT WLAN API bietet diese Aktionen, um drahtlose Geräte und Gateways mit AWS IoT Dingen zu verknüpfen.

- AssociateWirelessDeviceWithThing
- AssociateWirelessGatewayWithThing

# Anzeigen von Kostenzuordnungs- und Nutzungsdaten

Sie können Abrechnungsgruppentags verwenden, um Ihre Kosten zu kategorisieren und zu verfolgen. Wenn Sie Stichwörter auf Abrechnungsgruppen (und damit auf die Dinge, die sie beinhalten) anwenden, AWS generiert es einen Kostenverteilungsbericht als Datei mit kommagetrennten Werten (CSV), in der Ihre Nutzung und Kosten nach Ihren Stichwörtern zusammengefasst sind. Sie können Tags anwenden, die geschäftliche Kategorien (wie Kostenstellen, Anwendungsnamen oder Eigentümer) darstellen, um die Kosten für mehrere Services zu organisieren. Weitere Informationen zur Verwendung von Tags für die Kostenzuordnung finden Sie unter Verwenden von Kostenzuordnungs-Tags im Benutzerhandbuch AWS -Fakturierungs- und Kostenverwaltung.

> **Note**
>
> Um Nutzungs- und Kostendaten korrekt den Objekten zuzuordnen, die Sie in Abrechnungsgruppen gesetzt haben, muss jedes Gerät bzw. jede Anwendung die folgenden Bedingungen erfüllen:
>
> - Registriere dich als eine Sache in. AWS IoT Weitere Informationen finden Sie unter Geräte verwalten mit AWS IoT.
> - Stellen Sie eine Connect zum AWS IoT Message Broker her, MQTT indem Sie nur den Namen des Dings als Client-ID verwenden. Weitere Informationen finden Sie unter the section called “Gerätekommunikationsprotokolle”. Wenn Ihre Client-ID nicht mit dem Ding-Namen übereinstimmt, können Sie den exklusiven Ding-Anhang aktivieren, um die Zuordnung herzustellen. Weitere Informationen finden Sie unter ???.
> - Authentifizierung mit einem mit dem Objekt verbundenen Client-Zertifikat.

Für Abrechnungsgruppen sind die folgenden Preisdimensionen verfügbar (basierend auf der Aktivität der mit der Abrechnungsgruppe verbundenen Objekte):

- Verbindung (basierend auf dem Objektnamen, der als Client-ID verwendet wird)
- Nachrichtenübermittlung (nur basierend auf eingehenden Nachrichten von und ausgehenden Nachrichten an ein Objekt; MQTT nur).
- Schattenoperationen (basierend auf dem Objekt, dessen Nachricht eine Schattenaktualisierung ausgelöst hat)

- Ausgelöste Regeln (basierend auf dem Ding, dessen eingehende Nachricht die Regel ausgelöst hat; gilt nicht für Regeln, die durch MQTT Lebenszyklusereignisse ausgelöst wurden).
- Objektindex-Aktualisierungen (basierend auf dem Objekt, das dem Index hinzugefügt wurde)
- Remote-Aktionen (basierend auf dem aktualisierten Objekt)
- AWS IoT Device Defender Berichte erkennen (basierend auf dem Ding, dessen Aktivität gemeldet wird).

Kosten- und Nutzungsdaten, die auf Tags basieren (und für eine Abrechnungsgruppe gemeldet werden) reflektieren nicht die folgenden Aktivitäten:

- Geräte-Registrierungsoperationen (einschließlich Aktualisierungen von Objekten, Objektgruppen und Objekttypen). Weitere Informationen finden Sie unter Geräte verwalten mit AWS IoT).
- Aktualisierungen des Objektgruppenindex (beim Hinzufügen einer Objektgruppe)
- Index-Suchabfragen
- Gerätebereitstellung.
- AWS IoT Device Defender Prüfberichte.

# Sicherheit in AWS IoT

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für gelten AWS IoT, finden Sie unter AWS Services in Umfang nach Compliance-Programmen.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, einschließlich der Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können AWS IoT. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS IoT , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS IoT Ressourcen unterstützen.

Themen


- AWS IoT Sicherheit
- Authentifizierung
- Autorisierung
- Datenschutz in AWS IoT Core
- Identitäts- und Zugriffsmanagement für AWS IoT
- Protokollieren und Überwachen
- Überprüfung der Einhaltung der Vorschriften für AWS IoT Core
- Resilienz im AWS IoT-Kern

- Verwendung AWS IoT Core mit VPC-Endpunkten mit Schnittstelle
- Sicherheit der Infrastruktur in AWS IoT
- Sicherheitsüberwachung von Produktionsflotten oder Geräten mit Core AWS IoT
- Bewährte Sicherheitsmethoden in AWS IoT Core
- AWS Schulung und Zertifizierung

# AWS IoT Sicherheit

Jedes verbundene Gerät oder jeder verbundene Client muss über eine Berechtigung verfügen, um mit AWS IoT zu interagieren. Der gesamte Verkehr zu und von AWS IoT dort wird sicher über Transport Layer Security (TLS) gesendet. AWS Cloud-Sicherheitsmechanismen schützen Daten, wenn sie zwischen AWS IoT und anderen AWS Diensten übertragen werden.

- Sie sind für die Verwaltung von Geräte-Anmeldeinformationen (X.509-Zertifikate, AWS - Anmeldeinformationen, Amazon Cognito-Identitäten, Verbundidentitäten oder benutzerdefinierte Authentifizierungstoken) und Richtlinien in AWS IoT verantwortlich. Weitere Informationen finden Sie unter Schlüsselverwaltung in AWS IoT. Sie sind dafür verantwortlich, jedem Gerät eindeutige Identitäten zuzuweisen und die Berechtigungen für jedes Gerät oder jede Gerätegruppe zu verwalten.
- Ihre Geräte stellen AWS IoT mithilfe von X.509-Zertifikaten oder Amazon Cognito Cognito-Identitäten über eine sichere TLS-Verbindung eine Verbindung her. Während der Forschung und Entwicklung sowie für einige Anwendungen, die API-Aufrufe tätigen oder verwenden WebSockets, können Sie sich auch mithilfe von IAM-Benutzern und -Gruppen oder benutzerdefinierten

Authentifizierungstoken authentifizieren. Weitere Informationen finden Sie unter IAM-Benutzer, -Gruppen und -Rollen.

- Wenn Sie die AWS IoT Authentifizierung verwenden, ist der Message Broker dafür verantwortlich, Ihre Geräte zu authentifizieren, Gerätedaten sicher aufzunehmen und Zugriffsberechtigungen zu gewähren oder zu verweigern, die Sie mithilfe von Richtlinien für Ihre Geräte angeben. AWS IoT
- Wenn Sie die benutzerdefinierte Authentifizierung verwenden, ist ein benutzerdefinierter Autorisierer dafür verantwortlich, Ihre Geräte zu authentifizieren und Zugriffsberechtigungen zu gewähren oder zu verweigern, die Sie für Ihre Geräte mithilfe unserer IAM-Richtlinien angeben. AWS IoT
- Die AWS IoT Regel-Engine leitet Gerätedaten gemäß den von Ihnen definierten Regeln an andere Geräte oder AWS Dienste weiter. Es dient AWS Identity and Access Management dazu, Daten sicher an ihren Bestimmungsort zu übertragen. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT.

# Authentifizierung

Die Authentifizierung ist ein Mechanismus, mit dem Sie die Identität eines Clients oder Servers überprüfen können. Bei der Serverauthentifizierung stellen Geräte oder andere Clients sicher, dass sie mit einem tatsächlichen AWS IoT Endpunkt kommunizieren. Die Client-Authentifizierung ist der Prozess, bei dem sich Geräte oder andere Clients selbst authentifizieren. AWS IoT

## Übersicht zum X.509-Zertifikat

X.509-Zertifikate sind digitale Zertifikate, die den X.509-Standard für Public-Key-Infrastrukturen verwenden, um einen öffentlichen Schlüssel mit einer Identität in einem Zertifikat zu verknüpfen. X.509-Zertifikate werden von einer vertrauenswürdigen Entität ausgegeben, die als Zertifizierungsstelle (Certificate Authority, CA) bezeichnet wird. Die CA nutzen ein oder mehrere spezielle Zertifikate, die als CA-Zertifikate bezeichnet werden, zum Herausgeben der X.509-Zertifikate. Nur die Zertifizierungsstelle kann auf CA-Zertifikate zugreifen. X.509-Zertifikatsketten werden sowohl für die Serverauthentifizierung durch Clients als auch für die Clientauthentifizierung durch den Server verwendet.

## Serverauthentifizierung

Wenn Ihr Gerät oder ein anderer Client versucht, eine Verbindung herzustellen AWS IoT Core, sendet der AWS IoT Core Server ein X.509-Zertifikat, mit dem Ihr Gerät den Server authentifiziert.

Die Authentifizierung erfolgt auf der TLS-Ebene durch die Validierung der X.509-Zertifikatskette. Dies ist dieselbe Methode, die Ihr Browser verwendet, wenn Sie eine HTTPS-URL besuchen. Informationen zum Verwenden von Zertifikaten von Ihrer eigenen Zertifizierungsstelle finden Sie unter Verwalten eigener CA-Zertifikate.

Wenn Ihre Geräte oder andere Clients eine TLS-Verbindung zu einem AWS IoT Core Endpunkt aufbauen, wird eine Zertifikatskette AWS IoT Core angezeigt, anhand derer die Geräte überprüfen, ob sie mit einem anderen Server kommunizieren AWS IoT Core und nicht, der sich als ein anderer Server ausgibt. AWS IoT Core Welche Kette angezeigt wird, hängt von einer Kombination aus dem Endpunkttyp, zu dem das Gerät eine Verbindung herstellt, und der Cipher Suite ab, die der Client und die während des TLS-Handshakes AWS IoT Core ausgehandelt haben.

## Endpunkttypen

AWS IoT Core unterstützt. `iot:Data-ATS` `iot:Data-ATS`Endgeräte legen ein Serverzertifikat vor, das von einer Amazon Trust Services-Zertifizierungsstelle signiert wurde.

Zertifikate, die von ATS-Endpunkten vorgewiesen werden, sind von Starfield gegensigniert. Einige TLS-Client-Implementierungen erfordern die Überprüfung der Vertrauenswürdigkeit und die Installation der Starfield CA-Zertifikate in den Vertrauensspeichern des Clients.

> **Warning**
>
> Die Verwendung einer Zertifikat-Pinning-Methode, die das gesamte Zertifikat (einschließlich des Ausstellernamens usw.) hasht, wird nicht empfohlen, da dies zum Scheitern der Zertifikatsprüfung führt, da die von uns bereitgestellten ATS-Zertifikate von Starfield gegensigniert sind und einen anderen Ausstellernamen haben.

> **Important**
>
> Verwenden Sie `iot:Data-ATS` Endpunkte. Zertifikate von Symantec und Verisign sind veraltet und werden von nicht mehr unterstützt. AWS IoT Core

Sie können den Befehl `describe-endpoint` verwenden, um Ihren ATS-Endpunkt zu erstellen.

```
aws iot describe-endpoint --endpoint-type iot:Data-ATS
```

Der Befehl `describe-endpoint` gibt einen Endpunkt im folgenden Format zurück.

```
account-specific-prefix.iot.your-region.amazonaws.com
```

> **Note**
>
> Beim ersten Aufruf von `describe-endpoint` wird ein Endpunkt erstellt. Alle nachfolgenden Aufrufe von `describe-endpoint` geben den gleichen Endpunkt zurück.

> **Note**
>
> Um Ihren **`iot:Data-ATS`** Endpunkt in der Konsole zu sehen, wählen Sie Einstellungen AWS IoT Core . Die Konsole zeigt nur den `iot:Data-ATS`-Endpunkt an.

### Erstellen eines **`IotDataPlaneClient`** mit dem AWS SDK for Java

Um eine zu erstellen`IotDataPlaneClient`, die einen `iot:Data-ATS` Endpunkt verwendet, müssen Sie wie folgt vorgehen.

- Erstellen Sie mithilfe der DescribeEndpointAPI einen `iot:Data-ATS` Endpunkt.
- Geben Sie diesen Endpunkt an, wenn Sie den `IotDataPlaneClient` erstellen.

Im folgenden Beispiel werden beide Operationen ausgeführt.

```
public void setup() throws Exception {
        IotClient client =
 IotClient.builder().credentialsProvider(CREDENTIALS_PROVIDER_CHAIN).region(Region.US_EAST_1).b
        String endpoint = client.describeEndpoint(r -> r.endpointType("iot:Data-
ATS")).endpointAddress();
        iot = IotDataPlaneClient.builder()
                                .credentialsProvider(CREDENTIALS_PROVIDER_CHAIN)
                                .endpointOverride(URI.create("https://" + endpoint))
                                .region(Region.US_EAST_1)
                                .build();
}
```

## CA-Zertifikate für die Serverauthentifizierung

Je nachdem, welchen Typ von Datenendpunkt Sie verwenden und welche Verschlüsselungssuite Sie ausgehandelt haben, werden AWS IoT Core Serverauthentifizierungszertifikate mit einem der folgenden Root-CA-Zertifikate signiert:

Amazon Trust Services-Endpunkte (bevorzugt)

> **Note**
>
> Möglicherweise müssen Sie mit der rechten Maustaste auf diese Links klicken und Link speichern unter... auswählen, um diese Zertifikate als Dateien zu speichern.

- RSA 2048-Bit-Schlüssel: Amazon Root CA 1.
- RSA 4096-Bit-Schlüssel: Amazon Root CA 2. Für die spätere Verwendung reserviert.
- ECC-256-Bit-Schlüssel: Amazon Root CA 3.
- ECC-384-Bit-Schlüssel: Amazon Root CA 4. Für die spätere Verwendung reserviert.

Diese Zertifikate werden alle durch das Starfield Root CA-Zertifikat signiert. Alle neuen AWS IoT Core Regionen, beginnend mit der Markteinführung von AWS IoT Core in der Region Asien-Pazifik (Mumbai) am 9. Mai 2018, bieten ausschließlich ATS-Zertifikate an.

VeriSign Endgeräte (veraltet)

- RSA 2048-Bit-Schlüssel: Öffentliches primäres G5-Root-CA-Zertifikat der VeriSign Klasse 3

## Richtlinien für die Serverauthentifizierung

Es gibt viele Variablen, die die Fähigkeit eines Geräts zur Überprüfung des AWS IoT Core -Server-Authentifizierungszertifikats beeinflussen können. So können beispielsweise Geräte zu speicherbeschränkt sein, um alle möglichen Root-CA-Zertifikate aufzunehmen, oder Geräte können eine nicht standardmäßige Methode der Zertifikatsvalidierung implementieren. Aus diesen Gründen empfehlen wir, diese Richtlinien zu befolgen:

- Wir empfehlen, dass Sie Ihren ATS-Endpunkt verwenden und alle unterstützten Amazon Root CA-Zertifikate installieren.

- Wenn Sie nicht alle diese Zertifikate auf Ihrem Gerät speichern können und wenn Ihre Geräte keine ECC-basierte Validierung verwenden, können Sie die ECC-Zertifikate Amazon Root CA 3 und Amazon Root CA 4 weglassen. Wenn Ihre Geräte keine RSA-basierte Zertifikatsvalidierung implementieren, können Sie die RSA-Zertifikate Amazon Root CA 1 und Amazon Root CA 2 weglassen. Möglicherweise müssen Sie mit der rechten Maustaste auf diese Links klicken und Link speichern unter... auswählen, um diese Zertifikate als Dateien zu speichern.
- Wenn bei der Verbindung mit Ihrem ATS-Endpunkt Probleme bei der Validierung von Serverzertifikaten auftreten, versuchen Sie, das entsprechende signierte Amazon Root CA-Zertifikat in Ihrem Vertrauensspeicher hinzuzufügen. Möglicherweise müssen Sie mit der rechten Maustaste auf diese Links klicken und Link speichern unter... auswählen, um diese Zertifikate als Dateien zu speichern.
  - Gegensigniertes Amazon Root CA 1
  - Gegensigniertes Amazon Root CA 2: Für die spätere Verwendung reserviert.
  - Gegensigniertes Amazon Root CA 3
  - Gegensigniertes Amazon Root CA 4: Für die spätere Verwendung reserviert.
- Wenn bei der Validierung von Serverzertifikaten Probleme auftreten, muss Ihr Gerät möglicherweise explizit der Stammzertifizierungsstelle vertrauen. Versuchen Sie, das Starfield Root CA Certificate zu Ihrem Trust Store hinzuzufügen.
- Wenn nach der Ausführung der obigen Schritte immer noch Probleme auftreten, wenden Sie sich bitte an den AWS -Developer Support.

> **Note**
>
> CA-Zertifikate haben ein Ablaufdatum, nach dem sie nicht mehr zur Validierung eines Serverzertifikats verwendet werden können. Es kann sein, dass CA-Zertifikate vor ihrem Ablaufdatum ersetzt werden müssen. Stellen Sie sicher, dass Sie die CA-Stammzertifikate auf all Ihren Geräten oder Clients aktualisieren können, um eine ununterbrochene Verbindung sicherzustellen und bei bewährten Sicherheitsmethoden stets auf dem aktuellen Stand zu sein.

> **Note**
>
> Wenn Sie AWS IoT Core in Ihrem Gerätecode eine Verbindung herstellen, übergeben Sie das Zertifikat an die API, die Sie für die Verbindung verwenden. Die von Ihnen verwendete API hängt vom SDK ab. Weitere Informationen finden Sie unter AWS IoT Core Gerät SDKs.

## Client-Authentifizierung

AWS IoT unterstützt drei Arten von Identitätsprinzipalen für die Geräte- oder Client-Authentifizierung:

- X.509-Clientzertifikate
- IAM-Benutzer, -Gruppen und -Rollen
- Amazon-Cognito-Identitäten

Diese Identitäten können mit Geräten, mobilen, Web- oder Desktop-Anwendungen verwendet werden. Sie können sogar von Benutzern verwendet werden, die Befehle der AWS IoT Befehlszeilenschnittstelle (CLI) eingeben. In der Regel verwenden AWS IoT Geräte X.509-Zertifikate, während mobile Anwendungen Amazon Cognito Cognito-Identitäten verwenden. Web- und Desktop-Anwendungen verwenden IAM- oder Verbundidentitäten. AWS CLI -Befehle verwenden IAM. Weitere Informationen zu IAM-Identitäten finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT.

### X.509-Clientzertifikate

X.509-Zertifikate bieten die Möglichkeit, AWS IoT Client- und Geräteverbindungen zu authentifizieren. Client-Zertifikate müssen registriert werden, AWS IoT bevor ein Client mit ihnen kommunizieren kann. AWS IoT Ein Client-Zertifikat kann für mehrere AWS-Konto s in derselben Region registriert werden AWS-Region , um das Verschieben von Geräten zwischen Ihren AWS-Konto s in derselben Region zu erleichtern. Weitere Informationen finden Sie unter Verwendung von X.509-Clientzertifikaten in mehreren AWS-Konto s mit Registrierung mehrerer Konten.

Wir empfehlen, jedem Gerät oder Client ein eindeutiges Zertifikat zuzuordnen, damit feingranulare Client-Verwaltungsaktionen einschließlich Zertifikatswiderruf möglich sind. Geräte und Clients müssen darüber hinaus das Rotieren und Ersetzen von Zertifikaten unterstützen, um eine reibungslose Ausführung sicherzustellen, wenn Zertifikate ablaufen.

Informationen zur Verwendung von X.509-Zertifikaten zur Unterstützung mehrerer Geräte finden Sie unter Gerätebereitstellung. Dort sind die verschiedenen Optionen für die Zertifikatsverwaltung und -bereitstellung aufgeführt, die von AWS IoT unterstützt werden.

AWS IoT unterstützt die folgenden Typen von X.509-Client-Zertifikaten:

- X.509-Zertifikate, generiert von AWS IoT
- X.509-Zertifikate, signiert von einer Zertifizierungsstelle, die bei registriert ist. AWS IoT
- Von einer nicht bei AWS IoT registrierten Zertifizierungsstelle signierte X.509-Zertifikate

In diesem Abschnitt wird beschrieben, wie Sie X.509-Zertifikate in AWS IoT verwalten. Sie können die AWS IoT Konsole verwenden oder AWS CLI die folgenden Zertifikatsvorgänge ausführen:

- Erstellen Sie AWS IoT Client-Zertifikate
- Erstellen eigener Clientzertifikate
- Registrieren eines Clientzertifikats
- Aktivieren oder Deaktivieren eines Clientzertifikats
- Widerrufen eines Clientzertifikats

Weitere Informationen zu den AWS CLI Befehlen, die diese Operationen ausführen, finden Sie unter AWS IoT CLI-Referenz.

Verwenden von X.509-Clientzertifikaten

X.509-Zertifikate authentifizieren Client- und Geräteverbindungen zu. AWS IoT X.509-Zertifikate bieten mehrere Vorteile gegenüber anderen Identifikations- und Authentifizierungsmechanismen. X.509-Zertifikate ermöglichen die Verwendung asymmetrischer Schlüssel mit Geräten. Beispielsweise könnten Sie private Schlüssel nutzen und sicher auf einem Gerät aufbewahren, sodass vertrauliches kryptografisches Material das Gerät niemals verlässt. X.509-Zertifikate bieten eine stärkere Client-Authentifizierung als andere Systeme, wie z. B. Benutzername und Passwort oder Bearer-Token, da der private Schlüssel das Gerät nie verlässt.

AWS IoT authentifiziert Client-Zertifikate mithilfe des Client-Authentifizierungsmodus des TLS-Protokolls. TLS-Unterstützung ist in vielen Programmiersprachen und Betriebssystemen verfügbar und stellt die gängige Verschlüsselungsmethode für Daten dar. AWS IoT Fordert bei der TLS-Client-Authentifizierung ein X.509-Client-Zertifikat an und validiert den Status des Zertifikats AWS-Konto anhand einer Zertifikatsregistrierung. Anschließend fordert es den Client auf, den Besitz des privaten

Schlüssels nachzuweisen, der dem im Zertifikat enthaltenen öffentlichen Schlüssel entspricht. AWS IoT verlangt von den Clients, die Server Name Indication (SNI) -Erweiterung an das Transport Layer Security (TLS) -Protokoll zu senden. Weitere Informationen zum Konfigurieren der SNI-Erweiterung finden Sie unter Transportsicherheit in AWS IoT Core.

Um eine sichere und konsistente Client-Verbindung zum AWS IoT Core zu ermöglichen, muss ein X.509-Client-Zertifikat über Folgendes verfügen:

- In AWS IoT Core registriert. Weitere Informationen finden Sie unter Registrieren eines Clientzertifikats.
- Über den Status „`ACTIVE`“ verfügen. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren eines Clientzertifikats.
- Das Ablaufdatum des Zertifikats ist noch nicht erreicht.

Sie können Clientzertifikate erstellen, die die Amazon Root CA verwenden, und Sie können Ihre eigenen von einer anderen Zertifizierungsstelle (Certificate Authority, CA) signierten Clientzertifikate verwenden. Weitere Informationen zur Verwendung der AWS IoT Konsole zum Erstellen von Zertifikaten, die die Amazon Root-CA verwenden, finden Sie unterErstellen Sie AWS IoT Client-Zertifikate. Weitere Informationen zur Verwendung eigener X.509-Zertifikate finden Sie unter Erstellen eigener Clientzertifikate.

Der Ablaufzeitpunkt für mit einem CA-Zertifikat signierte Zertifikate wird bei der Erstellung des entsprechenden Zertifikats festgelegt. Von generierte X.509-Zertifikate AWS IoT laufen am 31. Dezember 2049 um Mitternacht UTC ab (2049-12-31T 23:59:59 Z).

AWS IoT Device Defender kann Audits an Ihren Geräten durchführen AWS-Konto und dabei die gängigen Best Practices für die IoT-Sicherheit unterstützen. Dazu gehört die Verwaltung der Ablaufdaten von X.509-Zertifikaten, die von Ihrer CA oder der Amazon Root CA signiert wurden. Weitere Informationen zur Verwaltung des Ablaufdatums eines Zertifikats finden Sie unter Ablaufen von Gerätezertifikaten und Ablaufende Zertifizierungsstellenzertifikate.

Im offiziellen AWS IoT Blog finden Sie einen tieferen Einblick in die Verwaltung der Rotation von Gerätezertifikaten und bewährte Sicherheitsmethoden unter So verwalten Sie die Rotation von IoT-Gerätezertifikaten mithilfe von AWS IoT.

Verwendung von X.509-Clientzertifikaten in mehreren AWS-Konto s mit Registrierung mehrerer Konten

Die Registrierung für mehrere Konten ermöglicht das Verschieben von Geräten zwischen Ihren AWS-Konto innerhalb derselben Region oder in unterschiedlichen Regionen. Sie können ein Gerät in einem Testkonto registrieren, testen und konfigurieren und dasselbe Gerät samt Gerätezertifikat anschließend in einem Produktionskonto registrieren und verwenden. Sie können auch das Client-Zertifikat auf dem Gerät oder die Gerätezertifikate ohne registrierte Zertifizierungsstelle registrieren. AWS IoT Weitere Informationen finden Sie unter Registrieren eines Clientzertifikats, das von einer nicht registrierten CA (CLI) signiert wurde.

> **Note**
>
> Zertifikate, die für die Registrierung mehrerer Konten verwendet werden, werden auf den Endpunkttypen `iot:Data-ATS`, `iot:Data` (Legacy), `iot:Jobs` und `iot:CredentialProvider` unterstützt. Weitere Informationen zu AWS IoT Geräteendpunkten finden Sie unterAWS IoT Gerätedaten und Dienstendpunkte.

Geräte, die die Registrierung mehrerer Konten verwenden, müssen die Server Name Indication (SNI) -Erweiterung an das Transport Layer Security (TLS) -Protokoll senden und die vollständige Endpunktadresse im `host_name` Feld angeben, wenn sie eine Verbindung herstellen. AWS IoT AWS IoT verwendet die Endpunktadresse`host_name`, um die Verbindung zum richtigen AWS IoT Konto weiterzuleiten. Vorhandene Geräte, die keine gültige Endpunktadresse in `host_name` senden, funktionieren weiterhin, können aber die Funktionen nicht nutzen, für die diese Informationen benötigt werden. Weitere Informationen zur SNI-Erweiterung und zum Identifizieren der Endpunktadresse für das Feld `host_name` finden Sie unter Transportsicherheit in AWS IoT Core.

So verwenden Sie die Registrierung für mehrere Konten

1. Sie können die Gerätezertifikate ohne Zertifizierungsstelle registrieren. Sie können die signierende Zertifizierungsstelle in mehreren Konten im `SNI_ONLY`-Modus registrieren und diese Zertifizierungsstelle verwenden, um dasselbe Clientzertifikat für mehrere Konten zu registrieren. Weitere Informationen finden Sie unter Registrieren Sie ein CA-Zertifikat im SNI_ONLY-Modus (CLI) – Empfohlen.
2. Sie können die Gerätezertifikate ohne Zertifizierungsstelle registrieren. Siehe Registrieren eines von einer nicht registrierten CA signierten Clientzertifikats (CLI). Die Registrierung einer

Zertifizierungsstelle ist optional. Sie müssen die Zertifizierungsstelle, mit der die Gerätezertifikate signiert wurden, nicht registrieren AWS IoT.

Algorithmen zum Signieren von Zertifikaten werden unterstützt von AWS IoT

AWS IoT unterstützt die folgenden Algorithmen zum Signieren von Zertifikaten:

- SHA256MIT RSA
- SHA384MIT RSA
- SHA512MIT RSA
- SHA256WITHRSAANDMGF1 (RSASSA-PSS)
- SHA384WITHRSAANDMGF1 (RSSA-PSS)
- SHA512WITHRSAANDMGF1 (RSSA-PSS)
- DSA_MIT_ SHA256
- ECDSA-MIT- SHA256
- ECDSA-MIT- SHA384
- ECDSA-MIT- SHA512

Weitere Informationen zur Authentifizierung und Sicherheit von Zertifikaten finden Sie unter Qualität der Gerätezertifikatschlüssel.

> **Note**
>
> Die Zertifikatssignierungsanforderung (Certificate Signing Request, CSR) muss einen öffentlichen Schlüssel enthalten. Bei dem Schlüssel kann es sich entweder um einen RSA-Schlüssel mit einer Länge von mindestens 2048 Bit oder um einen ECC-Schlüssel aus NIST P-256, NIST P-384 oder NIST P-521-Kurven handeln. Weitere Informationen finden Sie unter CreateCertificateFromCsr in der AWS IoT -API-Referenz.

Schlüsselalgorithmen werden unterstützt von AWS IoT

Die folgende Tabelle zeigt, wie Schlüsselalgorithmen unterstützt werden:

| Schlüsselalgorithmus | Algorithmus zum Signieren von Zertifikaten | TLS-Version | Unterstützt? Sie können zwischen Yes und No wählen |
|---|---|---|---|
| RSA mit einer Schlüssel größe von mindestens 2048 Bit | Alle | TLS 1.2 TLS 1.3 | Ja |
| ECC IST P-256/P-384/P-521 | Alle | TLS 1.2 TLS 1.3 | Ja |
| RSA-PSS mit einer Schlüsselgröße von mindestens 2048 Bit | Alle | TLS 1.2 | Nein |
| RSA-PSS mit einer Schlüsselgröße von mindestens 2048 Bit | Alle | TLS 1.3 | Ja |

Um ein Zertifikat mithilfe von CreateCertificateFromCSR zu erstellen, können Sie einen unterstützten Schlüsselalgorithmus verwenden, um einen öffentlichen Schlüssel für Ihre CSR zu generieren. Um Ihr eigenes Zertifikat mit RegisterCertificateunserer RegisterCertificateWithoutCA zu registrieren, können Sie einen unterstützten Schlüsselalgorithmus verwenden, um einen öffentlichen Schlüssel für das Zertifikat zu generieren.

Weitere Informationen finden Sie unter Sicherheitsrichtlinien.

Erstellen Sie AWS IoT Client-Zertifikate

AWS IoT stellt Client-Zertifikate bereit, die von der Amazon Root Certificate Authority (CA) signiert wurden.

In diesem Thema wird beschrieben, wie Sie ein von der Amazon Root-Zertifizierungsstelle signiertes Clientzertifikat erstellen und die Zertifikatsdateien herunterladen. Nachdem Sie die Clientzertifikatdateien erstellt haben, müssen Sie sie auf dem Client installieren.

> **Note**
>
> Jedes von bereitgestellte X.509-Client-Zertifikat AWS IoT enthält die Attribute des Ausstellers und des Antragstellers, die Sie bei der Erstellung des Zertifikats festgelegt haben. Die Zertifikatsattribute können erst ab der Erstellung des Zertifikats nicht mehr modifiziert werden.

Sie können die AWS IoT Konsole oder die verwenden AWS CLI , um ein von der Amazon Root-Zertifizierungsstelle signiertes AWS IoT Zertifikat zu erstellen.

Erstellen Sie ein AWS IoT Zertifikat (Konsole)

Um ein AWS IoT Zertifikat mit der AWS IoT Konsole zu erstellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im Navigationsbereich Sichern, Zertifikate und anschließend Erstellen.
3. Wählen Sie Zertifikat mit einem Klick erstellen (empfohlen) und dann Zertifikat erstellen.
4. Laden Sie die Clientzertifikatdateien für das Objekt, den öffentlichen Schlüssel und den privaten Schlüssel auf der Seite Zertifikat erstellt! an einen sicheren Speicherort herunter. Diese von generierten Zertifikate AWS IoT sind nur für die Verwendung mit AWS IoT Diensten verfügbar.

   Wenn Sie auch die Amazon-Root-CA-Zertifikatdatei benötigen, finden Sie auf dieser Seite auch den Link zu der Seite, auf der Sie sie herunterladen können.
5. Es wurde nun ein Clientzertifikat erstellt und bei AWS IoT registriert. Sie müssen das Zertifikat aktivieren, bevor Sie es in einem Client verwenden.

   Wählen Sie Aktivieren, um das Clientzertifikat jetzt zu aktivieren. Wenn Sie das Zertifikat jetzt nicht aktivieren möchten, können Sie unter Aktivieren eines Clientzertifikats (Konsole) erfahren, wie Sie das Zertifikat zu einem späteren Zeitpunkt aktivieren können.
6. Wenn Sie eine Richtlinie an das Zertifikat anfügen möchten, wählen Sie Anfügen einer Richtlinie.

   Wenn Sie jetzt keine Richtlinie anfügen möchten, wählen Sie Fertig , um den Vorgang abzuschließen. Sie können zu einem späteren Zeitpunkt eine Richtlinie anfügen.

Wenn Sie den Vorgang abgeschlossen haben, installieren Sie die Zertifikatdateien auf dem Client.

### AWS IoT Zertifikat erstellen (CLI)

Das AWS CLI bietet den create-keys-and-certificate Befehl zum Erstellen von Client-Zertifikaten, die von der Amazon Root-Zertifizierungsstelle signiert wurden. Mit diesem Befehl wird die Amazon Root-CA-Zertifikatdatei jedoch nicht heruntergeladen. Sie können die Amazon Root-CA-Zertifikatdatei von CA-Zertifikate für die Serverauthentifizierung herunterladen.

Dieser Befehl erstellt private Schlüssel-, öffentliche Schlüssel- und X.509-Zertifikatsdateien und registriert und aktiviert das Zertifikat mit AWS IoT.

```
aws iot create-keys-and-certificate \
    --set-as-active \
    --certificate-pem-outfile certificate_filename.pem \
    --public-key-outfile public_filename.key \
    --private-key-outfile private_filename.key
```

Wenn Sie das Zertifikat beim Erstellen und Registrieren nicht aktivieren möchten, erstellt dieser Befehl einen privaten und einen öffentlichen Schlüssel sowie X.509-Zertifikatdateien und registriert das Zertifikat, aktiviert es jedoch nicht. Unter Aktivieren eines Clientzertifikats (CLI) wird beschrieben, wie Sie das Zertifikat zu einem späteren Zeitpunkt aktivieren können.

```
aws iot create-keys-and-certificate \
    --no-set-as-active \
    --certificate-pem-outfile certificate_filename.pem \
    --public-key-outfile public_filename.key \
    --private-key-outfile private_filename.key
```

Installieren Sie die Zertifikatdateien auf dem Client.

### Erstellen eigener Clientzertifikate

AWS IoT unterstützt Client-Zertifikate, die von beliebigen Stamm- oder Zwischenzertifizierungsstellen (CA) signiert wurden. AWS IoT verwendet CA-Zertifikate, um den Besitz von Zertifikaten zu überprüfen. Um Gerätezertifikate verwenden zu können, die von einer Zertifizierungsstelle signiert wurden, die nicht die Zertifizierungsstelle von Amazon ist, muss das Zertifikat der Zertifizierungsstelle registriert sein, AWS IoT damit wir den Besitz des Gerätezertifikats überprüfen können.

AWS IoT unterstützt mehrere Möglichkeiten, eigene Zertifikate mitzubringen (BYOC):

- Registrieren Sie zunächst die Zertifizierungsstelle, die zum Signieren der Clientzertifikate verwendet wird, und registrieren Sie dann einzelne Clientzertifikate. Wenn Sie das Gerät oder den Client bei der ersten Verbindung mit seinem Client-Zertifikat registrieren möchten AWS IoT (auch bekannt als Just-in-Time-Provisioning), müssen Sie die signierende Zertifizierungsstelle bei AWS IoT registrieren und die automatische Registrierung aktivieren.
- Wenn Sie die signierende Zertifizierungsstelle nicht registrieren können, können Sie Clientzertifikate auch ohne CA registrieren. Bei Geräten, die ohne CA registriert sind, müssen Sie Server Name Indication (SNI) angeben, wenn Sie eine Verbindung zu AWS IoT herstellen.

> **Note**
>
> Um Client-Zertifikate mithilfe einer Zertifizierungsstelle zu registrieren, müssen Sie die signierende Zertifizierungsstelle bei AWS IoT keiner anderen Zertifizierungsstelle in der Hierarchie registrieren. CAs

> **Note**
>
> Ein CA-Zertifikat kann nur im `DEFAULT`-Modus von einem Konto in einer Region registriert werden. Ein CA-Zertifikat kann nur im `SNI_ONLY`-Modus von mehreren Konten in einer Region registriert werden.

Weitere Informationen zur Verwendung von X.509-Zertifikaten zur Unterstützung mehrerer Geräte finden Sie unter Gerätebereitstellung. Dort sind die verschiedenen Optionen für die Zertifikatsverwaltung und -bereitstellung aufgeführt, die von AWS IoT unterstützt werden.

Themen

- Verwalten eigener CA-Zertifikate
- Erstellen eines Clientzertifikats mit Ihrem CA-Zertifikat

## Verwalten eigener CA-Zertifikate

In diesem Abschnitt werden allgemeine Aufgaben für die Verwaltung eigener Zertifizierungsstellenzertifikate (Certificate Authority, CA) beschrieben.

Sie können Ihre Zertifizierungsstelle (CA) bei registrieren, AWS IoT wenn Sie Client-Zertifikate verwenden, die von einer Zertifizierungsstelle signiert wurden, die diese AWS IoT nicht erkennt.

Wenn Sie möchten, dass Clients ihre Client-Zertifikate AWS IoT bei der ersten Verbindung automatisch registrieren, muss die Zertifizierungsstelle, die die Client-Zertifikate signiert hat, bei der registriert sein AWS IoT. Andernfalls müssen Sie das CA-Zertifikat, das die Clientzertifikate signiert hat, nicht registrieren.

> **Note**
>
> Ein CA-Zertifikat kann nur im `DEFAULT`-Modus von einem Konto in einer Region registriert werden. Ein CA-Zertifikat kann nur im `SNI_ONLY`-Modus von mehreren Konten in einer Region registriert werden.

Themen:


- So erstellen Sie ein CA-Zertifikat
- Registrieren eines CA-Zertifikats
- Deaktivieren eines CA-Zertifikats


## So erstellen Sie ein CA-Zertifikat

Wenn Sie kein CA-Zertifikat besitzen, können Sie OpenSSL-v1.1.1i-Tools verwenden, um ein Zertifikat zu erstellen.

> **Note**
>
> Sie können dieses Verfahren nicht in der AWS IoT Konsole ausführen.

So erstellen Sie ein CA-Zertifikat mit OpenSSL-v1.1.1i-Tools.

1. Erzeugen Sie ein Schlüsselpaar.

   ```
   openssl genrsa -out root_CA_key_filename.key 2048
   ```

2. Verwenden Sie den privaten Schlüssel des Schlüsselpaars zur Erzeugung eines CA-Zertifikats.

   ```
   openssl req -x509 -new -nodes \
   ```

```
    -key root_CA_key_filename.key \
    -sha256 -days 1024 \
    -out root_CA_cert_filename.pem
```

### Registrieren eines CA-Zertifikats

Diese Verfahren beschreiben, wie Sie ein Zertifikat von einer Zertifizierungsstelle (CA) registrieren, die nicht die Zertifizierungsstelle von Amazon ist. AWS IoT Core verwendet CA-Zertifikate, um den Besitz von Zertifikaten zu überprüfen. Um Gerätezertifikate zu verwenden, die von einer Zertifizierungsstelle signiert wurden, bei der es sich nicht um die Zertifizierungsstelle von Amazon handelt, müssen Sie das CA-Zertifikat registrieren, AWS IoT Core damit die Inhaberschaft des Gerätezertifikats verifiziert werden kann.

#### Registrieren eines CA-Zertifikats (Konsole)

> **Note**
>
> Starten Sie die Konsole unter CA-Zertifikat registrieren, um ein CA-Zertifikat in der Konsole zu registrieren. Sie können Ihre CA im Modus für mehrere Konten registrieren, ohne dass Sie ein Verifizierungszertifikat bereitstellen müssen oder Zugriff auf den privaten Schlüssel benötigen. Eine CA kann im Modus für mehrere Konten von mehreren AWS-Konten gleichzeitig in derselben AWS-Region registriert werden. Sie können Ihre CA im Einzelkonto-Modus registrieren, indem Sie ein Verifizierungszertifikat und einen Eigentumsnachweis für den privaten Schlüssel der CA vorlegen.

#### Registrieren eines CA-Zertifikats (CLI)

Sie können ein CA-Zertifikat im `DEFAULT`-Modus oder im `SNI_ONLY`-Modus registrieren. Eine CA kann im `DEFAULT` Modus eins zu eins AWS-Konto registriert werden AWS-Region. Eine CA kann im `SNI_ONLY` Modus von mehreren AWS-Konten gleichzeitig registriert werden AWS-Region. Weitere Informationen zu CA-Zertifikaten finden Sie unter certificateMode.

> **Note**
>
> Es wird empfohlen, dass Sie eine CA im `SNI_ONLY`-Modus registrieren. Sie müssen weder ein Bestätigungszertifikat noch Zugriff auf den privaten Schlüssel vorlegen, und Sie können die Zertifizierungsstelle von mehreren AWS-Konten gleichzeitig registrieren AWS-Region.

### Registrieren Sie ein CA-Zertifikat im SNI_ONLY-Modus (CLI) – Empfohlen

#### Voraussetzungen

Stellen Sie sicher, dass Sie auf Ihrem Computer über Folgendes verfügen, bevor Sie fortfahren:

- Die Zertifikatsdatei der Root-CA (im folgenden Beispiel referenziert als *root_CA_cert_filename.pem*)
- OpenSSL v1.1.1i oder höher

Um ein CA-Zertifikat im **SNI_ONLY** Modus zu registrieren, verwenden Sie den AWS CLI

1. Registrieren Sie das CA-Zertifikat mit AWS IoT. Geben Sie mit dem Befehl register-ca-certificate den Namen der CA-Zertifikatsdatei ein. Weitere Informationen finden Sie unter register-ca-certificate in der Referenz zum AWS CLI -Befehl.

   ```
   aws iot register-ca-certificate \
       --ca-certificate file://root_CA_cert_filename.pem \
       --certificate-mode SNI_ONLY
   ```

   Bei Erfolg gibt dieser Befehl den zurück*certificateId*.

2. Zu diesem Zeitpunkt wurde das CA-Zertifikat registriert, ist AWS IoT aber inaktiv. Das CA-Zertifikat muss aktiv sein, damit Sie Clientzertifikate registrieren können, die von diesem Zertifikat signiert sind.

   In diesem Schritt wird das CA-Zertifikat aktiviert.

   Verwenden Sie Befehl update-certificate wie folgt, um das CA-Zertifikat zu aktivieren. Weitere Informationen finden Sie unter update-certificate in der AWS CLI -Befehlsreferenz.

   ```
   aws iot update-ca-certificate \
       --certificate-id certificateId \
       --new-status ACTIVE
   ```

Verwenden Sie den Befehl describe-ca-certificate, um den Status des CA-Zertifikats anzuzeigen. Weitere Informationen finden Sie unter describe-ca-certificate in der Referenz zum AWS CLI -Befehl.

### Registrieren eines CA-Zertifikats im **DEFAULT**-Modus (CLI)

#### Voraussetzungen

Stellen Sie sicher, dass Sie auf Ihrem Computer über Folgendes verfügen, bevor Sie fortfahren:

- Die Zertifikatsdatei der Root-CA (im folgenden Beispiel referenziert als *root_CA_cert_filename.pem*)
- Die private Schlüsseldatei des Root-CA-Zertifikats (im folgenden Beispiel referenziert als *root_CA_key_filename.key*)
- OpenSSL v1.1.1i oder höher

Um ein CA-Zertifikat im **DEFAULT** Modus zu registrieren, verwenden Sie den AWS CLI

1. Um einen Registrierungscode von zu erhalten AWS IoT, verwenden Sieget-registration-code. Speichern Sie den zurückgegebenen `registrationCode`, um ihn als `Common Name` des Verifizierungszertifikats für private Schlüssel zu verwenden. Weitere Informationen finden Sie unter get-registration-code in der Referenz zum AWS CLI -Befehl.

   ```
   aws iot get-registration-code
   ```

2. Generieren Sie ein Schlüsselpaar für das Verifizierungszertifikat für private Schlüssel:

   ```
   openssl genrsa -out verification_cert_key_filename.key 2048
   ```

3. Erstellen Sie eine Zertifikatssignierungsanforderung (Certificate Signing Request, CSR) für das Verifizierungszertifikat für private Schlüssel. Geben Sie im Feld `Common Name` des Zertifikats den von get-registration-code zurückgegebenen Wert für `registrationCode` ein.

   ```
   openssl req -new \
       -key verification_cert_key_filename.key \
       -out verification_cert_csr_filename.csr
   ```

   Sie werden aufgefordert, einige Informationen zum Zertifikat einzugeben, z. B. den `Common Name`.

   ```
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   ```

```
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
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) []:your_registration_code
    Email Address []:

    Please enter the following 'extra' attributes
    to be sent with your certificate request
    A challenge password []:
    An optional company name []:
```

4. Verwenden Sie die CSR, um ein Verifizierungszertifikat für private Schlüssel zu erstellen:

```
openssl x509 -req \
    -in verification_cert_csr_filename.csr \
    -CA root_CA_cert_filename.pem \
    -CAkey root_CA_key_filename.key \
    -CAcreateserial \
    -out verification_cert_filename.pem \
    -days 500 -sha256
```

5. Registrieren Sie das CA-Zertifikat mit AWS IoT. Geben Sie den Dateinamen des CA-Zertifikats und den Dateinamen des Verifizierungszertifikat für private Schlüssel wie folgt an den Befehl register-ca-certificate weiter. Weitere Informationen finden Sie unter register-ca-certificate in der Referenz zum AWS CLI -Befehl.

```
aws iot register-ca-certificate \
    --ca-certificate file://root_CA_cert_filename.pem \
    --verification-cert file://verification_cert_filename.pem
```

   Dieser Befehl gibt bei Erfolg den *certificateId* zurück.

6. Zu diesem Zeitpunkt wurde das CA-Zertifikat registriert, ist AWS IoT aber nicht aktiv. Das CA-Zertifikat muss aktiv sein, damit Sie Clientzertifikate registrieren können, die von diesem Zertifikat signiert sind.

In diesem Schritt wird das CA-Zertifikat aktiviert.

Verwenden Sie Befehl update-certificate wie folgt, um das CA-Zertifikat zu aktivieren. Weitere Informationen finden Sie unter update-certificate in der AWS CLI -Befehlsreferenz.

```
aws iot update-ca-certificate \
    --certificate-id certificateId \
    --new-status ACTIVE
```

Verwenden Sie den Befehl describe-ca-certificate, um den Status des CA-Zertifikats anzuzeigen. Weitere Informationen finden Sie unter describe-ca-certificate in der Referenz zum AWS CLI -Befehl.

Erstellen Sie ein CA-Verifizierungszertifikat, um das CA-Zertifikat in der Konsole zu registrieren.

> **Note**
>
> Dieses Verfahren wird nur verwendet, wenn Sie ein CA-Zertifikat von der AWS IoT Konsole aus registrieren.
> Wenn Sie dieses Verfahren nicht von der AWS IoT Konsole aus aufgerufen haben, starten Sie den Registrierungsprozess für das CA-Zertifikat in der Konsole unter CA-Zertifikat registrieren.

Stellen Sie sicher, dass Sie auf demselben Computer über Folgendes verfügen, bevor Sie fortfahren:

- Die Zertifikatsdatei der Root-CA (im folgenden Beispiel referenziert als *root_CA_cert_filename.pem*)
- Die private Schlüsseldatei des Root-CA-Zertifikats (im folgenden Beispiel referenziert als *root_CA_key_filename.key*)
- OpenSSL v1.1.1i oder höher

Erstellen Sie ein CA-Verifizierungszertifikat, um Ihr CA-Zertifikat in der Konsole zu registrieren und die Befehlszeilenschnittstelle zu verwenden.

1. Ersetzen Sie *verification_cert_key_filename.key* durch den Namen der Schlüsseldatei für das Verifizierungszertifikat, die Sie erstellen möchten (z. B.

**verification_cert.key**). Führen Sie anschließend diesen Befehl aus, um ein Schlüsselpaar für das Verifizierungszertifikat für private Schlüssel zu generieren:

```
openssl genrsa -out verification_cert_key_filename.key 2048
```

2. Ersetzen Sie *verification_cert_key_filename.key* durch den Namen der Schlüsseldatei, die Sie in Schritt 1 erstellt haben.

   Ersetzen Sie *verification_cert_csr_filename.csr* durch den Namen der Zertifikatsignierungsanforderungsdatei (Certificate Signing Request, CSR), die Sie erstellen möchten. Beispiel, **verification_cert.csr**.

   Führen Sie den Befehl aus, um die CSR-Datei zu erstellen.

   ```
   openssl req -new \
       -key verification_cert_key_filename.key \
       -out verification_cert_csr_filename.csr
   ```

   Der Befehl fordert Sie zur Eingabe zusätzlicher Informationen auf, die an späterer Stelle erläutert werden.

3. Kopieren Sie in der AWS IoT Konsole im Container für das Bestätigungszertifikat den Registrierungscode.

4. Im folgenden Beispiel wird gezeigt, welche Informationen der Befehl openssl fordert. Mit Ausnahme des Felds `Common Name` können Sie Ihre eigenen Werte eingeben oder sie leer lassen.

   Fügen Sie in das Feld `Common Name` den Registrierungscode ein, den Sie im vorherigen Schritt kopiert haben.

   ```
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   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) []:your_registration_code
    Email Address []:

    Please enter the following 'extra' attributes
    to be sent with your certificate request
    A challenge password []:
    An optional company name []:
```

Danach erstellt der Befehl die CSR-Datei.

5. Ersetzen Sie die *verification_cert_csr_filename.csr* durch die *verification_cert_csr_filename.csr*, die Sie im vorherigen Schritt verwendet haben.

   Ersetzen Sie *root_CA_cert_filename.pem* durch den Namen der CA-Zertifikatsdatei, die Sie registrieren möchten.

   Ersetzen Sie *root_CA_key_filename.key* durch den Namen der privaten Schlüsseldatei des CA-Zertifikats.

   Ersetzen Sie *verification_cert_filename.pem* durch den Namen der Verifizierungszertifikatdatei, die Sie erstellen möchten. Beispiel, **verification_cert.pem**.

   ```
   openssl x509 -req \
       -in verification_cert_csr_filename.csr \
       -CA root_CA_cert_filename.pem \
       -CAkey root_CA_key_filename.key \
       -CAcreateserial \
       -out verification_cert_filename.pem \
       -days 500 -sha256
   ```

6. Nachdem der OpenSSL-Befehl abgeschlossen ist, sollten Sie diese Dateien bereit haben, wenn Sie zur Konsole zurückkehren.

   - Ihre CA-Zertifikatsdatei (wurde im vorherigen Befehl *root_CA_cert_filename.pem* verwendet)
   - Das Bestätigungszertifikat, das Sie im vorherigen Schritt erstellt haben (das im vorherigen Befehl *verification_cert_filename.pem* verwendet wurde)

### Deaktivieren eines CA-Zertifikats

Wenn ein Zertifizierungsstellenzertifikat (CA) für die automatische Registrierung von Client-Zertifikaten aktiviert ist, wird das CA-Zertifikat AWS IoT überprüft, um sicherzustellen, dass es sich um die Zertifizierungsstelle handelt`ACTIVE`. Wenn das CA-Zertifikat aktiviert ist`INACTIVE`, kann das Client-Zertifikat AWS IoT nicht registriert werden.

Wenn Sie den Status des CA-Zertifikats auf `INACTIVE` setzen, verhindern Sie, dass neue Clientzertifikate, die von der CA ausgestellt werden, automatisch registriert werden.

> **Note**
>
> Alle registrierten Clientzertifikate, die vom kompromittierten CA-Zertifikat signiert wurden, sind so lange weiterhin aktiv, bis Sie sie jeweils explizit widerrufen.

#### Deaktivieren eines CA-Zertifikats (Konsole)

So deaktivieren Sie ein CA-Zertifikat mithilfe der AWS IoT -Konsole

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Sicher, wählen Sie CAs.
3. Suchen Sie in der Liste der Zertifizierungsstellen diejenige, die Sie deaktivieren möchten, und öffnen Sie das Optionsmenü über das Ellipsensymbol.
4. Wählen Sie im Optionsmenü die Option Deaktivieren.

Die Zertifizierungsstelle sollte in der Liste als Inaktiv angezeigt werden.

> **Note**
>
> Die AWS IoT Konsole bietet keine Möglichkeit, die Zertifikate aufzulisten, die von der Zertifizierungsstelle signiert wurden, die Sie deaktiviert haben. Eine Option zum Auflisten dieser Zertifikate mithilfe der AWS CLI finden Sie unter Deaktivieren eines CA-Zertifikats (CLI).

#### Deaktivieren eines CA-Zertifikats (CLI)

Das AWS CLI stellt den update-ca-certificateBefehl zum Deaktivieren eines CA-Zertifikats bereit.

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

Verwenden Sie den Befehl list-certificates-by-ca, um eine Liste aller registrierten Clientzertifikate zu erhalten, die von der angegebenen CA signiert wurden. Verwenden Sie für jedes Clientzertifikat, das mit dem angegebenen CA-Zertifikat signiert ist, den Befehl update-certificate, um das Clientzertifikat zu widerrufen und dadurch zu verhindern, dass es verwendet wird.

Verwenden Sie den Befehl describe-ca-certificate, um den Status des CA-Zertifikats anzuzeigen.

Erstellen eines Clientzertifikats mit Ihrem CA-Zertifikat

Sie können Ihre eigene Zertifizierungsstelle (Certificate Authority, CA) zum Erstellen von Clientzertifikaten verwenden. Das Client-Zertifikat muss AWS IoT vor der Verwendung registriert werden. Weitere Informationen zu den Registrierungsoptionen für Ihre Clientzertifikate finden Sie unter Registrieren eines Clientzertifikats.

Erstellen eines Clientzertifikats (CLI)

> **Note**
>
> Sie können dieses Verfahren nicht in der AWS IoT Konsole ausführen.

Um ein Client-Zertifikat mit dem zu erstellen AWS CLI

1. Erzeugen Sie ein Schlüsselpaar.

   ```
   openssl genrsa -out device_cert_key_filename.key 2048
   ```

2. Erstellen Sie eine CSR für das Clientzertifikat.

   ```
   openssl req -new \
       -key device_cert_key_filename.key \
       -out device_cert_csr_filename.csr
   ```

   Sie werden zur Eingabe einiger Informationen aufgefordert, wie hier gezeigt:

   ```
   You are about to be asked to enter information that will be incorporated
   ```

```
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
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 []:

    Please enter the following 'extra' attributes
    to be sent with your certificate request
    A challenge password []:
    An optional company name []:
```

3. Erstellen Sie ein Clientzertifikat aus der CSR.

```
openssl x509 -req \
    -in device_cert_csr_filename.csr \
    -CA root_CA_cert_filename.pem \
    -CAkey root_CA_key_filename.key \
    -CAcreateserial \
    -out device_cert_filename.pem \
    -days 500 -sha256
```

Zu diesem Zeitpunkt wurde das Client-Zertifikat erstellt, aber es wurde noch nicht registriert AWS IoT. Weitere Informationen dazu, wie und wann das Clientzertifikat registriert werden soll, finden Sie unter Registrieren eines Clientzertifikats.

Registrieren eines Clientzertifikats

Client-Zertifikate müssen registriert sein AWS IoT , um die Kommunikation zwischen dem Client und zu ermöglichen AWS IoT. Sie können jedes Client-Zertifikat manuell registrieren, oder Sie können die Client-Zertifikate so konfigurieren, dass sie automatisch registriert werden, wenn der Client AWS IoT zum ersten Mal eine Verbindung herstellt.

Wenn Sie möchten, dass Ihre Clients und Geräte ihre Clientzertifikate registrieren, wenn sie sich zum ersten Mal verbinden, müssen Sie Registrieren eines CA-Zertifikats das Clientzertifikat in den

Regionen bei AWS IoT signieren, in denen Sie es verwenden möchten. Die Amazon Root-CA wird automatisch bei registriert AWS IoT.

Kundenzertifikate können nach AWS-Konten Regionen gemeinsam genutzt werden. Die Verfahren in diesen Themen müssen in jedem Konto und jeder Region ausgeführt werden, in der Sie das Clientzertifikat verwenden möchten. Die Registrierung eines Clientzertifikats in einem Konto oder einer Region wird von einem anderen Konto/einer anderen Region nicht automatisch erkannt.

> **Note**
>
> Clients, die das TLS-Protokoll (Transport Layer Security) verwenden, um eine Verbindung mit AWS IoT herzustellen, müssen die SNI-Erweiterung (Server Name Indication) für TLS unterstützen. Weitere Informationen finden Sie unter Transportsicherheit in AWS IoT Core.

Themen

- Manuelles Registrieren eines Clientzertifikats
- Registrieren Sie ein Client-Zertifikat, wenn der Client eine Verbindung zur AWS IoT just-in-time Registrierung herstellt (JITR)

## Manuelles Registrieren eines Clientzertifikats

Sie können ein Client-Zertifikat manuell registrieren, indem Sie die AWS IoT Konsole und verwenden AWS CLI.

Das anzuwendende Registrierungsverfahren hängt davon ab, ob das Zertifikat von AWS-Konto s und Regionen gemeinsam genutzt wird. Die Registrierung eines Clientzertifikats in einem Konto oder einer Region wird von einem anderen Konto/einer anderen Region nicht automatisch erkannt.

Die Verfahren in diesem Thema müssen in jedem Konto und jeder Region ausgeführt werden, in der Sie das Clientzertifikat verwenden möchten. Client-Zertifikate können von AWS-Konto s und Regionen gemeinsam genutzt werden.

Registrieren eines von einer registrierten CA signierten Clientzertifikats (Konsole)

> **Note**
>
> Bevor Sie dieses Verfahren ausführen, stellen Sie sicher, dass Sie über die PEM-Datei des Client-Zertifikats verfügen und dass das Client-Zertifikat von einer Zertifizierungsstelle signiert wurde, bei der Sie sich registriert haben. AWS IoT

Um ein vorhandenes Zertifikat AWS IoT mithilfe der Konsole zu registrieren

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im Navigationsbereich im Abschnitt Verwalten die Option Sicherheit und anschließend Zertifikate.
3. Wählen Sie auf der Seite Zertifikate im Dialogfeld Zertifikate die Option Zertifikat hinzufügen und dann Zertifikate registrieren.
4. Gehen Sie auf der Seite Zertifikat registrieren im Dialogfeld Hochzuladende Zertifikate wie folgt vor:

   - Wählen Sie Zertifizierungsstelle ist bei AWS IoT registriert.
   - Wählen Sie unter CA-Zertifikat auswählen Ihre Zertifizierungsstelle aus.
     - Wählen Sie Neue Zertifizierungsstelle registrieren aus, um eine neue Zertifizierungsstelle zu registrieren, die nicht bei AWS IoT registriert ist.
     - Lassen Sie CA-Zertifikat auswählen leer, wenn die Amazon-Root-Zertifizierungsstelle Ihre Zertifizierungsstelle ist.
   - Wählen Sie bis zu 10 Zertifikate aus, die Sie hochladen und mit denen Sie sich registrieren möchten AWS IoT.
     - Verwenden Sie die Zertifikatsdateien, die Sie in Erstellen Sie AWS IoT Client-Zertifikate und Erstellen eines Clientzertifikats mit Ihrem CA-Zertifikat erstellt haben.
   - Wählen Sie Aktivieren oder Deaktivieren. Wenn Sie Deaktivieren wählen, erklärt Aktivieren oder Deaktivieren eines Clientzertifikats, wie Sie Ihr Zertifikat nach der Zertifikatsregistrierung aktivieren.
   - Wählen Sie Register aus.

Auf der Seite Zertifikate im Dialogfeld Zertifikate werden nun Ihre registrierten Zertifikate angezeigt.

Registrieren eines von einer nicht registrierten CA signierten Clientzertifikats (Konsole)

> **Note**
>
> Stellen Sie sicher, dass Sie über die PEM-Datei des Clientzertifikats verfügen, bevor Sie dieses Verfahren ausführen.

Um ein vorhandenes Zertifikat AWS IoT mithilfe der Konsole zu registrieren

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im linken Navigationsbereich Sichern, Zertifikate und anschließend Erstellen aus.
3. Suchen Sie unter Zertifikat erstellen den Eintrag Eigenes Zertifikat verwenden und wählen Sie Erste Schritte.
4. Wählen Sie unter CA auswählen die Option Weiter.
5. Wählen Sie unter Vorhandene Gerätezertifikate registrieren die Option Zertifikate auswählen und wählen Sie bis zu zehn Zertifikatdateien zum Registrieren aus.
6. Schließen Sie das Dateidialogfeld und wählen Sie aus, ob Sie die Clientzertifikate bei der Registrierung aktivieren oder widerrufen möchten.

   Wenn Sie ein Zertifikat bei der Registrierung nicht aktivieren, können Sie unter Aktivieren eines Clientzertifikats (Konsole) nachlesen, wie Sie es zu einem späteren Zeitpunkt aktivieren können.

   Wenn ein Zertifikat bei der Registrierung widerrufen wird, kann es später nicht aktiviert werden.

   Nachdem Sie die zu registrierenden Zertifikatdateien und die nach der Registrierung auszuführenden Aktionen ausgewählt haben, klicken Sie auf Zertifikate registrieren.

Die erfolgreich registrierten Clientzertifikate werden in der Liste der Zertifikate angezeigt.

Registrieren eines von einer registrierten CA signierten Clientzertifikats (CLI)

> **Note**
>
> Stellen Sie sicher, dass Sie über die PEM-Datei der CA und über die PEM-Datei des Clientzertifikats verfügen, bevor Sie dieses Verfahren ausführen. Das Client-Zertifikat muss von einer Zertifizierungsstelle (CA) signiert sein, bei der Sie sich registriert haben AWS IoT.

Verwenden Sie den Befehl register-certificate, um ein Clientzertifikat zu registrieren, ohne es zu aktivieren.

```
aws iot register-certificate \
    --certificate-pem file://device_cert_filename.pem \
    --ca-certificate-pem file://ca_cert_filename.pem
```

Das Client-Zertifikat ist bei registriert AWS IoT, aber es ist noch nicht aktiv. Informationen dazu, wie Sie es zu einem späteren Zeitpunkt aktivieren können, finden Sie unter Aktivieren eines Clientzertifikats (CLI).

Sie können das Clientzertifikat auch aktivieren, wenn Sie es mit dem folgenden Befehl registrieren.

```
aws iot register-certificate \
    --set-as-active \
    --certificate-pem file://device_cert_filename.pem \
    --ca-certificate-pem file://ca_cert_filename.pem
```

Weitere Informationen zur Aktivierung des Zertifikats, sodass es für die Herstellung einer Verbindung verwendet werden kann AWS IoT, finden Sie unter Aktivieren oder Deaktivieren eines Clientzertifikats

Registrieren eines von einer nicht registrierten CA signierten Clientzertifikats (CLI)

> **Note**
>
> Stellen Sie sicher, dass Sie über die PEM-Datei des Zertifikats verfügen, bevor Sie dieses Verfahren ausführen.

Verwenden Sie den Befehl register-certificate-without-ca, um ein Clientzertifikat zu registrieren, ohne es zu aktivieren.

```
aws iot register-certificate-without-ca \
    --certificate-pem file://device_cert_filename.pem
```

Das Client-Zertifikat ist registriert AWS IoT, aber es ist noch nicht aktiv. Informationen dazu, wie Sie es zu einem späteren Zeitpunkt aktivieren können, finden Sie unter Aktivieren eines Clientzertifikats (CLI).

Sie können das Clientzertifikat auch aktivieren, wenn Sie es mit dem folgenden Befehl registrieren.

```
aws iot register-certificate-without-ca \
    --status ACTIVE \
    --certificate-pem file://device_cert_filename.pem
```

Weitere Hinweise zur Aktivierung des Zertifikats, sodass es für die Herstellung einer Verbindung verwendet werden kann AWS IoT, finden Sie unterAktivieren oder Deaktivieren eines Clientzertifikats.

Registrieren Sie ein Client-Zertifikat, wenn der Client eine Verbindung zur AWS IoT just-in-time Registrierung herstellt (JITR)

Sie können ein CA-Zertifikat so konfigurieren, dass Client-Zertifikate, mit denen es signiert wurde, AWS IoT automatisch registriert werden, wenn der Client zum AWS IoT ersten Mal eine Verbindung herstellt.

Um Client-Zertifikate zu registrieren, wenn ein Client AWS IoT zum ersten Mal eine Verbindung herstellt, müssen Sie das CA-Zertifikat für die automatische Registrierung aktivieren und die erste Verbindung des Clients so konfigurieren, dass die erforderlichen Zertifikate bereitgestellt werden.

Konfigurieren eines CA-Zertifikats zur Unterstützung der automatischen Registrierung (Konsole)

Um ein CA-Zertifikat zur Unterstützung der automatischen Registrierung von Client-Zertifikaten mithilfe der AWS IoT Konsole zu konfigurieren

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im linken Navigationsbereich Secure, wählen Sie CAs.
3. Suchen Sie in der Liste der Zertifizierungsstellen diejenige, für die Sie die automatische Registrierung aktivieren möchten, und öffnen Sie das Optionsmenü über das Ellipsensymbol.
4. Wählen Sie im Optionsmenü Automatische Registrierung aktivieren.

> **Note**
>
> Der Status der automatischen Registrierung wird in der Liste der Zertifizierungsstellen nicht angezeigt. Um den Status der automatischen Registrierung einer Zertifizierungsstelle anzuzeigen, müssen Sie die Seite Details der Zertifizierungsstelle öffnen.

Konfigurieren eines CA-Zertifikats zur Unterstützung der automatischen Registrierung (CLI)

Wenn Sie Ihr CA-Zertifikat bereits registriert haben AWS IoT, verwenden Sie den update-ca-certificateBefehl, um das CA-Zertifikat auf festzulegen `autoRegistrationStatusENABLE`.

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

Wenn Sie `autoRegistrationStatus` bei der Registrierung des CA-Zertifikats aktivieren möchten, verwenden Sie den Befehl register-ca-certificate.

```
aws iot register-ca-certificate \
--allow-auto-registration  \
--ca-certificate file://root_CA_cert_filename.pem \
--verification-cert file://verification_cert_filename.pem
```

Verwenden Sie den Befehl describe-ca-certificate, um den Status des CA-Zertifikats anzuzeigen.

Konfigurieren der ersten Verbindung durch einen Client für die automatische Registrierung

Wenn ein Client zum ersten Mal versucht, eine Verbindung herzustellen, muss das mit Ihrem CA-Zertifikat signierte Client-Zertifikat während des Transport Layer Security (TLS) -Handshakes auf dem Client vorhanden sein. AWS IoT

Wenn der Client eine Verbindung herstellt AWS IoT, verwenden Sie das Client-Zertifikat, das Sie unter AWS IoT Client-Zertifikate erstellen oder Eigene Client-Zertifikate erstellen erstellt haben. AWS IoT erkennt das CA-Zertifikat als registriertes CA-Zertifikat, registriert das Client-Zertifikat und setzt seinen Status auf`PENDING_ACTIVATION`. Das bedeutet, dass das Clientzertifikat automatisch registriert wurde und auf die Aktivierung wartet. Das Clientzertifikat muss den Status `ACTIVE` aufweisen, damit es zur Verbindung mit AWS IoT verwendet werden kann. Informationen zur Aktivierung eines Clientzertifikats finden Sie unter Aktivieren oder Deaktivieren eines Clientzertifikats.

> **Note**
>
> Sie können Geräte mithilfe der AWS IoT Core just-in-time Registrierungsfunktion (JITR) bereitstellen, ohne die gesamte Vertrauenskette bei der ersten Verbindung der Geräte an senden zu müssen. AWS IoT Core Die Vorlage des CA-Zertifikats ist optional, aber das Gerät muss die Server Name Indication (SNI) senden, wenn es eine Verbindung herstellt.

Wenn ein Zertifikat AWS IoT automatisch registriert wird oder wenn ein Client ein Zertifikat im PENDING_ACTIVATION Status präsentiert, wird eine Nachricht zum folgenden MQTT-Thema AWS IoT veröffentlicht:

`$aws/events/certificates/registered/`*caCertificateId*

Dabei ist *caCertificateId* die ID des CA-Zertifikats, das das Gerätezertifikat ausgestellt hat.

Die im Topic veröffentlichte Nachricht weist die folgende Struktur auf:

```
{
        "certificateId": "certificateId",
        "caCertificateId": "caCertificateId",
        "timestamp": timestamp,
        "certificateStatus": "PENDING_ACTIVATION",
        "awsAccountId": "awsAccountId",
        "certificateRegistrationTimestamp": "certificateRegistrationTimestamp"
}
```

Sie können eine Regel zum Beobachten dieses Topics und Ausführen bestimmter Aktionen erstellen. Wir empfehlen, eine Lambda-Regel zu erstellen, mit der sichergestellt wird, dass sich das Clientzertifikat nicht auf einer Zertifikataufhebungsliste (Certificate Revocation List, CRL) befindet, und mit der das Zertifikat aktiviert und eine Richtlinie erstellt und an das Zertifikat angefügt wird. Die Richtlinie bestimmt, auf welche Ressourcen der Client zugreifen kann. Wenn die Richtlinie, die Sie erstellen, die Client-ID von den Verbindungsgeräten benötigt, können Sie die Client-ID () -Funktion der Regel verwenden, um die Client-ID abzurufen. Ein Beispiel für eine Regeldefinition kann wie folgt aussehen:

```
SELECT *,
   clientid() as clientid
from $aws/events/certificates/registered/caCertificateId
```

In diesem Beispiel abonniert die Regel das JITR-Thema `$aws/events/certificates/registered/`*caCertificateID* und verwendet die Funktion clientid (), um die Client-ID abzurufen. Die Regel hängt dann die Client-ID an die JITR-Nutzlast an. Weitere Hinweise zur clientid () -Funktion der Regel finden Sie unter clientid ().

Weitere Informationen zum Erstellen einer Lambda-Regel, die das `$aws/events/certificates/registered/`*caCertificateID* Thema überwacht und diese Aktionen ausführt, finden Sie unter just-in-time Registrierung von Client-Zertifikaten am. AWS IoT

Wenn bei der automatischen Registrierung der Client-Zertifikate ein Fehler oder eine Ausnahme auftritt, AWS IoT sendet es Ereignisse oder Meldungen an Ihre Logs in CloudWatch Logs. Weitere Informationen zur Einrichtung der Logs für Ihr Konto finden Sie in der CloudWatch Amazon-Dokumentation.

## Client-Zertifikate verwalten

AWS IoT bietet Funktionen zur Verwaltung von Client-Zertifikaten.

In diesem Thema:


- Aktivieren oder Deaktivieren eines Clientzertifikats
- Anfügen eines Objekts oder einer Richtlinie an ein Clientzertifikat
- Widerrufen eines Clientzertifikats
- Übertragen eines Zertifikats in ein anderes Konto


### Aktivieren oder Deaktivieren eines Clientzertifikats

AWS IoT überprüft, ob ein Client-Zertifikat aktiv ist, wenn es eine Verbindung authentifiziert.

Sie können Clientzertifikate erstellen und registrieren, ohne sie zu aktivieren, sodass sie erst verwendet werden können, wenn Sie dies möchten. Sie können auch aktive Clientzertifikate deaktivieren, um sie vorübergehend zu deaktivieren. Und Sie können Clientzertifikate widerrufen, um deren zukünftige Verwendung zu verhindern.

#### Aktivieren eines Clientzertifikats (Konsole)

Um ein Client-Zertifikat mit der Konsole zu aktivieren AWS IoT

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im linken Navigationsbereich Sichern und dann Zertifikate.
3. Suchen Sie in der Liste der Zertifikate dasjenige, die Sie aktivieren möchten, und öffnen Sie das Optionsmenü über das Ellipsensymbol.
4. Wählen Sie im Optionsmenü die Option Aktivieren.

Das Zertifikat sollte in der Liste der Zertifikate als Aktiv angezeigt werden.

Deaktivieren eines Clientzertifikats (Konsole)

Um ein Client-Zertifikat über die AWS IoT Konsole zu deaktivieren

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im linken Navigationsbereich Sichern und dann Zertifikate.
3. Suchen Sie in der Liste der Zertifikate dasjenige, die Sie deaktivieren möchten, und öffnen Sie das Optionsmenü über das Ellipsensymbol.
4. Wählen Sie im Optionsmenü die Option Deaktivieren.

Das Zertifikat sollte in der Liste der Zertifikate als Inaktiv angezeigt werden.

Aktivieren eines Clientzertifikats (CLI)

Das AWS CLI stellt den update-certificateBefehl zur Aktivierung eines Zertifikats bereit.

```
aws iot update-certificate \
    --certificate-id certificateId \
    --new-status ACTIVE
```

Wenn der Befehl erfolgreich ist, wird der Status des Zertifikats auf `ACTIVE` gesetzt. Führen Sie describe-certificate aus, um den Status des Zertifikats anzuzeigen.

```
aws iot describe-certificate \
    --certificate-id certificateId
```

Deaktivieren eines Clientzertifikats (CLI)

Der AWS CLI stellt den update-certificateBefehl zum Deaktivieren eines Zertifikats bereit.

```
aws iot update-certificate \
    --certificate-id certificateId \
    --new-status INACTIVE
```

Wenn der Befehl erfolgreich ist, wird der Status des Zertifikats auf `INACTIVE` gesetzt. Führen Sie describe-certificate aus, um den Status des Zertifikats anzuzeigen.

```
aws iot describe-certificate \
    --certificate-id certificateId
```

### Anfügen eines Objekts oder einer Richtlinie an ein Clientzertifikat

Wenn Sie ein Zertifikat unabhängig von einer AWS IoT Sache erstellen und registrieren, wird es weder über Richtlinien verfügen, die AWS IoT Operationen autorisieren, noch wird es mit einem Objekt verknüpft. AWS IoT In diesem Abschnitt wird beschrieben, wie Sie diese Beziehungen zu einem registrierten Zertifikat hinzufügen.

> **Important**
>
> Um dieses Verfahren ausführen zu können, müssen Sie das Objekt oder die Richtlinie, das/die Sie an das Zertifikat anfügen möchten, bereits erstellt haben.

Das Zertifikat authentifiziert ein Gerät mit, AWS IoT sodass es eine Verbindung herstellen kann. Durch das Anhängen des Zertifikats an eine Objektressource wird die Beziehung zwischen dem Gerät (über das Zertifikat) und der Objektressource hergestellt. Um das Gerät zur Ausführung von AWS IoT Aktionen zu autorisieren, z. B. damit das Gerät eine Verbindung herstellen und Nachrichten veröffentlichen kann, muss dem Zertifikat des Geräts eine entsprechende Richtlinie beigefügt werden.

#### Anfügen eines Objekts an ein Clientzertifikat (Konsole)

Sie benötigen für dieses Verfahren den Namen des Objekts.

So fügen Sie ein Objekt an ein registriertes Zertifikat an

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im linken Navigationsbereich Sicher und dann Zertifikate.
3. Suchen Sie in der Zertifikatsliste das Zertifikat, an das Sie eine Richtlinie anfügen möchten, öffnen Sie das Optionsmenü des Zertifikats über das Ellipsensymbol und wählen Sie Objekt anfügen.
4. Suchen Sie im Pop-up-Fenster den Namen des Objekts, das Sie an das Zertifikat anfügen möchten, markieren Sie das entsprechende Kontrollkästchen und wählen Sie Anfügen.

Das Objekt sollte nun in der Objektliste auf der Detailseite des Zertifikats angezeigt werden.

#### Anfügen einer Richtlinie an ein Clientzertifikat (Konsole)

Sie benötigen für dieses Verfahren den Namen des Richtlinienobjekts.

So fügen Sie ein Richtlinienobjekt an ein registriertes Zertifikat an

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im linken Navigationsbereich Sichern und dann Zertifikate.
3. Suchen Sie in der Zertifikatsliste das Zertifikat, an das Sie eine Richtlinie anfügen möchten, öffnen Sie das Optionsmenü des Zertifikats über das Ellipsensymbol und wählen Sie Richtlinie anfügen.
4. Suchen Sie im Pop-up-Fenster den Namen der Richtlinie, die Sie an das Zertifikat anfügen möchten, markieren Sie das entsprechende Kontrollkästchen und wählen Sie Anfügen.

Das Richtlinienobjekt sollte nun in der Richtlinienliste auf der Detailseite des Zertifikats angezeigt werden.

Anfügen eines Objekts an ein Clientzertifikat (CLI)

Das AWS CLI stellt den attach-thing-principalBefehl zum Anhängen eines Dingobjekts an ein Zertifikat bereit.

```
aws iot attach-thing-principal \
    --principal certificateArn \
    --thing-name thingName
```

Anfügen einer Richtlinie an ein Clientzertifikat (CLI)

Der AWS CLI stellt den attach-policyBefehl zum Anhängen eines Richtlinienobjekts an ein Zertifikat bereit.

```
aws iot attach-policy \
    --target certificateArn \
    --policy-name policyName
```

Widerrufen eines Clientzertifikats

Wenn Sie verdächtige Aktivitäten in einem registrierten Clientzertifikat erkennen, können Sie es widerrufen, damit es nicht noch einmal verwendet werden kann.

> **Note**
>
> Sobald ein Zertifikat gesperrt wurde, kann sein Status nicht mehr geändert werden. Das heißt, dass der Status des Zertifikats nicht in `Active` oder einen anderen Status geändert werden kann.

Widerrufen eines Clientzertifikats (Konsole)

Um ein Client-Zertifikat mithilfe der AWS IoT Konsole zu widerrufen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im linken Navigationsbereich Sichern und dann Zertifikate.
3. Suchen Sie in der Liste der Zertifikate dasjenige, die Sie widerrufen möchten, und öffnen Sie das Optionsmenü über das Ellipsensymbol.
4. Wählen Sie im Optionsmenü die Option Widerrufen.

Wenn das Zertifikat erfolgreich widerrufen wurde, wird es in der Liste der Zertifikate als Widerrufen angezeigt.

Widerrufen eines Clientzertifikats (CLI)

Das AWS CLI stellt den update-certificateBefehl zum Widerrufen eines Zertifikats bereit.

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

Wenn der Befehl erfolgreich ist, wird der Status des Zertifikats auf `REVOKED` gesetzt. Führen Sie describe-certificate aus, um den Status des Zertifikats anzuzeigen.

```
aws iot describe-certificate \
    --certificate-id certificateId
```

Übertragen eines Zertifikats in ein anderes Konto

X.509-Zertifikate, die zu einem Zertifikat gehören, AWS-Konto können auf ein anderes AWS-Kontoübertragen werden.

Um ein X.509-Zertifikat von einem auf ein anderes zu AWS-Konto übertragen

1. the section called “Starten einer Zertifikatsübertragung”

   Das Zertifikat muss deaktiviert und von allen Richtlinien und Objekten getrennt werden, bevor die Übertragung gestartet wird.
2. the section called “Annehmen oder Ablehnen einer Zertifikatsübertragung”

   Das empfangende Konto muss das übertragene Zertifikat ausdrücklich akzeptieren oder ablehnen. Nachdem das Empfängerkonto das Zertifikat akzeptiert hat, muss das Zertifikat aktiviert werden, bevor es verwendet werden kann.
3. the section called “Abbrechen einer Zertifikatsübertragung”

   Das ursprüngliche Konto kann eine Übertragung abbrechen, wenn das Zertifikat nicht akzeptiert wurde.

Starten einer Zertifikatsübertragung

Sie können mit der Übertragung eines Zertifikats auf ein anderes beginnen, AWS-Konto indem Sie die AWS IoT Konsole oder das AWS CLI verwenden.

Starten einer Zertifikatsübertragung (Konsole)

Sie benötigen die ID des Zertifikats, das Sie übertragen möchten. um dieses Verfahren abzuschließen.

Führen Sie dieses Verfahren von dem Konto aus, das das zu übertragende Zertifikat enthält.

So beginnen Sie die Übertragung eines Zertifikats in ein anderes AWS-Konto

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im linken Navigationsbereich Sichern und dann Zertifikate.

   Wählen Sie das Zertifikat mit dem Status Aktiv oder Inaktiv aus, das Sie übertragen möchten, und öffnen Sie die zugehörige Detailseite.
3. Wenn auf der Seite Details des Zertifikats im Menü Aktionen die Option Deaktivieren verfügbar ist, wählen Sie die Option Deaktivieren, um das Zertifikat zu deaktivieren.
4. Wählen Sie auf der Seite Details des Zertifikats im linken Menü die Option Richtlinien.

5. Wenn auf der Seite Richtlinien des Zertifikats Richtlinien mit dem Zertifikat verknüpft sind, trennen Sie die einzelnen Richtlinien, indem Sie das Optionsmenü der Richtlinie öffnen und Trennen wählen.

   Bevor Sie fortfahren, dürfen mit dem Zertifikat keine Richtlinien verbunden sein.
6. Wählen Sie auf der Seite Richtlinien des Zertifikats im linken Menü die Option Objekte.
7. Wenn auf der Seite Objekte des Zertifikats Objekte mit dem Zertifikat verknüpft sind, trennen Sie die einzelnen Objekte, indem Sie das Optionsmenü des Objekts öffnen und Trennen wählen.

   Bevor Sie fortfahren, dürfen mit dem Zertifikat keine Objekte verbunden sein.
8. Wählen Sie auf der Seite Details des Zertifikats im linken Menü die Option Details.
9. Wählen Sie auf der Seite Details des Zertifikats im Menü Aktionen die Option Übertragung starten, um das Dialogfeld Übertragung starten zu öffnen.
10. Geben Sie im Dialogfeld Übertragung starten die AWS-Konto Nummer des Kontos ein, das das Zertifikat erhalten soll, und optional eine Kurznachricht.
11. Wählen Sie Übertragung starten, um das Zertifikat zu übertragen.

Die Konsole sollte eine Meldung anzeigen, die den Erfolg oder Misserfolg der Übertragung angibt. Wenn die Übertragung gestartet wurde, wird der Status des Zertifikats auf Übertragen aktualisiert.

Starten einer Zertifikatsübertragung (CLI)

Um dieses Verfahren abzuschließen, benötigen Sie das *certificateId* und das *certificateArn* Zertifikat, das Sie übertragen möchten.

Führen Sie dieses Verfahren von dem Konto aus, das das zu übertragende Zertifikat enthält.

So beginnen Sie die Übertragung eines Zertifikats in ein anderes AWS -Konto

1. Verwenden Sie den Befehl update-certificate zum Deaktivieren des Zertifikats.

   ```
   aws iot update-certificate --certificate-id certificateId --new-status INACTIVE
   ```
2. Trennen Sie alle Richtlinien.

   1. Verwenden Sie den Befehl list-attached-policies, um die an das Zertifikat angehängten Richtlinien aufzulisten.

```
aws iot list-attached-policies --target certificateArn
```

2. Verwenden Sie für jede angehängte Richtlinie den Befehl detach-policy, um die Richtlinie zu trennen.

```
aws iot detach-policy --target certificateArn --policy-name policy-name
```

3. Trennen Sie alle Objekte.

1. Verwenden Sie den Befehl list-principal-things, um die an das Zertifikat angehängten Objekte aufzulisten.

```
aws iot list-principal-things --principal certificateArn
```

2. Verwenden Sie für jedes angehängte Objekt den Befehl detach-thing-principal, um das Objekt zu trennen.

```
aws iot detach-thing-principal --principal certificateArn --thing-name thing-name
```

4. Verwenden Sie den Befehl transfer-certificate, um die Zertifikatsübertragung zu starten.

```
aws iot transfer-certificate --certificate-id certificateId --target-aws-
account account-id
```

Annehmen oder Ablehnen einer Zertifikatsübertragung

Sie können ein Zertifikat, das Ihnen AWS-Konto von einem anderen übertragen wurde, akzeptieren oder ablehnen, AWS-Konto indem Sie die AWS IoT Konsole oder das verwenden AWS CLI.

Annehmen oder Ablehnen einer Zertifikatsübertragung (Konsole)

Sie benötigen die ID des Zertifikats, das in Ihr Konto übertragen wurde, um dieses Verfahren abzuschließen.

Führen Sie dieses Verfahren von dem Konto aus, das das übertragende Zertifikat empfängt.

So können Sie ein Zertifikat akzeptieren oder ablehnen, das in Ihr AWS-Kontoübertragen wurde

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im linken Navigationsbereich Sichern und dann Zertifikate.

Wählen Sie das Zertifikat mit dem Status Ausstehende Übertragung aus, das Sie akzeptieren oder ablehnen möchten, und öffnen Sie die zugehörige Detailseite.

3. Auf der Detailseite des Zertifikats im Menü Aktionen,

   - Wählen Sie Übertragung akzeptieren, um das Zertifikat zu akzeptieren.
   - Wählen Sie Übertragung ablehnen, um das Zertifikat abzulehnen.

Annehmen oder Ablehnen einer Zertifikatsübertragung (CLI)

Um dieses Verfahren abzuschließen, benötigen Sie den Namen *certificateId* der Zertifikatsübertragung, die Sie akzeptieren oder ablehnen möchten.

Führen Sie dieses Verfahren von dem Konto aus, das das übertragende Zertifikat empfängt.

So können Sie ein Zertifikat akzeptieren oder ablehnen, das in Ihr AWS-Kontoübertragen wurde

1. Verwenden Sie den Befehl accept-certificate-transfer, um das Zertifikat zu akzeptieren.

   ```
   aws iot accept-certificate-transfer --certificate-id certificateId
   ```

2. Verwenden Sie den Befehl reject-certificate-transfer, um das Zertifikat abzulehnen.

   ```
   aws iot reject-certificate-transfer --certificate-id certificateId
   ```

Abbrechen einer Zertifikatsübertragung

Sie können eine Zertifikatsübertragung abbrechen, bevor sie akzeptiert wurde, indem Sie die AWS IoT -Konsole oder die AWS CLI verwenden.

Abbrechen einer Zertifikatsübertragung (Konsole)

Sie benötigen die ID der Zertifikatsübertragung, die Sie abbrechen möchten, um dieses Verfahren abzuschließen.

Führen Sie dieses Verfahren von dem Konto aus, das die Zertifikatsübertragung gestartet hat.

So brechen Sie eine Zertifikatsübertragung ab

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS IoT Konsole.

2. Wählen Sie im linken Navigationsbereich Sichern und dann Zertifikate.

   Wählen Sie das Zertifikat mit dem Status Übertragen aus, dessen Übertragung Sie stornieren möchten, und öffnen Sie das zugehörige Optionsmenü.

3. Wählen Sie im Optionsmenü des Zertifikats die Option Übertragung widerrufen, um die Zertifikatsübertragung abzubrechen.

   > **Important**
   >
   > Achten Sie darauf, die Option Übertragung widerrufen nicht mit der Option Widerrufen zu verwechseln.
   > Mit der Option Übertragung widerrufen wird die Zertifikatsübertragung abgebrochen, während die Option Widerrufen das Zertifikat für das AWS IoT unwiderruflich unbrauchbar macht.

Abbrechen einer Zertifikatsübertragung (CLI)

Um dieses Verfahren abzuschließen, benötigen Sie den Namen *certificateId* der Zertifikatsübertragung, die Sie stornieren möchten.

Führen Sie dieses Verfahren von dem Konto aus, das die Zertifikatsübertragung gestartet hat.

Verwenden Sie den Befehl cancel-certificate-transfer, um die Zertifikatsübertragung abzubrechen.

```
aws iot cancel-certificate-transfer --certificate-id certificateId
```

Validierung benutzerdefinierter Client-Zertifikate

AWS IoT Core unterstützt die benutzerdefinierte Validierung von Client-Zertifikaten für X.509-Clientzertifikate, wodurch die Verwaltung der Client-Authentifizierung verbessert wird. Diese Methode zur Zertifikatsvalidierung wird auch als Zertifikatsprüfung vor der Authentifizierung bezeichnet. Dabei bewerten Sie Client-Zertifikate anhand Ihrer eigenen Kriterien (definiert in einer Lambda-Funktion) und widerrufen Client-Zertifikate oder das Zertifikat der Signing Certificate Authority (CA) der Zertifikate, um zu verhindern, dass Clients eine Verbindung herstellen können. AWS IoT Core Sie können beispielsweise Ihre eigenen Zertifikatssperrprüfungen erstellen, die den Status der Zertifikate anhand von Validierungsstellen überprüfen, die Online Certificate Status Protocol (OCSP) oder Certificate Revocation Lists (CRL) Endpunkte unterstützen, und Verbindungen für Clients mit

gesperrten Zertifikaten verhindern. Die Kriterien, die zur Bewertung von Client-Zertifikaten verwendet werden, werden in einer Lambda-Funktion (auch bekannt als Lambda vor der Authentifizierung) definiert. Sie müssen die in den Domänenkonfigurationen festgelegten Endpunkte verwenden und der Authentifizierungstyp muss ein X.509-Zertifikat sein. Darüber hinaus müssen Clients die Erweiterung Server Name Indication (SNI) angeben, wenn sie eine Verbindung herstellen. AWS IoT Core

> **Note**
>
> Diese Funktion wird in den AWS GovCloud (US) Regionen nicht unterstützt.

Die Überprüfung benutzerdefinierter Client-Zertifikate umfasst die folgenden Schritte.

- Schritt 1: Registrieren Sie Ihre X.509-Client-Zertifikate bei AWS IoT Core
- Schritt 2: Erstellen einer Lambda-Funktion
- Schritt 3: Autorisieren Sie AWS IoT den Aufruf Ihrer Lambda-Funktion
- Schritt 4: Legen Sie die Authentifizierungskonfiguration für eine Domain fest

### Schritt 1: Registrieren Sie Ihre X.509-Client-Zertifikate bei AWS IoT Core

Falls Sie dies noch nicht getan haben, registrieren und aktivieren Sie Ihre X.509-Client-Zertifikate mit. AWS IoT Core Andernfalls überspringen Sie diesen Schritt und gehen Sie direkt zum nächsten.

Gehen Sie wie folgt vor AWS IoT Core, um Ihre Client-Zertifikate bei zu registrieren und zu aktivieren:

1. Wenn Sie Kundenzertifikate direkt mit erstellen AWS IoT. Diese Client-Zertifikate werden automatisch bei registriert AWS IoT Core.
2. Wenn Sie Ihre eigenen Client-Zertifikate erstellen, folgen Sie diesen Anweisungen, um sie zu registrieren AWS IoT Core.
3. Folgen Sie diesen Anweisungen, um Ihre Client-Zertifikate zu aktivieren.

### Schritt 2: Erstellen einer Lambda-Funktion

Sie müssen eine Lambda-Funktion erstellen, die die Zertifikatsverifizierung durchführt und bei jedem Verbindungsversuch eines Clients für den konfigurierten Endpunkt aufgerufen wird. Folgen Sie beim Erstellen dieser Lambda-Funktion den allgemeinen Anweisungen unter Erstellen Sie Ihre erste

Lambda-Funktion. Stellen Sie außerdem sicher, dass die Lambda-Funktion die erwarteten Anfrage- und Antwortformate wie folgt einhält:

Beispiel für ein Lambda-Funktionsereignis

```
{
 "connectionMetadata": {
  "id": "string"
 },
 "principalId": "string",
 "serverName": "string",
 "clientCertificateChain": [
  "string",
  "string"
 ]
}
```

`connectionMetadata`

Metadaten oder zusätzliche Informationen zur Verbindung des Clients mit. AWS IoT Core

`principalId`

Die Haupt-ID, die dem Client in der TLS-Verbindung zugeordnet ist.

`serverName`

Die Hostnamenzeichenfolge (Server Name Indication, SNI). AWS IoT Core erfordert, dass Geräte die SNI-Erweiterung an das Transport Layer Security (TLS) -Protokoll senden und die vollständige Endpunktadresse im Feld angeben. `host_name`

`clientCertificateChain`

Das Zeichenkettenarray, das die X.509-Zertifikatskette des Clients darstellt.

Beispiel für eine Antwort auf eine Lambda-Funktion

```
{
 "isAuthenticated": "boolean"
}
```

`isAuthenticated`

Ein boolescher Wert, der angibt, ob die Anfrage authentifiziert ist.

> **Note**
>
> In der Lambda-Antwort `isAuthenticated` muss `true` mit der weiteren Authentifizierung und Autorisierung fortgefahren werden. Andernfalls kann das IoT-Client-Zertifikat deaktiviert und die benutzerdefinierte Authentifizierung mit X.509-Client-Zertifikaten für die weitere Authentifizierung und Autorisierung blockiert werden.

Schritt 3: Autorisieren Sie AWS IoT den Aufruf Ihrer Lambda-Funktion

Nachdem Sie die Lambda-Funktion erstellt haben, müssen Sie mithilfe des AWS IoT CLI-Befehls add-permission die Erlaubnis erteilen, sie aufzurufen. Beachten Sie, dass diese Lambda-Funktion bei jedem Verbindungsversuch zu Ihrem konfigurierten Endpunkt aufgerufen wird. Weitere Informationen finden Sie unter Autorisieren des AWS IoT Aufrufs Ihrer Lambda-Funktion.

Schritt 4: Legen Sie die Authentifizierungskonfiguration für eine Domain fest

Im folgenden Abschnitt wird beschrieben, wie Sie die Authentifizierungskonfiguration für eine benutzerdefinierte Domain mithilfe von festlegen AWS CLI.

Konfiguration des Client-Zertifikats für eine Domain festlegen (CLI)

Wenn Sie keine Domänenkonfiguration haben, verwenden Sie den create-domain-configurationCLI-Befehl, um eine zu erstellen. Wenn Sie bereits über eine Domänenkonfiguration verfügen, verwenden Sie den update-domain-configurationCLI-Befehl, um die Konfiguration des Client-Zertifikats für eine Domain zu aktualisieren. Sie müssen den ARN der Lambda-Funktion hinzufügen, die Sie im vorherigen Schritt erstellt haben.

```
aws iot create-domain-configuration \
    --domain-configuration-name domainConfigurationName \
    --authentication-type AWS_X509|CUSTOM_AUTH_X509 \
    --application-protocol SECURE_MQTT|HTTPS \
    --client-certificate-config 'clientCertificateCallbackArn":"arn:aws:lambda:us-
east-2:123456789012:function:my-function:1"}'
```

```
aws iot update-domain-configuration \
    --domain-configuration-name domainConfigurationName \
    --authentication-type AWS_X509|CUSTOM_AUTH_X509 \
    --application-protocol SECURE_MQTT|HTTPS \
```

```
    --client-certificate-config '{"clientCertificateCallbackArn":"arn:aws:lambda:us-east-2:123456789012:function:my-function:1"}'
```

`domain-configuration-name`

Der Name der Domänenkonfiguration.

`authentication-type`

Der Authentifizierungstyp der Domänenkonfiguration. Weitere Informationen finden Sie unter Auswahl eines Authentifizierungstyps.

`application-protocol`

Das Anwendungsprotokoll, mit dem Geräte kommunizieren AWS IoT Core. Weitere Informationen finden Sie unter Auswahl eines Anwendungsprotokolls.

`client-certificate-config`

Ein Objekt, das die Konfiguration der Client-Authentifizierung für eine Domäne angibt.

`clientCertificateCallbackArn`

Der Amazon-Ressourcenname (ARN) der Lambda-Funktion, die in der AWS IoT TLS-Schicht aufgerufen wird, wenn eine neue Verbindung hergestellt wird. Um die Client-Authentifizierung für die Durchführung einer benutzerdefinierten Client-Zertifikatsvalidierung anzupassen, müssen Sie den ARN der Lambda-Funktion hinzufügen, die Sie im vorherigen Schritt erstellt haben.

Weitere Informationen finden Sie in CreateDomainConfigurationund in UpdateDomainConfigurationder AWS IoT API-Referenz. Weitere Informationen zu Domänenkonfigurationen finden Sie unter Domänenkonfigurationen.

## IAM-Benutzer, -Gruppen und -Rollen

IAM-Benutzer, -Gruppen und -Rollen sind die Standardmechanismen zum Verwalten von Identitäts- und Authentifizierungsmethoden in AWS. Sie können sie verwenden, um mithilfe des AWS SDK und eine Verbindung zu AWS IoT HTTP-Schnittstellen herzustellen AWS CLI.

Mit IAM-Rollen können AWS IoT Sie auch in Ihrem Namen auf andere AWS Ressourcen in Ihrem Konto zugreifen. Wenn Sie beispielsweise möchten, dass ein Gerät seinen Status in einer DynamoDB-Tabelle veröffentlicht, ermöglichen AWS IoT IAM-Rollen die Interaktion mit Amazon DynamoDB. Weitere Informationen finden Sie unter IAM-Rollen.

AWS IoT Authentifiziert bei Message-Broker-Verbindungen über HTTP Benutzer, Gruppen und Rollen mithilfe des Signaturprozesses von Signature Version 4. Weitere Informationen finden Sie unter AWS API-Anfragen signieren.

Wenn Sie AWS Signature Version 4 mit verwenden AWS IoT, müssen Clients in ihrer TLS-Implementierung Folgendes unterstützen:

- TLS 1.2
- SHA-256 RSA-Zertifikats-Signaturprüfung für RSA-Zertifikate
- Eine der Cipher-Suiten aus dem Support-Abschnitt der TLS Cipher Suite.

Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT.

## Amazon-Cognito-Identitäten

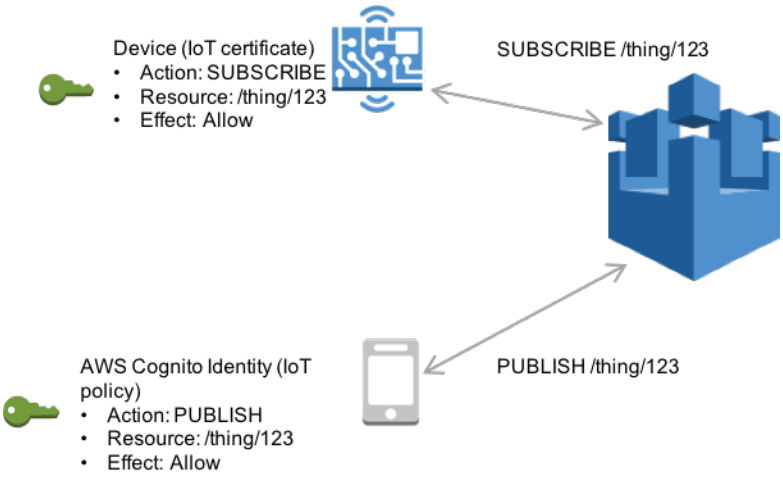
Amazon Cognito Identity ermöglicht es Ihnen, temporäre AWS Anmeldeinformationen mit eingeschränkten Rechten für die Verwendung in Mobil- und Webanwendungen zu erstellen. Wenn Sie Amazon Cognito Identity verwenden, erstellen Sie Identitätspools, die eindeutige Identitäten für Ihre Benutzer erstellen, und authentifizieren Sie sie bei Identitätsanbietern wie Login with Amazon, Facebook und Google. Sie können auch Amazon-Cognito-Identitäten mit Ihren eigenen vom Entwickler authentifizierten Identitäten verwenden. Weitere Informationen finden Sie unter Amazon Cognito Identity.

Um Amazon Cognito Identity zu verwenden, definieren Sie einen Amazon Cognito Cognito-Identitätspool, der einer IAM-Rolle zugeordnet ist. Die IAM-Rolle ist mit einer IAM-Richtlinie verknüpft, die Identitäten aus Ihrem Identitätspool den Zugriff auf Ressourcen wie Anrufdienste gewährt. AWS AWS

Amazon Cognito Identity erstellt nicht authentifizierte und authentifizierte Identitäten. Nicht authentifizierte Identitäten werden für Gastbenutzer in einer mobilen oder Webanwendung verwendet, die die App ohne Anmeldung nutzen möchten. Nicht authentifizierten Benutzern werden nur die Berechtigungen gewährt, die in der dem Identitätspool zugeordneten IAM-Richtlinie angegeben sind.

Wenn Sie authentifizierte Identitäten verwenden, müssen Sie zusätzlich zu der dem Identitätspool angehängten IAM-Richtlinie eine Richtlinie an eine Amazon Cognito AWS IoT Cognito-Identität anhängen. Um eine AWS IoT Richtlinie anzuhängen, verwenden Sie die AttachPolicyAPI und erteilen Sie einem einzelnen Benutzer Ihrer Anwendung Berechtigungen. AWS IoT Sie können die AWS IoT Richtlinie verwenden, um spezifische Berechtigungen für bestimmte Kunden und deren Geräte zuzuweisen.

Authentifizierte und nicht authentifizierte Benutzer sind unterschiedliche Identitätstypen. Wenn Sie der Amazon Cognito Identity keine AWS IoT Richtlinie beifügen, schlägt ein authentifizierter Benutzer die Autorisierung fehl AWS IoT und hat keinen Zugriff auf AWS IoT Ressourcen und Aktionen. Weitere Informationen zum Erstellen von Richtlinien für Amazon-Cognito-Identitäten finden Sie unter Beispiele für Veröffentlichungs-/Abonnement-Richtlinien und Autorisierung mit Amazon-Cognito-Identitäten.




## Benutzerspezifische Authentifizierung und Autorisierung

AWS IoT Core ermöglicht es Ihnen, benutzerdefinierte Autorisierer zu definieren, sodass Sie Ihre eigene Client-Authentifizierung und -Autorisierung verwalten können. Dies ist nützlich, wenn Sie andere Authentifizierungsmechanismen als die verwenden müssen, die von Haus aus unterstützt werden. AWS IoT Core (Weitere Informationen zu den nativ unterstützten Mechanismen finden Sie unter the section called “Client-Authentifizierung”.)

Wenn Sie beispielsweise vorhandene Geräte vor Ort zu migrieren AWS IoT Core und diese Geräte ein benutzerdefiniertes Bearer-Token oder einen MQTT-Benutzernamen und ein Passwort zur Authentifizierung verwenden, können Sie sie zu migrieren, AWS IoT Core ohne ihnen neue Identitäten bereitstellen zu müssen. Sie können die benutzerdefinierte Authentifizierung mit jedem der unterstützten Kommunikationsprotokolle verwenden. AWS IoT Core Weitere Informationen zu von AWS IoT Core unterstützten Protokollen finden Sie unter the section called “Gerätekommunikationsprotokolle”.

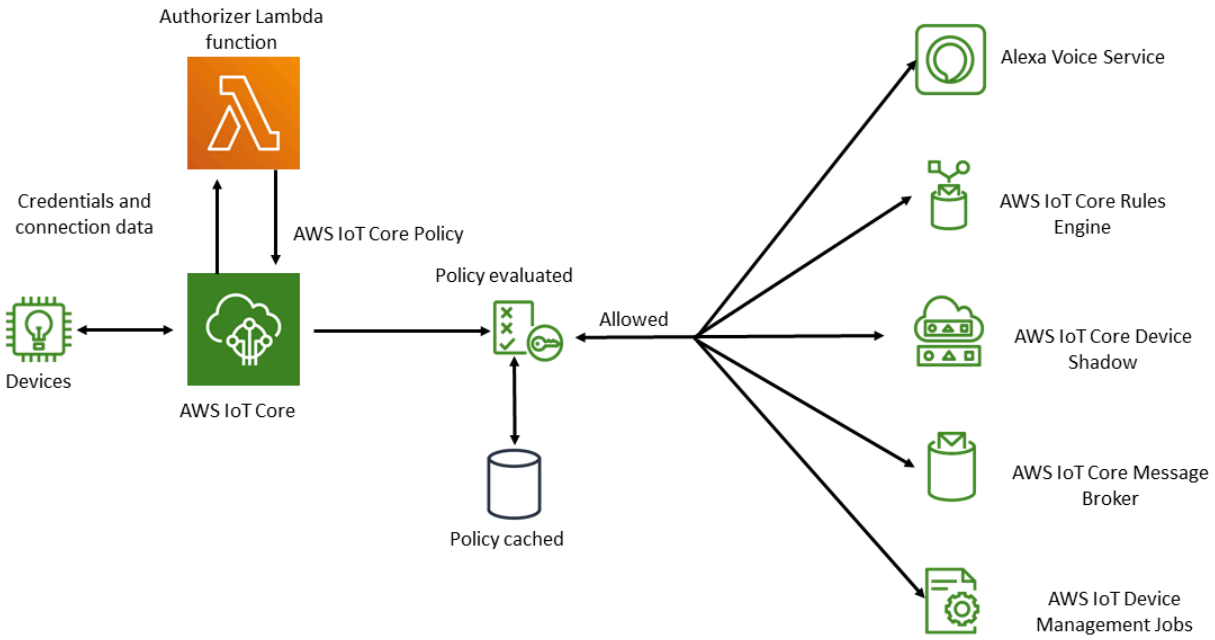
Themen

- Grundlegendes zum Workflow für die benutzerdefinierte Authentifizierung
- Benutzerdefinierte Autorisierer (CLI) erstellen und verwalten
- Benutzerdefinierte Authentifizierung mit X.509-Client-Zertifikaten
- Mithilfe der benutzerdefinierten Authentifizierung AWS IoT Core wird eine Verbindung hergestellt

- Fehlerbehebung für Ihre Genehmiger

## Grundlegendes zum Workflow für die benutzerdefinierte Authentifizierung

Mit der benutzerdefinierten Authentifizierung können Sie festlegen, wie Cliente mithilfe von Genehmigerressourcen authentifiziert und autorisiert werden.  Jeder Autorisierer enthält einen Verweis auf eine vom Kunden verwaltete Lambda-Funktion, einen optionalen öffentlichen Schlüssel zur Überprüfung der Geräteanmeldedaten und zusätzliche Konfigurationsinformationen. Das folgende Diagramm veranschaulicht den Autorisierungsablauf für die benutzerdefinierte Authentifizierung in. AWS IoT Core




AWS IoT Core benutzerdefinierter Authentifizierungs- und Autorisierungsworkflow

In der folgenden Liste werden die einzelnen Schritte des benutzerdefinierten Authentifizierungs- und Autorisierungsworkflows erläutert.

1. Ein Gerät stellt über einen der unterstützten Geräte eine Verbindung zum AWS IoT Core Datenendpunkt eines Kunden herthe section called “Gerätekommunikationsprotokolle”. Das Gerät übergibt Anmeldeinformationen entweder in die Header-Felder oder Abfrageparameter der Anfrage (für die WebSockets Protokolle HTTP Publish oder MQTT over) oder in das Feld für

Benutzername und Passwort der MQTT CONNECT-Nachricht (für die Protokolle MQTT und MQTT over). WebSockets

2. AWS IoT Core prüft auf eine von zwei Bedingungen:
   - Die eingehende Anforderung gibt einen Genehmiger an.
   - Für den AWS IoT Core Datenendpunkt, der die Anfrage empfängt, ist ein Standardautorisierer dafür konfiguriert.

   Wenn auf AWS IoT Core eine dieser Arten ein Autorisierer gefunden wird, wird die dem Autorisierer zugeordnete Lambda-Funktion AWS IoT Core ausgelöst.
3. (Optional) Wenn Sie die Tokensignatur aktiviert haben, AWS IoT Core validiert die Anforderungssignatur mithilfe des im Autorisierer gespeicherten öffentlichen Schlüssels, bevor die Lambda-Funktion ausgelöst wird. Wenn die Validierung fehlschlägt, stoppt AWS IoT Core die Anforderung, ohne die Lambda-Funktion aufzurufen.
4. Die Lambda-Funktion empfängt die Anmeldeinformationen und Verbindungsmetadaten in der Anforderung und trifft eine Authentifizierungsentscheidung.
5. Die Lambda-Funktion gibt die Ergebnisse der Authentifizierungsentscheidung und ein AWS IoT Core Richtliniendokument zurück, das festlegt, welche Aktionen in der Verbindung zulässig sind. Die Lambda-Funktion gibt auch Informationen zurück, die angeben, wie oft die Anmeldeinformationen in der Anforderung AWS IoT Core erneut überprüft werden, indem die Lambda-Funktion aufgerufen wird.
6. AWS IoT Core bewertet die Aktivität auf der Verbindung anhand der Richtlinie, die sie von der Lambda-Funktion erhalten hat.
7. Nachdem die Verbindung hergestellt wurde und Ihr benutzerdefinierter Authorizer Lambda zum ersten Mal aufgerufen wurde, kann der nächste Aufruf bei inaktiven Verbindungen ohne MQTT-Operationen um bis zu 5 Minuten verzögert werden. Danach folgen nachfolgende Aufrufe dem Aktualisierungsintervall in Ihrem benutzerdefinierten Authorizer Lambda. Dieser Ansatz kann übermäßige Aufrufe verhindern, die Ihr Lambda-Parallelitätslimit überschreiten könnten. AWS-Konto

### Überlegungen zur Skalierung

Da eine Lambda-Funktion die Authentifizierung und Autorisierung für Ihren Genehmiger abwickelt, unterliegt die Funktion den Lambda-Preis- und Servicebeschränkungen, z. B. der Rate der gleichzeitigen Ausführung. Weitere Informationen zu den Preisen für Lambda finden Sie unter Lambda-Preise. Sie können die Belastung Ihrer Lambda-Funktion verwalten, indem Sie die

`refreshAfterInSeconds`- und `disconnectAfterInSeconds`-Parameter in Ihrer Lambda-Funktionsantwort anpassen. Weitere Informationen über den Inhalt Ihrer Lambda-Funktionsantwort finden Sie unter the section called “Definieren Ihrer Lambda-Funktion”.

> **Note**
>
> Wenn Sie die Signierung aktiviert lassen, können Sie verhindern, dass Ihr Lambda übermäßig oft durch unbekannte Clients ausgelöst wird. Bedenken Sie dies, bevor Sie die Signierung in Ihrem Genehmiger deaktivieren.

> **Note**
>
> Das Timeout-Limit der Lambda-Funktion für den benutzerdefinierten Genehmiger beträgt 5 Sekunden.

## Benutzerdefinierte Autorisierer (CLI) erstellen und verwalten

AWS IoT Core implementiert benutzerdefinierte Authentifizierungs- und Autorisierungsschemata mithilfe benutzerdefinierter Autorisierer. Ein benutzerdefinierter Autorisierer ist eine AWS IoT Core Ressource, die Ihnen die Flexibilität bietet, Regeln und Richtlinien auf der Grundlage Ihrer spezifischen Anforderungen zu definieren und zu implementieren. Informationen zum Erstellen eines benutzerdefinierten Autorisierers mit step-by-step Anweisungen finden Sie unter Tutorial: Erstellen eines benutzerdefinierten Autorisierers für. AWS IoT Core

Jeder Genehmiger umfasst folgende Komponenten:

- Name: Eine eindeutige benutzerdefinierte Zeichenfolge, in der der Genehmiger identifiziert wird.
- ARN der Lambda-Funktion: Der Amazon-Ressourcenname (ARN) der Lambda-Funktion, die die Autorisierungs- und Authentifizierungslogik implementiert.
- Token-Schlüsselname: Der Schlüsselname, der verwendet wird, um das Token aus den HTTP-Headern, Abfrageparametern oder dem MQTT-CONNECT-Benutzernamen zu extrahieren, um die Signaturvalidierung durchzuführen. Dieser Wert ist erforderlich, wenn in Ihrem Genehmiger die Signierung aktiviert ist.
- Markierung „Signieren deaktiviert“ (optional): Ein boolescher Wert, der angibt, ob die Signaturanforderung für Anmeldeinformationen deaktiviert werden soll. Dies ist nützlich für

Szenarien, in denen das Signieren der Anmeldeinformationen keinen Sinn macht, z. B. bei Authentifizierungsschemata, die MQTT-Benutzernamen und -Passwörter verwenden. Der Standardwert ist `false`, also ist das Signieren standardmäßig aktiviert.

- Öffentlicher Schlüssel zur Tokensignierung: Der öffentliche Schlüssel, den AWS IoT Core zur Validierung der Tokensignatur verwendet. Die Mindestlänge beträgt 2.048 Bit. Dieser Wert ist erforderlich, wenn in Ihrem Genehmiger die Signierung aktiviert ist.

Lambda berechnet Ihnen die Anzahl der Ausführungen Ihrer Lambda-Funktion und die Dauer der Ausführung des Codes in Ihrer Funktion. Weitere Informationen zu den Preisen für Lambda finden Sie unter Lambda-Preise. Weitere Informationen zum Erstellen von Lambda-Funktionen finden Sie im Lambda-Entwicklerhandbuch.

> **Note**
>
> Wenn Sie die Signierung aktiviert lassen, können Sie verhindern, dass Ihr Lambda übermäßig oft durch unbekannte Clients ausgelöst wird. Bedenken Sie dies, bevor Sie die Signierung in Ihrem Genehmiger deaktivieren.

> **Note**
>
> Das Timeout-Limit der Lambda-Funktion für den benutzerdefinierten Genehmiger beträgt 5 Sekunden.

In diesem Kapitel:


- Definieren Ihrer Lambda-Funktion
- Erstellen eines Genehmigers
- Autorisieren AWS IoT zum Aufrufen Ihrer Lambda-Funktion
- Testen Ihrer Genehmiger
- Verwalten von benutzerdefinierten Genehmigern


## Definieren Ihrer Lambda-Funktion

Wenn AWS IoT Core Sie Ihren Autorisierer aufrufen, löst er das dem Autorisierer zugeordnete Lambda mit einem Ereignis aus, das das folgende JSON-Objekt enthält. Das JSON-Beispielobjekt

enthält alle möglichen Felder. Felder, die für die Verbindungsanforderung nicht relevant sind, sind nicht enthalten.

```
{
    "token" :"aToken",
    "signatureVerified": Boolean, // Indicates whether the device gateway has validated
 the signature.
    "protocols": ["tls", "http", "mqtt"], // Indicates which protocols to expect for
 the request.
    "protocolData": {
        "tls" : {
            "serverName": "serverName" // The server name indication (SNI) host_name
 string.
        },
        "http": {
            "headers": {
                "#{name}": "#{value}"
            },
            "queryString": "?#{name}=#{value}"
        },
        "mqtt": {
            "username": "myUserName",
            "password": "myPassword", // A base64-encoded string.
            "clientId": "myClientId" // Included in the event only when the device
 sends the value.
        }
    },
    "connectionMetadata": {
        "id": UUID // The connection ID. You can use this for logging.
    },
}
```

Die Lambda-Funktion sollte diese Informationen verwenden, um die eingehende Verbindung zu authentifizieren und zu entscheiden, welche Aktionen in der Verbindung zulässig sind. Die Funktion sollte eine Antwort senden, die die folgenden Werte enthält.

- `isAuthenticated`: Ein boolescher Wert, der angibt, ob die Anforderung authentifiziert wurde.
- `principalId`: Eine alphanumerische Zeichenfolge, die als Kennung für das Token dient, das von der benutzerdefinierten Autorisierungsanforderung gesendet wurde. Der Wert muss eine alphanumerische Zeichenfolge mit mindestens einem und nicht mehr als 128 Zeichen sein und dem folgenden regulären Ausdrucksmuster (Regex) entsprechen: `([a-zA-Z0-9]){1,128}`.

Sonderzeichen, die nicht alphanumerisch sind, dürfen nicht zusammen mit dem in verwendet werden. `principalId` AWS IoT Core Informationen darüber, ob nicht-alphanumerische Sonderzeichen für die zulässig sind, finden Sie in der Dokumentation zu anderen AWS Diensten. `principalId`

- `policyDocuments`: Eine Liste von AWS IoT Core Richtliniendokumenten im JSON-Format Weitere Informationen zum Erstellen von Richtlinien finden Sie unter. AWS IoT Core the section called “AWS IoT Core Richtlinien” Die maximale Anzahl von Richtliniendokumenten ist 10. Jedes Richtliniendokument darf maximal 2048 Zeichen enthalten.
- `disconnectAfterInSeconds`: Eine Ganzzahl, die die maximale Dauer der Verbindung zum AWS IoT Core -Gateway angibt (in Sekunden). Der Mindestwert ist 300 Sekunden und der Höchstwert 86 400 Sekunden. Der Standardwert ist 86.400.

> **Note**
>
> Der Wert von `disconnectAfterInSeconds` (von der Lambda-Funktion zurückgegeben) wird festgelegt, wenn die Verbindung hergestellt wird. Dieser Wert kann bei nachfolgenden Lambda-Aufrufen zur Richtlinienaktualisierung nicht geändert werden.

- `refreshAfterInSeconds`: Eine Ganzzahl, die das Intervall zwischen Richtlinienaktualisierungen angibt. Wenn dieses Intervall abläuft, ruft AWS IoT Core die Lambda-Funktion auf, um Richtlinienaktualisierungen zu ermöglichen. Der Mindestwert ist 300 Sekunden und der Höchstwert 86 400 Sekunden.

Das folgende JSON-Objekt enthält ein Beispiel für eine Antwort, die Ihre Lambda-Funktion senden kann.

```
{
"isAuthenticated":true, //A Boolean that determines whether client can connect.
"principalId": "xxxxxxxx",  //A string that identifies the connection in logs.
"disconnectAfterInSeconds": 86400,
"refreshAfterInSeconds": 300,
 "policyDocuments": [
      {
        "Version": "2012-10-17",
        "Statement": [
           {
              "Action": "iot:Publish",
              "Effect": "Allow",
```

```
            "Resource": "arn:aws:iot:us-east-1:<your_aws_account_id>:topic/
customauthtesting"
          }
        ]
      }
    ]
}
```

Der `policyDocument` Wert muss ein AWS IoT Core gültiges Richtliniendokument enthalten. Weitere Informationen zu AWS IoT Core Richtlinien finden Sie unterthe section called “AWS IoT Core Richtlinien”. In MQTT über TLS und MQTT über WebSockets Verbindungen wird diese Richtlinie für das im Feldwert angegebene Intervall AWS IoT Core zwischengespeichert. `refreshAfterInSeconds` Bei HTTP-Verbindungen wird die Lambda-Funktion für jede Autorisierungsanforderung aufgerufen, es sei denn, Ihr Gerät verwendet persistente HTTP-Verbindungen (auch HTTP-Keep-Alive oder HTTP-Verbindungswiederverwendung genannt). Sie können bei der Konfiguration des Genehmigers wählen, ob Sie das Caching aktivieren möchten. AWS IoT Core Autorisiert während dieses Intervalls Aktionen in einer bestehenden Verbindung gegen diese zwischengespeicherte Richtlinie, ohne Ihre Lambda-Funktion erneut auszulösen. Wenn bei der benutzerdefinierten Authentifizierung Fehler auftreten, AWS IoT Core wird die Verbindung beendet. AWS IoT Core beendet die Verbindung auch, wenn sie länger als der im Parameter angegebene Wert geöffnet war. `disconnectAfterInSeconds`

Im Folgenden finden JavaScript Sie eine Lambda-Beispielfunktion von Node.js, die in der MQTT Connect-Nachricht nach einem Passwort mit dem Wert von sucht `test` und eine Richtlinie zurückgibt, die die Erlaubnis erteilt, eine Verbindung AWS IoT Core mit einem Client herzustellen `myClientName` und zu einem Thema zu veröffentlichen, das denselben Clientnamen enthält. Wenn es das erwartete Passwort nicht findet, gibt es eine Richtlinie zurück, die diese beiden Aktionen verweigert.

```
// A simple Lambda function for an authorizer. It demonstrates
// how to parse an MQTT password and generate a response.

exports.handler = function(event, context, callback) {
    var uname = event.protocolData.mqtt.username;
    var pwd = event.protocolData.mqtt.password;
    var buff = new Buffer(pwd, 'base64');
    var passwd = buff.toString('ascii');
    switch (passwd) {
        case 'test':
            callback(null, generateAuthResponse(passwd, 'Allow'));
```

```
            break;
        default:
            callback(null, generateAuthResponse(passwd, 'Deny'));
    }
};

// Helper function to generate the authorization response.
var generateAuthResponse = function(token, effect) {
    var authResponse = {};
    authResponse.isAuthenticated = true;
    authResponse.principalId = 'TEST123';

    var policyDocument = {};
    policyDocument.Version = '2012-10-17';
    policyDocument.Statement = [];
    var publishStatement = {};
    var connectStatement = {};
    connectStatement.Action = ["iot:Connect"];
    connectStatement.Effect = effect;
    connectStatement.Resource = ["arn:aws:iot:us-east-1:123456789012:client/
myClientName"];
    publishStatement.Action = ["iot:Publish"];
    publishStatement.Effect = effect;
    publishStatement.Resource = ["arn:aws:iot:us-east-1:123456789012:topic/telemetry/
myClientName"];
    policyDocument.Statement[0] = connectStatement;
    policyDocument.Statement[1] = publishStatement;
    authResponse.policyDocuments = [policyDocument];
    authResponse.disconnectAfterInSeconds = 3600;
    authResponse.refreshAfterInSeconds = 300;

    return authResponse;
}
```

Die vorhergehende Lambda-Funktion gibt das folgende JSON zurück, wenn sie das erwartete Passwort von `test` in der MQTT-Connect-Nachricht empfängt. Die Werte der `password`- und `principalId`-Eigenschaften sind die Werte aus der MQTT-Connect-Nachricht.

```
{
  "password": "password",
  "isAuthenticated": true,
  "principalId": "principalId",
  "policyDocuments": [
```

```
    {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Action": "iot:Connect",
          "Effect": "Allow",
          "Resource": "*"
        },
        {
          "Action": "iot:Publish",
          "Effect": "Allow",
          "Resource": "arn:aws:iot:region:accountId:topic/telemetry/${iot:ClientId}"
        },
        {
          "Action": "iot:Subscribe",
          "Effect": "Allow",
          "Resource": "arn:aws:iot:region:accountId:topicfilter/telemetry/
${iot:ClientId}"
        },
        {
          "Action": "iot:Receive",
          "Effect": "Allow",
          "Resource": "arn:aws:iot:region:accountId:topic/telemetry/${iot:ClientId}"
        }
      ]
    }
  ],
  "disconnectAfterInSeconds": 3600,
  "refreshAfterInSeconds": 300
}
```

### Erstellen eines Genehmigers

Sie können mithilfe der API einen Autorisierer erstellen. CreateAuthorizer Das folgende Beispiel beschreibt den Befehl.

```
aws iot create-authorizer
--authorizer-name MyAuthorizer
--authorizer-function-arn arn:aws:lambda:us-
west-2:<account_id>:function:MyAuthorizerFunction  //The ARN of the Lambda function.
[--token-key-name MyAuthorizerToken //The key used to extract the token from headers.
[--token-signing-public-keys FirstKey=
 "-----BEGIN PUBLIC KEY-----
```

```
  [...insert your public key here...]
  -----END PUBLIC KEY-----"
[--status ACTIVE]
[--tags <value>]
[--signing-disabled | --no-signing-disabled]
```

Sie können den `signing-disabled`-Parameter verwenden, um die Signaturvalidierung für jeden Aufruf Ihres Genehmigers zu deaktivieren. Es wird ausdrücklich empfohlen, dass die Signierung nur wenn unbedingt notwendig zu deaktivieren. Die Signaturvalidierung schützt Sie vor übermäßigen Aufrufen Ihrer Lambda-Funktion von unbekannten Geräten. Sie können den `signing-disabled`-Status eines Genehmigers nicht mehr ändern, nachdem Sie ihn erstellt haben. Zum Ändern dieses Verhaltens müssen Sie einen anderen benutzerdefinierten Genehmiger mit einem anderen Wert für den `signing-disabled`-Parameter erstellen.

Die Werte für die `tokenKeyName`- und `tokenSigningPublicKeys`-Parameter sind optional, wenn Sie das Signieren deaktiviert haben. Sie sind jedoch erforderlich, wenn das Signieren aktiviert ist.

Nachdem Sie Ihre Lambda-Funktion und den benutzerdefinierten Autorisierer erstellt haben, müssen Sie dem AWS IoT Core Dienst ausdrücklich die Berechtigung erteilen, die Funktion in Ihrem Namen aufzurufen. Sie können dies mit dem folgenden Befehl tun.

> **Note**
>
> Der Standard-IoT-Endpunkt unterstützt möglicherweise nicht die Verwendung von benutzerdefinierten Autorisierern mit Lambda-Funktionen. Stattdessen können Sie Domänenkonfigurationen verwenden, um einen neuen Endpunkt zu definieren und diesen Endpunkt dann für den benutzerdefinierten Autorisierer anzugeben.

```
aws lambda add-permission --function-name <lambda_function_name>
--principal iot.amazonaws.com --source-arn <authorizer_arn>
--statement-id Id-123 --action "lambda:InvokeFunction"
```

Autorisieren AWS IoT zum Aufrufen Ihrer Lambda-Funktion

In diesem Abschnitt erteilen Sie der benutzerdefinierten Autorisierungsressource, die Sie gerade erstellt haben, die Erlaubnis, die Lambda-Funktion auszuführen. Um die Berechtigung zu erteilen, können Sie den CLI-Befehl add-permission verwenden.

Erteilen Sie Ihrer Lambda-Funktion die Erlaubnis mit dem AWS CLI

1. Geben Sie nach der Eingabe Ihrer Werte den folgenden Befehl ein. Beachten Sie, dass der Wert `statement-id` eindeutig sein muss. *Id-1234*Ersetzen Sie es durch den exakten Wert, den Sie haben, andernfalls wird möglicherweise eine `ResourceConflictException` Fehlermeldung angezeigt.

```
aws lambda add-permission  \
--function-name "custom-auth-function" \
--principal "iot.amazonaws.com" \
--action "lambda:InvokeFunction" \
--statement-id "Id-1234" \
--source-arn authorizerArn
```

2. Wenn der Befehl erfolgreich ist, gibt er eine Berechtigungsanweisung zurück, wie in diesem Beispiel. Sie können mit dem nächsten Abschnitt fortfahren, um den benutzerdefinierten Autorisierer zu testen.

```
{
    "Statement": "{\"Sid\":\"Id-1234\",\"Effect\":\"Allow\",\"Principal
\":{\"Service\":\"iot.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction
\",\"Resource\":\"arn:aws:lambda:Region:57EXAMPLE833:function:custom-
auth-function\",\"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":
\"arn:aws:lambda:Region:57EXAMPLE833:function:custom-auth-function\"}}}"
}
```

   Wenn der Befehl nicht erfolgreich ist, wird ein Fehler zurückgegeben, wie in diesem Beispiel. Sie müssen den Fehler überprüfen und korrigieren, bevor Sie fortfahren können.

```
An error occurred (AccessDeniedException) when calling the AddPermission operation:
 User: arn:aws:iam::57EXAMPLE833:user/EXAMPLE-1 is not authorized to perform:
 lambda:AddPer
mission on resource: arn:aws:lambda:Region:57EXAMPLE833:function:custom-auth-
function
```

### Testen Ihrer Genehmiger

Sie können die TestInvokeAuthorizerAPI verwenden, um den Aufruf und die Rückgabewerte Ihres Autorisierers zu testen. Mit dieser API können Sie Protokollmetadaten angeben und die Signaturvalidierung in Ihrem Authorizer testen.

Die folgenden Tabs zeigen, wie Sie den verwenden können, AWS CLI um Ihren Authorizer zu testen.

Unix-like

```
aws iot test-invoke-authorizer --authorizer-name NAME_OF_AUTHORIZER \
--token TOKEN_VALUE --token-signature TOKEN_SIGNATURE
```

Windows CMD

```
aws iot test-invoke-authorizer --authorizer-name NAME_OF_AUTHORIZER ^
--token TOKEN_VALUE --token-signature TOKEN_SIGNATURE
```

Windows PowerShell

```
aws iot test-invoke-authorizer --authorizer-name NAME_OF_AUTHORIZER `
--token TOKEN_VALUE --token-signature TOKEN_SIGNATURE
```

Der Wert des `token-signature`-Parameters ist das signierte Token. Weitere Informationen zum Abrufen dieses Werts finden Sie unter the section called “Signieren des Tokens”.

Wenn Ihr Genehmiger einen Benutzernamen und ein Passwort verwendet, können Sie diese Informationen mithilfe des `--mqtt-context`-Parameters weitergeben. Die folgenden Registerkarten zeigen, wie Sie mithilfe der `TestInvokeAuthorizer`-API ein JSON-Objekt, das einen Benutzernamen, ein Passwort und einen Clientnamen enthält, an Ihren benutzerdefinierten Genehmiger senden.

Unix-like

```
aws iot test-invoke-authorizer --authorizer-name NAME_OF_AUTHORIZER  \
--mqtt-context '{"username": "USER_NAME", "password": "dGVzdA==",
 "clientId":"CLIENT_NAME"}'
```

Windows CMD

```
aws iot test-invoke-authorizer --authorizer-name NAME_OF_AUTHORIZER  ^
--mqtt-context '{"username": "USER_NAME", "password": "dGVzdA==",
 "clientId":"CLIENT_NAME"}'
```

Windows PowerShell

```
aws iot test-invoke-authorizer --authorizer-name NAME_OF_AUTHORIZER  `
--mqtt-context '{"username": "USER_NAME", "password": "dGVzdA==",
 "clientId":"CLIENT_NAME"}'
```

Das Passwort muss base64-kodiert sein. Das folgende Beispiel zeigt, wie Sie ein Passwort in einer Unix-ähnlichen Umgebung kodieren.

```
echo -n PASSWORD | base64
```

Verwalten von benutzerdefinierten Genehmigern

Sie können Ihre Autorisierer wie folgt verwalten. APIs

- ListAuthorizers: Zeigt alle Autorisierer in Ihrem Konto an.
- DescribeAuthorizer: Zeigt die Eigenschaften des angegebenen Autorisierers an. Zu diesen Werten gehören das Erstellungsdatum, das Datum der letzten Änderung und andere Attribute.
- SetDefaultAuthorizer: Gibt den Standardautorisierer für Ihre AWS IoT Core Datenendpunkte an. AWS IoT Core verwendet diesen Autorisierer, wenn ein Gerät keine AWS IoT Core Anmeldeinformationen weitergibt und keinen Autorisierer angibt. Weitere Informationen zur Verwendung von AWS IoT Core Anmeldeinformationen finden Sie unter. the section called “Client-Authentifizierung”
- UpdateAuthorizer: Ändert den Status, den Namen des Token-Schlüssels oder die öffentlichen Schlüssel für den angegebenen Autorisierer.
- DeleteAuthorizer: Löscht den angegebenen Autorisierer.

> **Note**
>
> Sie können die Signaturanforderungen eines Genehmigers nicht aktualisieren. Das bedeutet, dass Sie das Signieren in einem vorhandenen Genehmiger, der dies fordert, nicht deaktivieren können. Sie können auch nicht die Anmeldung bei einem vorhandenen Genehmiger verlangen, der dies nicht fordert.

# Benutzerdefinierte Authentifizierung mit X.509-Client-Zertifikaten

Wenn Sie Geräte mit verbinden AWS IoT Core, stehen Ihnen mehrere Authentifizierungstypen zur Verfügung. Sie können X.509-Clientzertifikate verwenden, mit denen Sie Client- und Geräteverbindungen authentifizieren können, oder benutzerdefinierte Autorisierer definieren, um Ihre eigene Client-Authentifizierungs- und Autorisierungslogik zu verwalten. In diesem Thema wird beschrieben, wie Sie die benutzerdefinierte Authentifizierung mit X.509-Clientzertifikaten verwenden.

Die Verwendung einer benutzerdefinierten Authentifizierung mit X.509-Zertifikaten kann hilfreich sein, wenn Sie Ihre Geräte bereits mit X.509-Zertifikaten authentifiziert haben und zusätzliche Validierungen und benutzerdefinierte Autorisierungen durchführen möchten. Wenn Sie beispielsweise die Daten Ihrer Geräte, wie z. B. deren Seriennummern, im X.509-Client-Zertifikat speichern, können Sie nach der AWS IoT Core Authentifizierung des X.509-Client-Zertifikats einen benutzerdefinierten Autorisierer verwenden, um bestimmte Geräte anhand der im Feld des Zertifikats gespeicherten Informationen zu identifizieren. CommonName Die Verwendung einer benutzerdefinierten Authentifizierung mit X.509-Zertifikaten kann Ihr Gerätesicherheitsmanagement beim Verbinden von Geräten verbessern AWS IoT Core und bietet mehr Flexibilität bei der Verwaltung der Authentifizierungs- und Autorisierungslogik. AWS IoT Core unterstützt die benutzerdefinierte Authentifizierung mit X.509-Zertifikaten unter Verwendung des X.509-Zertifikats und des benutzerdefinierten Autorisierungstyps, der sowohl mit dem MQTT-Protokoll als auch mit dem HTTPS-Protokoll funktioniert. Weitere Informationen zu den Authentifizierungstypen und Anwendungsprotokollen, die von AWS IoT Core Geräteendpunkten unterstützt werden, finden Sie unter Gerätekommunikationsprotokolle.

> **Note**
>
> Die benutzerdefinierte Authentifizierung mit X.509-Clientzertifikaten wird in den AWS GovCloud (US) Regionen nicht unterstützt.

> **Important**
>
> Sie müssen einen Endpunkt verwenden, der mithilfe von Domänenkonfigurationen erstellt wurde. Darüber hinaus müssen Clients die Erweiterung Server Name Indication (SNI) angeben, wenn sie eine Verbindung herstellen AWS IoT Core.

Das Verfahren zur Authentifizierung von Geräten mithilfe der benutzerdefinierten Authentifizierung mit X.509-Clientzertifikaten besteht aus den folgenden Schritten.

- Schritt 1: Registrieren Sie Ihre X.509-Clientzertifikate bei AWS IoT Core
- Schritt 2: Erstellen einer Lambda-Funktion
- Schritt 3: Erstellen Sie einen benutzerdefinierten Autorisierer
- Schritt 4: Legen Sie den Authentifizierungstyp und das Anwendungsprotokoll in einer Domänenkonfiguration fest

### Schritt 1: Registrieren Sie Ihre X.509-Clientzertifikate bei AWS IoT Core

Falls Sie dies noch nicht getan haben, registrieren und aktivieren Sie Ihre X.509-Client-Zertifikate mit. AWS IoT Core Andernfalls überspringen Sie diesen Schritt und gehen Sie direkt zum nächsten.

Gehen Sie wie folgt vor AWS IoT Core, um Ihre Client-Zertifikate bei zu registrieren und zu aktivieren:

1. Wenn Sie Kundenzertifikate direkt mit erstellen AWS IoT. Diese Client-Zertifikate werden automatisch bei registriert AWS IoT Core.
2. Wenn Sie Ihre eigenen Client-Zertifikate erstellen, folgen Sie diesen Anweisungen, um sie zu registrieren AWS IoT Core.
3. Folgen Sie diesen Anweisungen, um Ihre Client-Zertifikate zu aktivieren.

### Schritt 2: Erstellen einer Lambda-Funktion

AWS IoT Core verwendet benutzerdefinierte Autorisierer, um benutzerdefinierte Authentifizierungs- und Autorisierungsschemata zu implementieren. Ein benutzerdefinierter Autorisierer ist mit einer Lambda-Funktion verknüpft, die bestimmt, ob ein Gerät authentifiziert ist und welche Operationen das Gerät ausführen darf. Wenn ein Gerät eine Verbindung herstellt AWS IoT Core, AWS IoT Core ruft es die Autorisierungsdetails ab, einschließlich des Autorisierernamens und der zugehörigen Lambda-Funktion, und ruft die Lambda-Funktion auf. Die Lambda-Funktion empfängt ein Ereignis, das ein JSON-Objekt mit den X.509-Client-Zertifikatsdaten des Geräts enthält. Ihre Lambda-Funktion verwendet dieses Event-JSON-Objekt, um die Authentifizierungsanfrage auszuwerten, die zu ergreifenden Aktionen zu entscheiden und eine Antwort zurückzusenden.

Beispiel für ein Lambda-Funktionsereignis

Das folgende JSON-Beispielobjekt enthält alle möglichen Felder, die eingeschlossen werden können. Das eigentliche JSON-Objekt wird nur Felder enthalten, die für die spezifische Verbindungsanforderung relevant sind.

```
{
 "token": "aToken",
 "signatureVerified": true,
 "protocols": [
  "tls",
  "mqtt"
 ],
 "protocolData": {
  "tls": {
   "serverName": "serverName",
   "x509CertificatePem": "x509CertificatePem",
   "principalId": "principalId"
  },
  "mqtt": {
   "clientId": "myClientId",
                    "username": "myUserName",
                    "password": "myPassword"
  }
 },
 "connectionMetadata": {
  "id": "UUID"
 }
}
```

`signatureVerified`

Ein boolescher Wert, der angibt, ob die im Authorizer konfigurierte Token-Signatur verifiziert wurde oder nicht, bevor die Lambda-Funktion des Autorisierers aufgerufen wird. Wenn der Autorisierer so konfiguriert ist, dass er die Tokensignatur deaktiviert, ist dieses Feld falsch.

`protocols`

Ein Array, das die Protokolle enthält, die für die Anfrage zu erwarten sind.

`protocolData`

Ein Objekt, das Informationen zu den in der Verbindung verwendeten Protokollen enthält. Es enthält protokollspezifische Details, die für die Authentifizierung, Autorisierung und mehr nützlich sein können.

`tls`- Dieses Objekt enthält Informationen zum TLS-Protokoll (Transport Layer Security).

- `serverName`- Die Hostnamenzeichenfolge (Server Name Indication, SNI). AWS IoT Core erfordert, dass Geräte die SNI-Erweiterung an das Transport Layer Security (TLS) -Protokoll senden und die vollständige Endpunktadresse vor Ort angeben. `host_name`
- `x509CertificatePem`- Das X.509-Zertifikat im PEM-Format, das für die Client-Authentifizierung in der TLS-Verbindung verwendet wird.
- `principalId`- Die dem Client in der TLS-Verbindung zugeordnete Prinzipal-ID.

`mqtt`- Dieses Objekt enthält Informationen zum MQTT-Protokoll.

- `clientId`- Eine Zeichenfolge muss nur für den Fall angegeben werden, dass das Gerät diesen Wert sendet.
- `username`- Der im MQTT Connect-Paket angegebene Benutzername.
- `password`- Das im MQTT Connect-Paket angegebene Passwort.

`connectionMetadata`

Metadaten der Verbindung.

`id`- Die Verbindungs-ID, die Sie für die Protokollierung und Fehlerbehebung verwenden können.

> **Note**
>
> In diesem Fall `principalId` handelt es sich um das JSON-Objekt `x509CertificatePem` und um zwei neue Felder in der Anfrage. Der Wert von `principalId` ist derselbe wie der Wert von`certificateId`. Weitere Informationen finden Sie unter Zertifikat.

Beispiel für eine Antwort auf eine Lambda-Funktion

Die Lambda-Funktion sollte Informationen aus dem JSON-Ereignisobjekt verwenden, um die eingehende Verbindung zu authentifizieren und zu entscheiden, welche Aktionen in der Verbindung zulässig sind.

Das folgende JSON-Objekt enthält eine Beispielantwort, die Ihre Lambda-Funktion senden kann.

```
{
 "isAuthenticated": true,
 "principalId": "xxxxxxxx",
 "disconnectAfterInSeconds": 86400,
 "refreshAfterInSeconds": 300,
 "policyDocuments": [
  {
   "Version": "2012-10-17",
   "Statement": [
    {
     "Effect": "Allow",
     "Action": "iot:Publish",
     "Resource": "arn:aws:iot:us-east-1:123456789012:topic/customauthtesting"
    }
   ]
  }
 ]
}
```

In diesem Beispiel sollte diese Funktion eine Antwort senden, die die folgenden Werte enthält.

`isAuthenticated`

Ein boolescher Wert, der angibt, ob die Anfrage authentifiziert ist.

`principalId`

Eine alphanumerische Zeichenfolge, die als Kennung für das von der benutzerdefinierten Autorisierungsanfrage gesendete Token dient. Der Wert muss eine alphanumerische Zeichenfolge mit mindestens einem und nicht mehr als 128 Zeichen sein. Es identifiziert die Verbindung in Protokollen. Der Wert von `principalId` muss mit dem Wert von `principalId` im Event-JSON-Objekt identisch sein (d. h. certificateId des X.509-Zertifikats).

`policyDocuments`

Eine Liste von Richtliniendokumenten im AWS IoT Core JSON-Format. Der Wert ist optional und unterstützt Ding-Richtlinienvariablen und Zertifikatsrichtlinienvariablen. Die maximale Anzahl von Richtliniendokumenten ist 10. Jedes Richtliniendokument darf maximal 2048 Zeichen enthalten. Wenn Sie mehrere Richtlinien an Ihr Client-Zertifikat und die Lambda-Funktion angehängt haben, ist die Berechtigung eine Sammlung aller Richtlinien. Weitere Informationen zum Erstellen von AWS IoT Core Richtlinien finden Sie unter Richtlinien.

`disconnectAfterInSeconds`

Eine Ganzzahl, die die maximale Dauer (in Sekunden) der Verbindung zum AWS IoT Core Gateway angibt. Der Mindestwert ist 300 Sekunden und der Höchstwert ist 86.400 Sekunden. `disconnectAfterInSeconds`gilt für die gesamte Lebensdauer einer Verbindung und wird bei aufeinanderfolgenden Richtlinienaktualisierungen nicht aktualisiert.

`refreshAfterInSeconds`

Eine Ganzzahl, die das Intervall zwischen Richtlinienaktualisierungen angibt. Wenn dieses Intervall abgelaufen ist, AWS IoT Core ruft die Lambda-Funktion auf, um Richtlinienaktualisierungen zu ermöglichen. Der Mindestwert ist 300 Sekunden und der Höchstwert 86 400 Sekunden.

### Beispiel-Lambda-Funktion

Im Folgenden finden Sie ein Beispiel für eine Lambda-Funktion von Node.js. Die Funktion untersucht das X.509-Zertifikat des Clients und extrahiert relevante Informationen wie die Seriennummer, den Fingerabdruck und den Namen des Antragstellers. Wenn die extrahierten Informationen den erwarteten Werten entsprechen, wird dem Client der Zugriff auf die Verbindung gewährt. Dieser Mechanismus stellt sicher, dass nur autorisierte Clients mit gültigen Zertifikaten eine Verbindung herstellen können.

```
const crypto = require('crypto');

exports.handler = async (event) => {

    // Extract the certificate PEM from the event
    const certPem = event.protocolData.tls.x509CertificatePem;

    // Parse the certificate using Node's crypto module
    const cert = new crypto.X509Certificate(certPem);

    var effect = "Deny";
    // Allow permissions only for a particular certificate serial, fingerprint, and
 subject
    if (cert.serialNumber === "7F8D2E4B9C1A5036DE8F7C4B2A91E5D80463BC9A1257" // This is
 a random serial
        && cert.fingerprint ===
 "F2:9A:C4:1D:B5:E7:08:3F:6B:D0:4E:92:A7:C1:5B:8D:16:0F:E3:7A" // This is a random
 fingerprint
        && cert.subject === "allow.example.com") {
```

```
      effect = "Allow";
    }

    return generateAuthResponse(event.protocolData.tls.principalId, effect);
};


// Helper function to generate the authorization response.
function generateAuthResponse(principalId, effect) {
    const authResponse = {
        isAuthenticated: true,
        principalId,
        disconnectAfterInSeconds: 3600,
        refreshAfterInSeconds: 300,
        policyDocuments: [
          {
            Version: "2012-10-17",
            Statement: [
              {
                Action: ["iot:Connect"],
                Effect: effect,
                Resource: [
                  "arn:aws:iot:us-east-1:123456789012:client/myClientName"
                ]
              },
              {
                Action: ["iot:Publish"],
                Effect: effect,
                Resource: [
                  "arn:aws:iot:us-east-1:123456789012:topic/telemetry/myClientName"
                ]
              },
              {
                Action: ["iot:Subscribe"],
                Effect: effect,
                Resource: [
                   "arn:aws:iot:us-east-1:123456789012:topicfilter/telemetry/
myClientName"
                ]
              },
              {
                Action: ["iot:Receive"],
                Effect: effect,
                Resource: [
```

```
                    "arn:aws:iot:us-east-1:123456789012:topic/telemetry/myClientName"
                ]
              }
            ]
          }
        ]
      };

  return authResponse;
}
```

Die vorhergehende Lambda-Funktion gibt das folgende JSON zurück, wenn sie ein Zertifikat mit der erwarteten Seriennummer, dem Fingerabdruck und dem Betreff empfängt. Der Wert von ist `x509CertificatePem` das im TLS-Handshake bereitgestellte Client-Zertifikat. Weitere Informationen finden Sie unter Definieren Ihrer Lambda-Funktion.

```
{
 "isAuthenticated": true,
 "principalId": "principalId in the event JSON object",
 "policyDocuments": [
  {
   "Version": "2012-10-17",
   "Statement": [
    {
     "Action": "iot:Connect",
     "Effect": "Allow",
     "Resource": "arn:aws:iot:us-east-1:123456789012:client/myClientName"
    },
    {
     "Action": "iot:Publish",
     "Effect": "Allow",
     "Resource": "arn:aws:iot:us-east-1:123456789012:topic/telemetry/myClientName"
    },
    {
     "Action": "iot:Subscribe",
     "Effect": "Allow",
     "Resource": "arn:aws:iot:us-east-1:123456789012:topicfilter/telemetry/
myClientName"
    },
    {
     "Action": "iot:Receive",
     "Effect": "Allow",
     "Resource": "arn:aws:iot:us-east-1:123456789012:topic/telemetry/myClientName"
```

```
    }
   ]
  }
 ],
 "disconnectAfterInSeconds": 3600,
 "refreshAfterInSeconds": 300
}
```

Schritt 3: Erstellen Sie einen benutzerdefinierten Autorisierer

Nachdem Sie die Lambda-Funktion definiert haben, erstellen Sie einen benutzerdefinierten Authorizer, um Ihre eigene Client-Authentifizierungs- und Autorisierungslogik zu verwalten. Sie können den detaillierten Anweisungen in Schritt 3: Erstellen einer Kundenautorisierungsressource und deren Autorisierung folgen. Weitere Informationen finden Sie unter Einen Autorisierer erstellen.

Bei der Erstellung des benutzerdefinierten Autorisierers müssen Sie die AWS IoT Erlaubnis erteilen, die Lambda-Funktion aufzurufen, nachdem sie erstellt wurde. Eine ausführliche Anleitung finden Sie unter Autorisieren AWS IoT zum Aufrufen Ihrer Lambda-Funktion.

Schritt 4: Legen Sie den Authentifizierungstyp und das Anwendungsprotokoll in einer Domänenkonfiguration fest

Um Geräte mithilfe einer benutzerdefinierten Authentifizierung mit X.509-Clientzertifikaten zu authentifizieren, müssen Sie den Authentifizierungstyp und das Anwendungsprotokoll in einer Domänenkonfiguration festlegen und die SNI-Erweiterung senden. Der Wert von `authenticationType` muss sein`CUSTOM_AUTH_X509`, und der Wert von `applicationProtocol` kann entweder oder sein. `SECURE_MQTT` `HTTPS`

Legen Sie den Authentifizierungstyp und das Anwendungsprotokoll in der Domänenkonfiguration (CLI) fest

Wenn Sie keine Domänenkonfiguration haben, verwenden Sie den create-domain-configurationBefehl, um eine zu erstellen. Der Wert von `authenticationType` muss sein`CUSTOM_AUTH_X509`, und der Wert von `applicationProtocol` kann entweder `SECURE_MQTT` oder sein`HTTPS`.

```
aws iot create-domain-configuration \
    --domain-configuration-name domainConfigurationName \
    --authentication-type CUSTOM_AUTH_X509 \
    --application-protocol SECURE_MQTT \
```

```
    --authorizer-config '{
        "defaultAuthorizerName": my-custom-authorizer
    }'
```

Wenn Sie bereits über eine Domänenkonfiguration verfügen, verwenden Sie bei `applicationProtocol` Bedarf den update-domain-configurationBefehl update `authenticationType` und. Beachten Sie, dass Sie den Authentifizierungstyp oder das Protokoll auf dem Standardendpunkt (`iot:Data-ATS`) nicht ändern können.

```
aws iot update-domain-configuration \
    --domain-configuration-name domainConfigurationName \
    --authentication-type CUSTOM_AUTH_X509 \
    --application-protocol SECURE_MQTT \
    --authorizer-config '{
        "defaultAuthorizerName": my-custom-authorizer
    }'
```

`domain-configuration-name`

Der Name der Domänenkonfiguration.

`authentication-type`

Der Authentifizierungstyp der Domänenkonfiguration. Weitere Informationen finden Sie unter Auswahl eines Authentifizierungstyps.

`application-protocol`

Das Anwendungsprotokoll, mit dem Geräte kommunizieren AWS IoT Core. Weitere Informationen finden Sie unter Auswahl eines Anwendungsprotokolls.

`--authorizer-config`

Ein Objekt, das die Autorisierungskonfiguration in einer Domänenkonfiguration angibt.

`defaultAuthorizerName`

Der Name des Autorisierers für eine Domänenkonfiguration.

Weitere Informationen finden Sie unter CreateDomainConfigurationund in UpdateDomainConfigurationder AWS IoT API-Referenz. Weitere Informationen zur Domänenkonfiguration finden Sie unter Domänenkonfigurationen.

## Mithilfe der benutzerdefinierten Authentifizierung AWS IoT Core wird eine Verbindung hergestellt

Geräte können AWS IoT Core mithilfe der benutzerdefinierten Authentifizierung mit jedem Protokoll, das Geräte-Messaging AWS IoT Core unterstützt, eine Verbindung herstellen. Weitere Informationen zu unterstützten Kommunikationsprotokollen finden Sie unter the section called "Gerätekommunikationsprotokolle". Die Verbindungsdaten, die Sie an die Lambda-Funktion Ihres Genehmigers übergeben, hängen vom verwendeten Protokoll ab. Weitere Informationen zum Erstellen der Lambda-Funktion Ihres Genehmigers finden Sie unter the section called "Definieren Ihrer Lambda-Funktion". In den folgenden Abschnitten wird erläutert, wie Sie eine Verbindung zur Authentifizierung mit jedem unterstützten Protokoll herstellen.

### HTTPS

Geräte, an die Daten AWS IoT Core mithilfe der HTTP Publish API gesendet werden, können Anmeldeinformationen entweder über Anforderungsheader oder Abfrageparameter in ihren HTTP-POST-Anfragen übergeben. Geräte können mithilfe des Header- oder Abfrageparameters `x-amz-customauthorizer-name` einen aufzurufenden Genehmiger angeben. Wenn Sie die Tokensignatur in Ihrem Genehmiger aktiviert haben, müssen Sie den *`token-key-name`* und die `x-amz-customauthorizer-signature` entweder in den Anforderungsheadern oder Abfrageparametern übergeben. Beachten Sie, dass der *`token-signature`* Wert URL-codiert sein muss, wenn er vom Browser JavaScript aus verwendet wird.

> **Note**
>
> Der Kundengenehmiger für das HTTPS-Protokoll unterstützt nur Veröffentlichungsvorgänge. Weitere Informationen über das HTTP-Protokoll finden Sie unter the section called "Gerätekommunikationsprotokolle".

Die folgenden Beispielanforderungen zeigen, wie Sie diese Parameter sowohl in Anforderungsheadern als auch in Abfrageparametern übergeben.

```
//Passing credentials via headers
POST /topics/topic?qos=qos HTTP/1.1
Host: your-endpoint
x-amz-customauthorizer-signature: token-signature
token-key-name: token-value
```

```
x-amz-customauthorizer-name: authorizer-name

//Passing credentials via query parameters
POST /topics/topic?qos=qos&x-amz-customauthorizer-signature=token-signature&token-key-name=token-value HTTP/1.1
```

MQTT

Geräte, die über eine MQTT-Verbindung eine Verbindung herstellen, können Anmeldeinformationen über die `password` Felder `username` und AWS IoT Core von MQTT-Nachrichten weiterleiten. Der Wert `username` kann optional auch eine Abfragezeichenfolge enthalten, die zusätzliche Werte (einschließlich eines Tokens, einer Signatur und eines Genehmigernamens) an Ihren Genehmiger übergibt. Sie können diese Abfragezeichenfolge verwenden, wenn Sie anstelle der Werte `username` und `password` ein tokenbasiertes Authentifizierungsschema verwenden möchten.

> **Note**
>
> Die Daten im Passwortfeld sind Base64-codiert von. AWS IoT Core Ihre Lambda-Funktion muss sie dekodieren.

Das folgende Beispiel enthält eine `username`-Zeichenfolge mit zusätzlichen Parametern, die ein Token und eine Signatur angeben.

```
username?x-amz-customauthorizer-name=authorizer-name&x-amz-customauthorizer-signature=token-signature&token-key-name=token-value
```

Um einen Authorizer aufzurufen, müssen Geräte, die über MQTT und benutzerdefinierte Authentifizierung eine Verbindung herstellen, eine Verbindung über Port 443 herstellen. AWS IoT Core Sie müssen außerdem die TLS-Erweiterung Application Layer Protocol Negotiation (ALPN) mit dem Wert `mqtt` und die Erweiterung Server Name Indication (SNI) mit dem Hostnamen ihres Datenendpunkts übergeben. AWS IoT Core Der Wert `x-amz-customauthorizer-signature` sollte URL-kodiert sein, um Fehler zu vermeiden. Wir empfehlen außerdem dringend, dass die Werte `x-amz-customauthorizer-name` und `token-key-name` URL-kodiert sind. Weitere Informationen zu diesen Werten finden Sie unter the section called “Gerätekommunikationsprotokolle”. Die V2 AWS IoT Geräte SDKs - SDKs, Mobil- und AWS IoT Geräteclient kann diese beiden Erweiterungen konfigurieren.

### MQTT über WebSockets

Geräte, die AWS IoT Core über MQTT-Over eine Verbindung herstellen, WebSockets können Anmeldeinformationen auf eine der beiden folgenden Arten weitergeben.

- Über Anforderungsheader oder Abfrageparameter in der HTTP-UPGRADE-Anfrage, um die WebSockets Verbindung herzustellen.
- Über die Felder `username` und `password` in der MQTT-CONNECT-Nachricht.

Wenn Sie Anmeldeinformationen über die MQTT-Connect-Nachricht weitergeben, sind die TLS-Erweiterungen ALPN und SNI erforderlich. Weitere Informationen zu diesen Erweiterungen finden Sie unter the section called “MQTT”. Das folgende Beispiel zeigt, wie Sie Anmeldeinformationen über die HTTP-Upgrade-Anforderung übergeben.

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

#### Signieren des Tokens

Sie müssen das Token mit dem privaten Schlüssel des Paars aus öffentlichem und privatem Schlüssel signieren, das Sie im `create-authorizer`-Aufruf verwendet haben. Die folgenden Beispiele zeigen, wie die Tokensignatur mithilfe eines UNIX-ähnlichen Befehls und erstellt wird. JavaScript Sie verwenden den SHA-256-Hash-Algorithmus, um die Signatur zu kodieren.

Command line

```
echo -n TOKEN_VALUE | openssl dgst -sha256 -sign PEM encoded RSA private key |
 openssl base64
```

JavaScript

```
const crypto = require('crypto')

const key = "PEM encoded RSA private key"

const k = crypto.createPrivateKey(key)
let sign = crypto.createSign('SHA256')
sign.write(t)
sign.end()
const s = sign.sign(k, 'base64')
```

## Fehlerbehebung für Ihre Genehmiger

In diesem Thema werden häufig auftretende Probleme, die zu Konflikten bei benutzerdefinierten Authentifizierungsworkflows führen können, sowie Schritte zu deren Behebung beschrieben. Um Probleme am effektivsten zu beheben, aktivieren Sie CloudWatch Protokolle für AWS IoT Core und setzen Sie die Protokollebene auf DEBUG. Sie können CloudWatch Protokolle in der AWS IoT Core Konsole aktivieren (https://console.aws.amazon.com/iot/). Weitere Informationen zum Aktivieren und Konfigurieren von Protokollen für AWS IoT Core finden Sie unter the section called “Konfigurieren Sie die AWS IoT Protokollierung”.

> **Note**
>
> Wenn Sie die Protokollebene für längere Zeit auf DEBUG belassen, CloudWatch können große Mengen an Protokolldaten gespeichert werden. Dies kann Ihre CloudWatch Gebühren erhöhen. Erwägen Sie, die ressourcenbasierte Protokollierung zu verwenden, um die Ausführlichkeit nur für Geräte in einer bestimmten Objektgruppe zu erhöhen. Weitere Informationen zur ressourcenbasierten Protokollierung finden Sie unter the section called “Konfigurieren Sie die AWS IoT Protokollierung”. Wenn Sie mit der Fehlerbehebung fertig sind, reduzieren Sie außerdem die Protokollebene auf eine weniger ausführliche Ebene.

Bevor Sie mit der Problembehandlung beginnen, überprüfen Sie the section called “Grundlegendes zum Workflow für die benutzerdefinierte Authentifizierung” für eine allgemeine Übersicht über den benutzerdefinierten Authentifizierungsprozess. Dadurch können Sie leichter die mögliche Ursache eines Problems nachvollziehen und danach suchen.

In diesem Thema werden zwei Bereiche behandelt, die Sie untersuchen sollten.

- Probleme im Zusammenhang mit der Lambda-Funktion Ihres Genehmigers.
- Probleme im Zusammenhang mit Ihrem Gerät.

### Nach Problemen mit der Lambda-Funktion Ihres Genehmigers suchen

Gehen Sie wie folgt vor, um sicherzustellen, dass die Verbindungsversuche Ihrer Geräte Ihre Lambda-Funktion aufrufen.

1. Überprüfen Sie, welche Lambda-Funktion Ihrem Genehmiger zugeordnet ist.

   Sie können dies tun, indem Sie die DescribeAuthorizerAPI aufrufen oder im Bereich Secure der AWS IoT Core Konsole auf den gewünschten Autorisierer klicken.
2. Überprüfen Sie die Aufrufmetriken der Lambda-Funktion. Führen Sie dazu die folgenden Schritte aus.

   a. Öffnen Sie die AWS Lambda Konsole (https://console.aws.amazon.com/lambda/) und wählen Sie die Funktion aus, die Ihrem Autorisierer zugeordnet ist.

   b. Wählen Sie die Registerkarte Überwachen und überprüfen Sie die Metriken des für Ihr Problem relevanten Zeitraums.
3. Wenn Sie keine Aufrufe sehen, überprüfen Sie, ob der Benutzer berechtigt AWS IoT Core ist, Ihre Lambda-Funktion aufzurufen. Wenn Sie Aufrufe sehen, fahren Sie mit dem nächsten Schritt fort. Führen Sie die folgenden Schritte aus, um sicherzustellen, dass Ihre Lambda-Funktion über die erforderlichen Berechtigungen verfügt.

   a. Wählen Sie in der Konsole den Tab „Berechtigungen“ für Ihre Funktion aus. AWS Lambda

   b. Suchen Sie den Abschnitt Ressourcenbasierte Richtlinie am Seitenende. Wenn Ihre Lambda-Funktion über die erforderlichen Berechtigungen verfügt, sieht die Richtlinie wie im folgenden Beispiel aus.

```
{
  "Version": "2012-10-17",
  "Id": "default",
  "Statement": [
    {
      "Sid": "Id123",
      "Effect": "Allow",
      "Principal": {
        "Service": "iot.amazonaws.com"
      },
```

```
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-
east-1:111111111111:function:FunctionName",
      "Condition": {
        "ArnLike": {
          "AWS:SourceArn": "arn:aws:iot:us-east-1:111111111111:authorizer/
AuthorizerName"
        },
        "StringEquals": {
          "AWS:SourceAccount": "111111111111"
        }
      }
    }
  ]
}
```

c. Diese Richtlinie erteilt dem AWS IoT Core Schulleiter die `InvokeFunction` Erlaubnis für Ihre Funktion. Wenn Sie sie nicht sehen, müssen Sie sie mithilfe der AddPermissionAPI hinzufügen. Im folgenden Beispiel wird gezeigt, wie Sie sie über AWS CLI hinzufügen können.

```
aws lambda add-permission --function-name FunctionName --principal
 iot.amazonaws.com --source-arn AuthorizerARn --statement-id Id-123 --action
 "lambda:InvokeFunction"
```

4. Wenn Sie Aufrufe sehen, stellen Sie sicher, dass keine Fehler vorliegen. Ein Fehler könnte darauf hinweisen, dass die Lambda-Funktion das Verbindungsereignis, das an sie AWS IoT Core gesendet wird, nicht richtig verarbeitet.

   Hinweise zur Behandlung des Ereignisses in Ihrer Lambda-Funktion finden Sie unter the section called “Definieren Ihrer Lambda-Funktion”. Sie können die Testfunktion in der AWS Lambda Konsole (https://console.aws.amazon.com/lambda/) verwenden, um Testwerte in der Funktion fest zu codieren, um sicherzustellen, dass die Funktion Ereignisse korrekt verarbeitet.

5. Wenn Sie Aufrufe ohne Fehler sehen, Ihre Geräte jedoch keine Verbindung herstellen (oder Nachrichten veröffentlichen, abonnieren und empfangen) können, liegt das Problem möglicherweise daran, dass die Richtlinie, die Ihre Lambda-Funktion zurückgibt, keine Berechtigungen für die Aktionen gewährt, die Ihre Geräte ausführen möchten. Führen Sie die folgenden Schritte aus, um festzustellen, ob ein Fehler bei der Richtlinie vorliegt, die die Funktion zurückgibt.

a. Verwenden Sie eine Amazon CloudWatch Logs Insights-Abfrage, um Protokolle über einen kurzen Zeitraum auf Fehler zu überprüfen. Die folgende Beispielabfrage sortiert Ereignisse nach Zeitstempel und sucht nach Fehlern.

```
display clientId, eventType, status, @timestamp | sort @timestamp desc | filter
 status = "Failure"
```

b. Aktualisieren Sie Ihre Lambda-Funktion, um die Daten zu protokollieren, zu denen sie zurückkehrt, AWS IoT Core und das Ereignis, das die Funktion auslöst. Sie können diese Protokolle verwenden, um die Richtlinie zu überprüfen, die die Funktion erstellt.

6. Wenn Sie Aufrufe ohne Fehler sehen, Ihre Geräte jedoch keine Verbindung herstellen (oder Nachrichten veröffentlichen, abonnieren und empfangen) können, könnte eine weitere Ursache sein, dass Ihre Lambda-Funktion das Timeout-Limit überschritten hat. Das Timeout-Limit der Lambda-Funktion für den benutzerdefinierten Genehmiger beträgt 5 Sekunden. Sie können die Funktionsdauer in CloudWatch Protokollen oder Metriken überprüfen.

Untersuchen von Geräteproblemen

Wenn Sie keine Probleme mit dem Aufrufen Ihrer Lambda-Funktion oder mit der Richtlinie, die die Funktion zurückgibt, feststellen, suchen Sie nach Problemen bei den Verbindungsversuchen Ihrer Geräte. Fehlerhaft formatierte Verbindungsanfragen können dazu führen, dass Ihr Autorisierer AWS IoT Core nicht ausgelöst wird. Verbindungsprobleme können sowohl auf TLS- als auch auf Anwendungsebene auftreten.

Mögliche Probleme mit der TLS-Ebene:

- Kunden müssen bei allen benutzerdefinierten Authentifizierungsanfragen entweder einen Hostnamen-Header (HTTP, MQTT over WebSockets) oder die Server Name Indication TLS-Erweiterung (HTTP, MQTT over WebSockets, MQTT) übergeben. In beiden Fällen muss der übergebene Wert mit einem der Datenendpunkte Ihres Kontos übereinstimmen. AWS IoT Core Dies sind die Endpunkte, die zurückgegeben werden, wenn Sie die folgenden CLI-Befehle ausführen.
  - `aws iot describe-endpoint --endpoint-type iot:Data-ATS`
  - `aws iot describe-endpoint --endpoint-type iot:Data`(für ältere VeriSign Endpunkte)

- Geräte, die eine benutzerdefinierte Authentifizierung in MQTT-Verbindungen verwenden, müssen auch die TLS-Erweiterung „Application Layer Protocol Negotiation“ (ALPN) mit dem Wert `mqtt` übergeben.
- Die benutzerdefinierte Authentifizierung ist derzeit nur auf Port 443 verfügbar.

Mögliche Probleme auf Anwendungsebene:

- Wenn das Signieren aktiviert ist (das Feld `signingDisabled` in Ihrem Genehmiger lautet „false“), suchen Sie nach den folgenden Signaturproblemen.
  - Stellen Sie sicher, dass Sie die Tokensignatur entweder im `x-amz-customauthorizer-signature`-Header oder in einem Abfragezeichenfolgenparameter übergeben.
  - Stellen Sie sicher, dass der Service keinen anderen Wert als das Token signiert.
  - Stellen Sie sicher, dass Sie das Token im Header- oder Abfrageparameter übergeben, den Sie im Feld `token-key-name` in Ihrem Genehmiger angegeben haben.
- Stellen Sie sicher, dass der Genehmigername, den Sie im `x-amz-customauthorizer-name`-Header- oder Abfragezeichenfolgenparameter übergeben, gültig ist oder dass Sie einen Standardgenehmiger für Ihr Konto angegeben haben.

# Autorisierung

Autorisierung ist der Prozess der Erteilung von Berechtigungen an eine authentifizierte Identität. Sie gewähren Nutzungsberechtigungen AWS IoT Core und IAM-Richtlinien. AWS IoT Core Dieses Thema behandelt AWS IoT Core -Richtlinien. Weitere Informationen zu IAM-Richtlinien finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT und Wie AWS IoT funktioniert mit IAM.

AWS IoT Core Richtlinien bestimmen, was eine authentifizierte Identität bewirken kann. Eine authentifizierte Identität wird von Geräten, mobilen Anwendungen, Webanwendungen und Desktop-Anwendungen verwendet. Eine authentifizierte Identität kann sogar ein Benutzer sein, der AWS IoT Core CLI-Befehle eingibt. Eine Identität kann nur dann AWS IoT Core Operationen ausführen, wenn sie über eine Richtlinie verfügt, die ihr die Erlaubnis für diese Operationen erteilt.

Sowohl AWS IoT Core Richtlinien als auch IAM-Richtlinien werden verwendet, um die Operationen AWS IoT Core zu steuern, die eine Identität (auch Principal genannt) ausführen kann. Welchen Richtlinientyp Sie verwenden, hängt von der Art der Identität ab, mit der Sie sich authentifizieren. AWS IoT Core

AWS IoT Core Operationen sind in zwei Gruppen unterteilt:

- Mit der API der Steuerebene können Sie administrative Aufgaben wie Erstellen oder Aktualisieren von Zertifikaten, Things, Regeln usw. ausführen.
- Die Data Plane API ermöglicht das Senden von Daten an und das Empfangen von Daten von AWS IoT Core.

Der von Ihnen verwendete Richtlinientyp hängt davon ab, ob Sie die API der Steuerebene oder der Datenebene nutzen.

In der folgenden Tabelle sind die Identitätstypen, die von ihnen verwendeten Protokolle und die Richtlinientypen für die Autorisierung aufgelistet.

AWS IoT Core Datenebenen-API und Richtlinientypen

| Protokoll- und Authentifizierungsmechanismus | SDK | Identitätstyp | Richtlinientyp |
|---|---|---|---|
| MQTT über TLS/TCP, gegenseitige TLS-Authentifizierung (Port 8883 oder 443)[†]) | AWS IoT Geräte-SDK | X.509-Zertifikate | AWS IoT Core Richtlinie |
| MQTT über HTTPS/WebSocket, AWS SigV4-Authentifizierung (Port 443) | AWS SDK für Mobilgeräte | Eine authentifizierte Amazon-Cognito-Identität | IAM und Richtlinien AWS IoT Core |
| | | Eine nicht authentifizierte Amazon-Cognito-Identität | IAM-Richtlinie |

| Protokoll- und Authentifizierungsmechanismus | SDK | Identitätstyp | Richtlinientyp | | |
|---|---|---|---|---|---|
| | | IAM oder Verbundidentität | IAM-Richtlinie | | |
| HTTPS, Authentifizierung mit AWS Signaturversion 4 (Port 443) | AWS CLI | Amazon-Cognito, IAM oder Verbundidentität | IAM-Richtlinie | | |
| HTTPS, gegenseitige TLS-Authentifizierung (Port 8443) | Keine SDK-Unterstützung | X.509-Zertifikate | AWS IoT Core Richtlinie | | |
| HTTPS über benutzerdefinierte Authentifizierung (Port 443) | AWS IoT Geräte-SDK | Genehmiger | Genehmigerrichtlinie | | |

AWS IoT Core API- und Richtlinientypen auf der Kontrollebene

| Protokoll- und Authentifizierungsmechanismus | SDK | Identitätstyp | Richtlinientyp | | |
|---|---|---|---|---|---|
| AWS HTTPS-Signaturauthentifizierung, Version 4 (Port 443) | AWS CLI | Amazon-Cognito-Identität | IAM-Richtlinie | | |
| | | IAM oder Verbundidentität | IAM-Richtlinie | | |

AWS IoT Core Richtlinien sind an X.509-Zertifikate, Amazon Cognito Cognito-Identitäten oder Dinggruppen angehängt. IAM-Richtlinien sind einem IAM-Benutzer, einer IAM-Gruppe oder einer IAM-Rolle angefügt. Wenn Sie die AWS IoT Konsole oder die AWS IoT Core CLI verwenden, um die Richtlinie anzuhängen (an ein Zertifikat, Amazon Cognito Identity oder eine Dinggruppe), verwenden Sie eine AWS IoT Core Richtlinie. Andernfalls verwenden Sie eine IAM-Richtlinie. AWS IoT Core Richtlinien, die einer Dinggruppe zugeordnet sind, gelten für alle Dinge innerhalb dieser Dinggruppe. Damit die AWS IoT Core Richtlinie wirksam wird, müssen der Name `clientId` und der Name der Sache übereinstimmen.

Die richtlinienbasierte Autorisierung ist ein leistungsstarkes Werkzeug. Sie gibt Ihnen die komplette Kontrolle darüber, welche Berechtigungen ein Gerät, ein Benutzer oder eine Anwendung in AWS IoT Core hat. Stellen Sie sich zum Beispiel ein Gerät vor, zu dem über ein Zertifikat eine AWS IoT Core Verbindung hergestellt wird. Sie können dem Gerät den Zugriff auf alle MQTT-Topics gewähren oder seinen Zugriff auf ein einzelnes Topic einschränken. Ein anderes Beispiel ist ein Benutzer, der CLI-Befehle in der Befehlszeile eingibt. Mithilfe einer Richtlinie können Sie dem Benutzer den Zugriff auf Befehle oder AWS IoT Core Ressourcen gewähren oder verweigern. Sie können auch den Zugriff einer Anwendung auf AWS IoT Core -Ressourcen steuern.

Aufgrund der Art und Weise, in der AWS IoT Richtliniendokumente zwischenspeichert, kann es einige Minuten dauern, bis Änderungen an einer Richtlinie wirksam werden. Das heißt, dass es einige Minuten dauern kann, bis der kürzlich gewährte Zugriff auf eine Ressource tatsächlich hergestellt ist. Außerdem kann nach dem Widerruf des Zugriffs noch mehrere Minuten lang auf eine Ressource zugegriffen werden.

## AWS Schulung und Zertifizierung

Weitere Informationen zur Autorisierung finden Sie im AWS IoT Core Kurs Deep Dive into AWS IoT Core Authentication and Authorization auf der Website für AWS Schulungen und Zertifizierungen.

## AWS IoT Core Richtlinien

AWS IoT Core Richtlinien sind JSON-Dokumente. Sie folgen denselben Konventionen wie IAM-Richtlinien. AWS IoT Core unterstützt benannte Richtlinien, sodass viele Identitäten auf dasselbe Richtliniendokument verweisen können. Bei benannten Richtlinien wird Versionierung verwendet, um Rollbacks zu vereinfachen.

AWS IoT Core Mithilfe von Richtlinien können Sie den Zugriff auf die AWS IoT Core Datenebene steuern. Die AWS IoT Core -Datenebene besteht aus Operationen, mit denen Sie eine Verbindung zum AWS IoT Core Message Broker herstellen, MQTT-Nachrichten senden und empfangen sowie einen Geräteschatten abrufen oder aktualisieren können.

Eine AWS IoT Core Richtlinie ist ein JSON-Dokument, das eine oder mehrere Richtlinienerklärungen enthält. Jede Anweisung enthält:

- `Effect`, das angibt, ob die Aktion zugelassen oder verweigert wird.
- `Action`, das die Aktion angibt, die die Richtlinie zulässt oder verweigert.
- `Resource`, das die Ressource oder die Ressourcen angibt, für die die Aktion zugelassen oder verweigert wird.

Es kann zwischen 6 und 8 Minuten dauern, bis Änderungen an einer Richtlinie wirksam werden, da die Richtliniendokumente AWS IoT zwischengespeichert werden. Das heißt, dass es einige Minuten dauern kann, bis der kürzlich gewährte Zugriff auf eine Ressource tatsächlich hergestellt ist. Außerdem kann nach dem Widerruf des Zugriffs noch mehrere Minuten lang auf eine Ressource zugegriffen werden.

AWS IoT Core Richtlinien können an X.509-Zertifikate, Amazon Cognito Cognito-Identitäten und Dinggruppen angehängt werden. Die einer Objektgruppe angefügten Richtlinien gelten für alle Objekte innerhalb dieser Gruppe. Damit die Richtlinie wirksam wird, müssen die `clientId` und der Objektname übereinstimmen. AWS IoT Core -Richtlinien folgen derselben Richtlinienbewertungslogik wie IAM-Richtlinien. Standardmäßig werden alle Richtlinien implizit verweigert. Eine explizite Zugriffserlaubnis in einer identitätsbasierten oder ressourcenbasierten Richtlinie setzt das Standardverhalten außer Kraft. Eine explizite Zugriffsverweigerung überschreibt

jede Zugriffserlaubnis in einer Richtlinie. Weitere Informationen finden Sie unter Auswertungslogik für Richtlinien im AWS Identity and Access Management -Benutzerhandbuch.

Themen


- AWS IoT Core politische Maßnahmen
- AWS IoT Core Ressourcen für Aktionen
- AWS IoT Core Richtlinienvariablen
- Serviceübergreifende Confused-Deputy-Prävention
- AWS IoT Core Beispiele für Richtlinien
- Autorisierung mit Amazon-Cognito-Identitäten


## AWS IoT Core politische Maßnahmen

Die folgenden Richtlinienaktionen werden von AWS IoT Core definiert:

MQTT-Richtlinienaktionen

`iot:Connect`

Stellt die Berechtigung dar, eine Verbindung zum AWS IoT Core Message Broker herzustellen. Die Berechtigung `iot:Connect` wird jedes Mal geprüft, wenn eine `CONNECT`-Anforderung an den Broker gesendet wird. Der Message Broker ermöglicht nicht die gleichzeitige Verbindung von zwei Clients mit der gleichen Client-ID. Nachdem sich der zweite Client verbunden hat, schließt der Broker die bestehende Verbindung. Verwenden Sie die `iot:Connect`-Berechtigung, um sicherzustellen, dass sich nur autorisierte Clients mit einer bestimmten Client-ID verbinden können.

`iot:GetRetainedMessage`

Dies ist die Berechtigung zum Abrufen des Inhalts einer einzelnen beibehaltenen Nachricht. Archivierte Nachrichten sind die Nachrichten, die mit gesetztem RETAIN-Flag veröffentlicht und von gespeichert wurden AWS IoT Core. Informationen zur Berechtigung zum Abrufen einer Liste aller beibehaltenen Nachrichten des Kontos finden Sie unter `iot:ListRetainedMessages`.

`iot:ListRetainedMessages`

Dies ist die Berechtigung, zusammenfassende Informationen über die beibehaltenen Nachrichten des Kontos abzurufen, nicht jedoch den Inhalt der Nachrichten. Archivierte Nachrichten sind

Nachrichten, die mit gesetztem RETAIN-Flag veröffentlicht und von gespeichert wurden AWS IoT Core. Der für diese Aktion angegebene Ressourcen-ARN muss * lauten. Informationen zur Berechtigung zum Abrufen des Inhalts einer einzelnen beibehaltenen Nachricht finden Sie unter `iot:GetRetainedMessage`.

`iot:Publish`

Dies ist die Berechtigung zum Veröffentlichen unter einem MQTT-Topic. Diese Berechtigung wird jedes Mal geprüft, wenn eine PUBLISH-Anforderung an den Broker gesendet wird. Sie können es verwenden, um Clients Nachrichten unter bestimmten Topic-Mustern veröffentlichen zu lassen.

> **Note**
>
> Um die Berechtigung `iot:Publish` zu erteilen, müssen Sie auch die Berechtigung `iot:Connect` erteilen.

`iot:Receive`

Stellt die Berechtigung dar, eine Nachricht von zu empfangen AWS IoT Core. Die `iot:Receive`-Berechtigung wird jedes Mal geprüft, wenn eine Nachricht an einen Client zugestellt wird. Da diese Berechtigung bei jedem Zustellvorgang geprüft wird, können Sie sie nutzen, um Clients, die zurzeit ein Topic abonnieren, Berechtigungen zu entziehen.

`iot:RetainPublish`

Dies ist die Berechtigung, eine MQTT-Nachricht mit gesetztem RETAIN-Flag zu veröffentlichen.

> **Note**
>
> Um die Berechtigung `iot:RetainPublish` zu erteilen, müssen Sie auch die Berechtigung `iot:Publish` erteilen.

`iot:Subscribe`

Dies ist die Berechtigung zum Abonnieren eines Topic-Filters. Diese Berechtigung wird jedes Mal geprüft, wenn eine SUBSCRIBE-Anforderung an den Broker gesendet wird. Verwenden Sie sie, um Clients das Abonnieren von Topics zu ermöglichen, die bestimmten Topic-Mustern entsprechen.

> **Note**
>
> Um die Berechtigung `iot:Subscribe` zu erteilen, müssen Sie auch die Berechtigung `iot:Connect` erteilen.

Aktionen für Geräteschattenrichtlinien

`iot:DeleteThingShadow`

Dies ist die Berechtigung zum Löschen des Geräteschattens eines Objekts. Die Berechtigung `iot:DeleteThingShadow` wird bei jeder Anforderung zum Löschen des Geräteschatteninhalts eines Objekts geprüft.

`iot:GetThingShadow`

Dies ist die Berechtigung zum Abrufen des Geräteschattens eines Objekts. Die Berechtigung `iot:GetThingShadow` wird bei jeder Anforderung zum Abrufen des Geräteschatteninhalts eines Objekts geprüft.

`iot:ListNamedShadowsForThing`

Dies ist die Berechtigung zum Auflisten der benannten Schatten eines Objekts. Die Berechtigung `iot:ListNamedShadowsForThing` wird bei jeder Anforderung zum Auflisten der benannten Schatten eines Objekts geprüft.

`iot:UpdateThingShadow`

Dies ist die Berechtigung zum Aktualisieren eines Device Shadow. Die Berechtigung `iot:UpdateThingShadow` wird bei jeder Anforderung zum Aktualisieren des Geräteschatteninhalts eines Objekts geprüft.

> **Note**
>
> Der Richtlinienaktionen für die Auftragsausführung gilt nur für den HTTP-TLS-Endpunkt. Wenn Sie den MQTT-Endpunkt verwenden, müssen Sie die in diesem Thema definierten MQTT-Richtlinienaktionen verwenden.
> Ein Beispiel für eine Richtlinie zur Auftragsausführung, die dies veranschaulicht, finden Sie unter the section called “Beispiel für grundlegende Auftragsrichtlinie”, das mit dem MQTT-Protokoll funktioniert.

AWS IoT Core Politische Maßnahmen zur Ausführung von Job

`iotjobsdata:DescribeJobExecution`

Stellt die Berechtigung für den Abruf einer Auftragsausführung für ein bestimmtes Objekt dar. Die `iotjobsdata:DescribeJobExecution`-Berechtigung wird jedes Mal überprüft, wenn eine Anforderung zur Ausführung eines Auftrags gestellt wird.

`iotjobsdata:GetPendingJobExecutions`

Stellt die Berechtigung zum Abrufen der Liste der Aufträge dar, die sich nicht in einem Endstatus für ein Objekt befinden. Die Berechtigung `iotjobsdata:GetPendingJobExecutions` wird jedes Mal überprüft, wenn eine Anforderung zum Abrufen der Liste gestellt wird.

`iotjobsdata:UpdateJobExecution`

Stellt die Berechtigung zum Aktualisieren einer Auftragsausführung dar. Die Berechtigung `iotjobsdata:UpdateJobExecution` wird jedes Mal überprüft, wenn eine Anforderung zum Aktualisieren des Status einer Auftragsausführung gestellt wird.

`iotjobsdata:StartNextPendingJobExecution`

Stellt die Berechtigung zum Abrufen und Starten der nächsten ausstehenden Auftragsausführung für ein Objekt dar. (Um eine Auftragsausführung mit dem Status QUEUED auf IN_PROGRESS zu aktualisieren.) Die Berechtigung `iotjobsdata:StartNextPendingJobExecution` wird jedes Mal überprüft, wenn eine Anforderung zum Starten der nächsten ausstehenden Auftragsausführung gestellt wird.

AWS IoT Core Richtlinienaktion des Anmeldeinformationsanbieters

`iot:AssumeRoleWithCertificate`

Stellt die Berechtigung dar, den AWS IoT Core Anmeldeinformationsanbieter anzurufen, um eine IAM-Rolle mit zertifikatsbasierter Authentifizierung zu übernehmen. Die `iot:AssumeRoleWithCertificate` Berechtigung wird jedes Mal überprüft, wenn eine Anfrage an den AWS IoT Core Anmeldeinformationsanbieter gestellt wird, eine Rolle zu übernehmen.

## AWS IoT Core Ressourcen für Aktionen

Um eine Ressource für eine AWS IoT Core Richtlinienaktion anzugeben, verwenden Sie den Amazon-Ressourcennamen (ARN) der Ressource. Alle Ressourcen ARNs folgen dem folgenden Format:

```
arn:partition:iot:region:AWS-account-ID:Resource-type/Resource-name
```

Die folgende Tabelle zeigt die Ressource, die für jeden Aktionstyp angegeben werden muss. Die ARN-Beispiele beziehen sich auf die Konto-ID `123456789012`, in der Partition `aws` und sind regionsspezifisch `us-east-1`. Weitere Informationen zu den Formaten für ARNs finden Sie unter Amazon Resource Names (ARNs) im AWS Identity and Access Management Benutzerhandbuch.

| Aktion | Ressourcentyp | Ressourcenname | ARN-Beispiel |
|---|---|---|---|
| `iot:Connect` | `client` | Die Client-ID des Clients | `arn:aws:iot:us-east-1:123456789012:client/myClientId` |
| `iot:DeleteThingShadow` | `thing` | Der Name des Objekts und gegebenenfalls der Name des Schattens | `arn:aws:iot:us-east-1:123456789012:thing/thingOne arn:aws:iot:us-east-1:123456789012:thing/thingOne/shadowOne` |
| `iotjobsdata:DescribeJobExecution` | `thing` | Der Name des Objekts | `arn:aws:iot:us-east-1:123456789012:thing/thingOne` |
| `iotjobsdata:GetPendingJobExecutions` | `thing` | Der Name des Objekts | `arn:aws:iot:us-east-1:123456789012:thing/thingOne` |

| Aktion | Ressourcentyp | Ressourcenname | ARN-Beispiel |
|---|---|---|---|
| iot:GetRetainedMessage | topic | Ein beibehaltenes Nachrichten-Topic | arn:aws:iot:us-east-1:123456789012:topic/myTopicName |
| iot:GetThingShadow | thing | Der Name des Objekts und gegebenenfalls der Name des Schattens | arn:aws:iot:us-east-1:123456789012:thing/thingOne arn:aws:iot:us-east-1:123456789012:thing/thingOne/shadowOne |
| iot:ListNamedShadowsForThing | Alle | Alle | * |
| iot:ListRetainedMessages | Alle | Alle | * |
| iot:Publish | topic | Eine Topic-Zeichenfolge | arn:aws:iot:us-east-1:123456789012:topic/myTopicName |
| iot:Receive | topic | Eine Topic-Zeichenfolge | arn:aws:iot:us-east-1:123456789012:topic/myTopicName |
| iot:RetainPublish | topic | Ein Topic, das mit gesetztem RETAIN-Flag veröffentlicht werden soll | arn:aws:iot:us-east-1:123456789012:topic/myTopicName |
| iotjobsdata:StartNextPendingJobExecution | thing | Der Name des Objekts | arn:aws:iot:us-east-1:123456789012:thing/thingOne |

| Aktion | Ressou ntyp | Ressourcenname | ARN-Beispiel |
| --- | --- | --- | --- |
| `iot:Subsc ribe` | `topic1 er` | Eine Zeichenfolge für einen Topic-Filter | `arn:aws:iot:us-eas t-1:123456789012:t opicfilter/myTopic Filter` |
| `iotjobsda ta:Update JobExecut ion` | `thing` | Der Name des Objekts | `arn:aws:iot:us-eas t-1:123456789012:thing/ thingOne` |
| `iot:Updat eThingSha dow` | `thing` | Der Name des Objekts und gegebenenfalls der Name des Schattens | `arn:aws:iot:us-eas t-1:123456789012:thing/ thingOne arn:aws:iot:us- east-1:123456789012:t hing/thingOne/shadowOne` |
| `iot:Assum eRoleWith Certificate` | `rolea1` | Das Rollenalias, das auf einen Rollen-ARN verweist | `arn:aws:iot:us-eas t-1:123456789012:r olealias/Credentia lProviderRole_alias` |

## AWS IoT Core Richtlinienvariablen

AWS IoT Core definiert Richtlinienvariablen, die in AWS IoT Core Richtlinien im `Condition` Block `Resource` oder verwendet werden können. Bei Anwendung der Richtlinien werden die Variablen durch tatsächliche Werte ersetzt. Wenn beispielsweise ein Gerät mit der Client-ID 100-234-3456 mit dem AWS IoT Core Message Broker verbunden ist, wird die `iot:ClientId` Richtlinienvariable im Richtliniendokument durch 100-234-3456 ersetzt.

AWS IoT Core Richtlinien können Platzhalterzeichen verwenden und folgen einer ähnlichen Konvention wie IAM-Richtlinien. Ein in die Zeichenfolge eingefügtes * (Sternchen) kann als Platzhalter behandelt werden, der mit beliebigen Zeichen übereinstimmt. Sie können beispielsweise * verwenden, um mehrere MQTT-Topic-Namen im `Resource`-Attribut einer Richtlinie zu beschreiben. Die Zeichen + und # werden in einer Richtlinie als Literalzeichenfolgen behandelt. Ein Beispiel für

eine Richtlinie, die die Verwendung von Platzhaltern veranschaulicht, finden Sie unter Verwenden von Platzhalterzeichen in MQTT und AWS IoT Core -Richtlinien.

Sie können auch vordefinierte Richtlinienvariablen mit festen Werten verwenden, um Zeichen darzustellen, die andernfalls eine besondere Bedeutung haben. Zu diesen Sonderzeichen gehören `$(*)`, `$(?)` und `$($)`. Weitere Informationen zu Richtlinienvariablen und Sonderzeichen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags und Erstellen einer Bedingung mit mehreren Schlüsseln oder Werten.

Themen

- Grundlegende Richtlinienvariablen AWS IoT Core
- Objektrichtlinienvariablen
- AWS IoT Core X.509-Zertifikatsrichtlinienvariablen

## Grundlegende Richtlinienvariablen AWS IoT Core

AWS IoT Core definiert die folgenden grundlegenden Richtlinienvariablen:

- `aws:SourceIp`: Die IP-Adresse des Clients, der mit dem AWS IoT Core Message Broker verbunden ist.
- `iot:ClientId`: Die Client-ID für die Verbindung zum AWS IoT Core Message Broker.
- `iot:DomainName`: Der Domainname des Clients, mit dem eine Verbindung hergestellt wurde AWS IoT Core.

Beispiele

- Beispiele für ClientId und SourceIp Richtlinienvariablen
- Beispiele für iot:DomainName Richtlinienvariablen

### Beispiele für **`ClientId`** und **`SourceIp`** Richtlinienvariablen

Die folgende AWS IoT Core Richtlinie zeigt eine Richtlinie, die Richtlinienvariablen verwendet. `aws:SourceIp`kann im Condition-Element Ihrer Richtlinie verwendet werden, um es Prinzipalen zu ermöglichen, API-Anfragen nur innerhalb eines bestimmten Adressbereichs zu stellen. Beispiele finden Sie unter Autorisieren von Benutzern und Cloud-Services zur Nutzung von AWS IoT -Aufträgen.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/clientid1"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Publish"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topic/my/topic/${iot:ClientId}"
   ],
   "Condition": {
    "IpAddress": {
     "aws:SourceIp": "123.45.167.89"
    }
   }
  }
 ]
}
```

In diesen Beispielen `${iot:ClientId}` wird bei der Auswertung der Richtlinie durch die ID des Clients ersetzt, der mit dem AWS IoT Core Message Broker verbunden ist. Wenn Sie Richtlinienvariablen wie beispielsweise `${iot:ClientId}` verwenden, können Sie versehentlich den Zugriff auf Themen ermöglichen. Wenn Sie beispielsweise eine Richtlinie nutzen, in der mit `${iot:ClientId}` ein bestimmter Topic-Filter angegeben wird:

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

```
 ]
}
```

... kann ein Client mit der Client-ID + eine Verbindung zum &IoT; Message Broker herstellen. Damit könnte der Benutzer jedes Thema abonnieren, das dem Themenfilter `my/+/topic` entspricht. Um sich vor solchen Sicherheitslücken zu schützen, verwenden Sie die `iot:Connect` Richtlinienaktion, um zu kontrollieren, welcher Client eine Verbindung herstellen IDs kann. Mit dieser Richtlinie zum Beispiel dürfen nur die Clients mit der Client-ID `clientid1` eine Verbindung herstellen:

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

> **Note**
>
> Die Verwendung der Richtlinienvariable `${iot:ClientId}` mit `Connect` wird nicht empfohlen. Der `ClientId`-Wert wird nicht überprüft, sodass eine Anfügung mit einer anderen Client-ID die Validierung zwar bestehen, aber einen Verbindungsabbruch verursachen kann. Da jede `ClientId` erlaubt ist, können mit einer zufälligen Client-ID die Richtlinien für Objektgruppen umgangen werden.

### Beispiele für **`iot:DomainName`** Richtlinienvariablen

Sie können die `iot:DomainName` Richtlinienvariable hinzufügen, um einzuschränken, welche Domänen verwendet werden dürfen. Durch das Hinzufügen der `iot:DomainName` Richtlinienvariablen können Geräte nur eine Verbindung zu bestimmten konfigurierten Endpunkten herstellen.

Die folgende Richtlinie ermöglicht es Geräten, eine Verbindung mit der angegebenen Domäne herzustellen.

```
{
 "Version": "2012-10-17",
 "Statement": {
  "Sid": "AllowConnectionsToSpecifiedDomain",
  "Effect": "Allow",
  "Action": [
   "iot:Connect"
  ],
  "Resource": "arn:aws:iot:us-east-1:123456789012:client/clientid",
  "Condition": {
   "StringEquals": {
    "iot:DomainName": "d1234567890abcdefghij-ats.iot.us-east-1.amazonaws.com"
   }
  }
 }
}
```

Die folgende Richtlinie verweigert Geräten die Verbindung mit der angegebenen Domäne.

```
{
 "Version": "2012-10-17",
 "Statement": {
  "Sid": "DenyConnectionsToSpecifiedDomain",
  "Effect": "Deny",
  "Action": [
   "iot:Connect"
  ],
  "Resource": "arn:aws:iot:us-east-1:123456789012:client/clientid",
  "Condition": {
   "StringEquals": {
    "iot:DomainName": "d1234567890abcdefghij-ats.iot.us-east-1.amazonaws.com"
   }
  }
 }
}
```

Weitere Informationen zum Bedingungsoperator für Richtlinien finden Sie unter IAM-JSON-Richtlinienelemente: Bedingungsoperatoren. Weitere Informationen zu Domänenkonfigurationen finden Sie unter Was ist eine Domänenkonfiguration? .

### Objektrichtlinienvariablen

Mithilfe von Dingrichtlinienvariablen können Sie AWS IoT Core Richtlinien schreiben, die Berechtigungen auf der Grundlage von Dingeigenschaften wie Dingnamen, Dingtypen und Dingattributwerten gewähren oder verweigern. Sie können Ding-Richtlinienvariablen verwenden, um dieselbe Richtlinie auf die Steuerung vieler AWS IoT Core Geräte anzuwenden. Weitere Informationen zur Gerätebereitstellung finden Sie unter Gerätebereitstellung.

Wenn Sie eine nicht ausschließliche Zuordnung von Dingen verwenden, kann dasselbe Zertifikat an mehrere Dinge angehängt werden. Um eine klare Zuordnung aufrechtzuerhalten und mögliche Konflikte zu vermeiden, müssen Sie Ihre Client-ID mit dem Namen des Dings abgleichen. In diesem Fall erhalten Sie den Namen des Dings aus der Client-ID in der `Connect` MQTT-Nachricht, die gesendet wird, wenn ein Ding eine Verbindung AWS IoT Core herstellt.

Beachten Sie Folgendes, wenn Sie Objektrichtlinienvariablen in AWS IoT Core -Richtlinien verwenden.

- Verwenden Sie die AttachThingPrincipalAPI, um Zertifikate oder Principals (authentifizierte Amazon Cognito Cognito-Identitäten) an eine Sache anzuhängen.
- Wenn eine nicht ausschließliche Ding-Assoziation vorhanden ist und Sie Ding-Namen durch Ding-Richtlinienvariablen ersetzen, muss der Wert von `clientId` in der MQTT-Verbindungsnachricht oder der TLS-Verbindung exakt mit dem Ding-Namen übereinstimmen.

Folgende Thing-Richtlinienvariablen stehen zur Verfügung:

- `iot:Connection.Thing.ThingName`

  Dies ergibt den Namen der Sache in der AWS IoT Core Registrierung, für die die Richtlinie ausgewertet wird. AWS IoT Core verwendet das Zertifikat, das das Gerät bei der Authentifizierung vorlegt, um zu ermitteln, welches Objekt zur Überprüfung der Verbindung verwendet werden soll. Diese Richtlinienvariable ist nur verfügbar, wenn ein Gerät eine Verbindung über MQTT oder MQTT über das Protokoll herstellt. WebSocket
- `iot:Connection.Thing.ThingTypeName`

  Dies wird in den Objekttyp aufgelöst, auf das die Richtlinie angewendet wurde. Die Client-ID der WebSocket MQTT/-Verbindung muss mit dem Namen der Sache identisch sein. Diese Richtlinienvariable ist nur verfügbar, wenn eine Verbindung über MQTT oder MQTT über das Protokoll hergestellt wird. WebSocket

- `iot:Connection.Thing.Attributes[`*`attributeName`*`]`

  Dies wird in den Wert des angegebenen Attributs aufgelöst, das mit dem Thing verknüpft ist, auf das die Richtlinie angewendet wurde. Ein Thing kann bis zu 50 Attribute aufweisen. Jedes Attribut ist als Richtlinienvariable verfügbar: `iot:Connection.Thing.Attributes[`*`attributeName`*`]` wo *`attributeName`* ist der Name des Attributs. Die Client-ID der MQTT/WebSocket Verbindung muss mit dem Namen des Dings identisch sein. Diese Richtlinienvariable ist nur verfügbar, wenn eine Verbindung über MQTT oder MQTT über das WebSocket Protokoll hergestellt wird.

- `iot:Connection.Thing.IsAttached`

  `iot:Connection.Thing.IsAttached: ["true"]`erzwingt, dass nur die Geräte, die sowohl im AWS IoT Principal registriert als auch mit diesem verbunden sind, auf die in der Richtlinie enthaltenen Berechtigungen zugreifen können. Sie können diese Variable verwenden, um zu verhindern, dass ein Gerät eine Verbindung herstellt, AWS IoT Core wenn es ein Zertifikat vorlegt, das nicht an ein IoT-Ding in der AWS IoT Core Registrierung angehängt ist. Diese Variable hat Werte `true` oder `false` gibt an, dass das verbindende Ding über die API an das Zertifikat oder die Amazon Cognito Cognito-Identität in der Registrierung angehängt ist. AttachThingPrincipal Der Objektname wird als Client-ID verwendet.

Wenn Ihre Client-ID mit Ihrem Ding-Namen übereinstimmt oder wenn Sie Ihr Zertifikat ausschließlich an eine Sache anhängen, kann die Verwendung von Richtlinienvariablen in der Richtliniendefinition die Richtlinienverwaltung vereinfachen. Anstatt individuelle Richtlinien für jedes IoT-Ding zu erstellen, können Sie mithilfe der Ding-Richtlinienvariablen eine einzelne Richtlinie definieren. Diese Richtlinie kann dynamisch auf alle Geräte angewendet werden. Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die zeigt, wie sie funktioniert. Weitere Informationen finden Sie unter ???.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Condition": {
    "StringLike": {
     "iot:ClientId": "*${iot:Connection.Thing.Attributes[envType]}"
    }
   },
   "Effect": "Allow",
   "Action": "iot:Connect",
   "Resource": "arn:aws:iot:us-east-1:123456789012:client/*"
  }
```

```
  ]
}
```

In diesem Richtlinienbeispiel können Dinge eine Verbindung herstellen, AWS IoT Core wenn ihre Client-ID mit dem Wert ihres `envType` Attributs endet. Nur Dinge mit einem passenden Client-ID-Muster dürfen eine Verbindung herstellen.

### AWS IoT Core X.509-Zertifikatsrichtlinienvariablen

X.509-Zertifikatsrichtlinienvariablen helfen beim Schreiben AWS IoT Core von Richtlinien. Diese Richtlinien gewähren Berechtigungen auf der Grundlage von X.509-Zertifikatsattributen. In den folgenden Abschnitten wird beschrieben, wie diese Zertifikatsrichtlinienvariablen verwendet werden.

> **Important**
>
> Wenn Ihr X.509-Zertifikat kein bestimmtes Zertifikatattribut enthält, aber die entsprechende Zertifikatsrichtlinienvariable in Ihrem Richtliniendokument verwendet wird, kann die Richtlinienbewertung zu unerwartetem Verhalten führen.

#### CertificateId

In der RegisterCertificateAPI `certificateId` erscheint das im Antworttext. Um Informationen zu Ihrem Zertifikat zu erhalten, verwenden Sie das `certificateId` in DescribeCertificate.

#### Ausstellerattribute

Die folgenden AWS IoT Core Richtlinienvariablen unterstützen das Zulassen oder Verweigern von Berechtigungen auf der Grundlage von Zertifikatsattributen, die vom Zertifikataussteller festgelegt wurden.

- `iot:Certificate.Issuer.DistinguishedNameQualifier`
- `iot:Certificate.Issuer.Country`
- `iot:Certificate.Issuer.Organization`
- `iot:Certificate.Issuer.OrganizationalUnit`
- `iot:Certificate.Issuer.State`
- `iot:Certificate.Issuer.CommonName`
- `iot:Certificate.Issuer.SerialNumber`

- `iot:Certificate.Issuer.Title`
- `iot:Certificate.Issuer.Surname`
- `iot:Certificate.Issuer.GivenName`
- `iot:Certificate.Issuer.Initials`
- `iot:Certificate.Issuer.Pseudonym`
- `iot:Certificate.Issuer.GenerationQualifier`

Subject-Attribute

Die folgenden AWS IoT Core Richtlinienvariablen unterstützen das Erteilen oder Verweigern von Berechtigungen auf der Grundlage der vom Zertifikatsaussteller festgelegten Attributen des Zertifikatsinhabers.

- `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-Zertifikate bieten diesen Attributen die Möglichkeit, einen oder mehrere Werte zu enthalten. Standardmäßig wird bei Attributen mit mehreren Werten der erste Wert zurückgegeben. So kann beispielsweise das Attribut `Certificate.Subject.Country` eine Liste von Ländernamen enthalten, aber wenn es in einer Richtlinie ausgewertet wird, wird `iot:Certificate.Subject.Country` durch den ersten Ländernamen ersetzt.

Einen spezifischen Attributwert, der nicht dem ersten Wert entspricht, können Sie unter Verwendung eines 1-basierten Indexes anfordern. `iot:Certificate.Subject.Country.1` wird z. B. durch den zweiten Ländernamen im Attribut `Certificate.Subject.Country` ersetzt. Wenn Sie einen Index angeben, der nicht vorhanden ist (wenn Sie zum Beispiel einen dritten Wert anfordern, obwohl dem Attribut nur zwei Werte zugeordnet sind), findet keine Ersetzung statt und die Autorisierung schlägt fehl. Sie können das Suffix `.List` verwenden, um alle Werte des Attributs anzugeben.

Attribute des alternativen Ausstellernamens

Die folgenden AWS IoT Core Richtlinienvariablen unterstützen die Erteilung oder Verweigerung von Berechtigungen auf der Grundlage von Attributen mit alternativen Namen des Ausstellers, die vom Zertifikataussteller festgelegt wurden.

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

Attribute des alternativen Subjektnamens

Die folgenden AWS IoT Core Richtlinienvariablen unterstützen die Erteilung oder Verweigerung von Berechtigungen auf der Grundlage von Attributen mit alternativen Namen, die vom Zertifikataussteller festgelegt wurden.

- `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`

Weitere Attribute

Sie können sie verwenden`iot:Certificate.SerialNumber`, um den Zugriff auf AWS IoT Core Ressourcen auf der Grundlage der Seriennummer eines Zertifikats zu erlauben oder zu verweigern. Die Richtlinienvariable `iot:Certificate.AvailableKeys` enthält die Namen aller Zertifikat-Richtlinienvariablen, die Werte enthalten.

## Verwenden von X.509-Zertifikatsrichtlinienvariablen

Dieses Thema enthält Einzelheiten zur Verwendung von Zertifikatsrichtlinienvariablen. X.509-Zertifikatsrichtlinienvariablen sind wichtig, wenn Sie AWS IoT Core Richtlinien erstellen, die Berechtigungen auf der Grundlage von X.509-Zertifikatattributen gewähren. Wenn Ihr X.509-Zertifikat kein bestimmtes Zertifikatattribut enthält, aber die entsprechende Zertifikatsrichtlinienvariable in Ihrem Richtliniendokument verwendet wird, kann die Richtlinienbewertung zu unerwartetem Verhalten führen. Dies liegt daran, dass die fehlende Richtlinienvariable in der Richtlinienerklärung nicht bewertet wird.

In diesem Thema:


- Beispiel für ein X.509-Zertifikat
- Verwendung von Zertifikatsausstellerattributen als Zertifikatsrichtlinienvariablen
- Verwendung von Zertifikatsantragsattributen als Variablen für die Zertifikatsrichtlinie
- Verwendung von alternativen Namensattributen des Zertifikatausstellers als Variablen für die Zertifikatsrichtlinie
- Verwendung von Attributen mit alternativen Namen für den Antragsteller des Zertifikats als Variablen für die Zertifikatsrichtlinie
- Verwendung eines anderen Zertifikatsattributs als Zertifikatsrichtlinienvariable
- Einschränkungen bei Richtlinienvariablen für X.509-Zertifikate
- Beispielrichtlinien, die Zertifikatsrichtlinienvariablen verwenden


### Beispiel für ein X.509-Zertifikat

Ein typisches X.509-Zertifikat könnte wie folgt aussehen. Dieses Beispielzertifikat enthält Zertifikatattribute. Bei der Bewertung von AWS IoT Core Richtlinien werden die folgenden Zertifikatsattribute als Zertifikatsrichtlinienvariablen aufgefüllt: `Serial Number`,`Issuer`,`Subject`,`X509v3 Issuer Alternative Name`, und`X509v3 Subject Alternative Name`.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            92:12:85:cb:b7:a5:e0:86
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=IoT Devices, OU=SmartHome, ST=WA, CN=IoT Devices Primary CA,
```

```
    GN=Primary CA1/initials=XY/dnQualifier=Example corp,
    SN=SmartHome/ title=CA1/pseudonym=Primary_CA/generationQualifier=2/serialNumber=987

        Validity
            Not Before: Mar 26 03:25:40 2024 GMT
            Not After : Apr 28 03:25:40 2025 GMT
        Subject: C=US, O=IoT Devices, OU=LightBulb, ST=NY, CN=LightBulb Device Cert,
    GN=Bulb/initials=ZZ/dnQualifier=Bulb001,
    SN=Multi Color/title=RGB/pseudonym=RGB Device/generationQualifier=4/
serialNumber=123
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    << REDACTED >>
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Subject Alternative Name:
                DNS:example.com, IP Address:1.2.3.4, URI:ResourceIdentifier001,
 email:device1@example.com, DirName:/C=US/O=IoT/OU=SmartHome/CN=LightBulbCert
            X509v3 Issuer Alternative Name:
                DNS:issuer.com, IP Address:5.6.7.8, URI:PrimarySignerCA,
 email:primary@issuer.com, DirName:/C=US/O=Issuer/OU=IoT Devices/CN=Primary Issuer CA
    Signature Algorithm: sha256WithRSAEncryption
         << REDACTED >>
```

Verwendung von Zertifikatsausstellerattributen als Zertifikatsrichtlinienvariablen

Die folgende Tabelle enthält Einzelheiten dazu, wie die Attribute des Zertifikatsausstellers in einer AWS IoT Core Richtlinie aufgefüllt werden.

Ausstellerattribute, die in einer Richtlinie ausgefüllt werden sollen

| Attribute des Zertifikatsausstellers | Variablen für die Zertifikatsrichtlinie |
| --- | --- |
| • C=US<br>• o=IoT-Geräte | • `iot:Certificate.Issuer.Country = US`<br>• `iot:Certificate.Issuer.Organization = IoT Devices` |

| Attribute des Zertifikatsausstellers | Variablen für die Zertifikatsrichtlinie |
| --- | --- |
| • OU= SmartHome<br>• ST=WA<br>• CN=Primäre CA für IoT-Geräte<br>• GN=Primär CA1<br>• Initialen=XY<br>• dnqualifier=Beispiel Corp<br>• SN= SmartHome<br>• Titel= CA1<br>• Pseudonym=Primary_CA<br>• Qualifikator für die Generierung = 2<br>• Seriennummer = 987 | • `iot:Certificate.Issuer.OrganizationalUnit = SmartHome`<br>• `iot:Certificate.Issuer.State = WA`<br>• `iot:Certificate.Issuer.CommonName = IoT Devices Primary CA`<br>• `iot:Certificate.Issuer.GivenName = Primary CA1`<br>• `iot:Certificate.Issuer.initials = XY`<br>• `iot:Certificate.Issuer.Distinguished NameQualifier = Example corp`<br>• `iot:Certificate.Issuer.Surname = SmartHome`<br>• `iot:Certificate.Issuer.Title = CA1`<br>• `iot:Certificate.Issuer.Pseudonym = Primary_CA`<br>• `iot:Certificate.Issuer.GenerationQualifier = 2`<br>• `iot:Certificate.Issuer.SerialNumber = 987` |

Verwendung von Zertifikatsantragsattributen als Variablen für die Zertifikatsrichtlinie

Die folgende Tabelle enthält Einzelheiten dazu, wie die Attribute des Zertifikatssubjekts in einer AWS IoT Core Richtlinie aufgefüllt werden.

Betreff-Attribute, die in einer Richtlinie ausgefüllt werden sollen

| Betreff-Attribute des Zertifikats | Variablen für die Zertifikatsrichtlinie |
| --- | --- |
| • C=US<br>• o=IoT-Geräte<br>• ST=NY<br>• CN= Gerätezertifikat LightBulb | • `iot:Certificate.Subject.Country = US`<br>• `iot:Certificate.Subject.Organization = IoT Devices`<br>• `iot:Certificate.Subject.State = NY` |

| Betreff-Attribute des Zertifikats | Variablen für die Zertifikatsrichtlinie |
| --- | --- |
| • GN=Glühbirne<br>• Initialen=ZZ<br>• DNQualifier = BULB001<br>• sn=Mehrfarbig<br>• Titel=RGB<br>• Pseudonym=RGB-Gerät<br>• Qualifier für die Generierung = 4<br>• Seriennummer = 123 | • `iot:Certificate.Subject.CommonName = LightBulb Device Cert`<br>• `iot:Certificate.Subject.GivenName = Bulb`<br>• `iot:Certificate.Subject.initials = ZZ`<br>• `iot:Certificate.Subject.DistinguishedNameQualifier = Bulb001`<br>• `iot:Certificate.Subject.Surname = Multi Color`<br>• `iot:Certificate.Subject.Title = RGB`<br>• `iot:Certificate.Subject.Pseudonym = RGB Device`<br>• `iot:Certificate.Subject.GenerationQualifier = 4`<br>• `iot:Certificate.Subject.SerialNumber = 123` |

Verwendung von alternativen Namensattributen des Zertifikatausstellers als Variablen für die Zertifikatsrichtlinie

Die folgende Tabelle enthält Einzelheiten darüber, wie alternative Namensattribute von Zertifikatsausstellern in eine AWS IoT Core Richtlinie eingefügt werden.

Attribute für alternative Namen des Ausstellers, die in eine Richtlinie eingetragen werden sollen

| Alternativer Name des X509v3-Emittenten | Attribut in einer Richtlinie |
| --- | --- |
| • DNS: Issuer.com<br>• IP-Adresse: 5.6.7.8<br>• URI: CA PrimarySigner<br>• E-Mail: primary@issuer.com<br>• DirName: /C= US/O=Issuer/OU=IoT Devices/CN =Primäre Emittentin CA | • `iot:Certificate.Issuer.AlternativeName.DNSName = issuer.com`<br>• `iot:Certificate.Issuer.AlternativeName.IPAddress = 5.6.7.8`<br>• `iot:Certificate.Issuer.AlternativeName.UniformResourceIdentifier = PrimarySignerCA` |

| Alternativer Name des X509v3-Emittenten | Attribut in einer Richtlinie |
| --- | --- |
| | • `iot:Certificate.Issuer.AlternativeName.RFC822Name = primary@issuer.com`<br>• `iot:Certificate.Issuer.AlternativeName.DirectoryName = cn=Primary Issuer CA,ou=IoT Devices,o=Issuer,c=US` |

Verwendung von Attributen mit alternativen Namen für den Antragsteller des Zertifikats als Variablen für die Zertifikatsrichtlinie

Die folgende Tabelle enthält Einzelheiten dazu, wie die Attribute für alternative Namen von Zertifikatsempfängern in einer AWS IoT Core Richtlinie aufgefüllt werden.

Attribute mit alternativen Namen für Antragsteller, die in einer Richtlinie ausgefüllt werden sollen

| X509v3 Alternativer Name des Betreffs | Attribut in einer Richtlinie |
| --- | --- |
| • DNS: example.com<br>• IP-Adresse: 1.2.3.4<br>• URI: 001 ResourceIdentifier<br>• E-Mail: device1@example.com<br>• DirName: /C= = US/O=IoT/OU=SmartHome/CN LightBulbCert | • `iot:Certificate.Subject.AlternativeName.DNSName = example.com`<br>• `iot:Certificate.Subject.AlternativeName.IPAddress = 1.2.3.4`<br>• `iot:Certificate.Subject.AlternativeName.UniformResourceIdentifier = ResourceIdentifier001`<br>• `iot:Certificate.Subject.AlternativeName.RFC822Name = device1@example.com`<br>• `iot:Certificate.Subject.AlternativeName.DirectoryName = cn=LightBulbCert,ou=SmartHome,o=IoT,c=US` |

Verwendung eines anderen Zertifikatsattributs als Zertifikatsrichtlinienvariable

Die folgende Tabelle enthält Einzelheiten dazu, wie andere Zertifikatsattribute in eine AWS IoT Core Richtlinie aufgenommen werden.

Andere Attribute, die in einer Richtlinie aufgefüllt werden sollen

| Anderes Zertifikatsattribut | Richtlinienvariable für Zertifikate |
| --- | --- |
| `Serial Number: 92:12:85:cb:b7:a5:e0:86` | `iot:Certificate.SerialNumber = 105256223 89124227206` |

Einschränkungen bei Richtlinienvariablen für X.509-Zertifikate

Folgende Einschränkungen gelten bei den Richtlinienvariablen für X.509-Zertifikate:

Fehlende Richtlinienvariablen

Wenn Ihr X.509-Zertifikat kein bestimmtes Zertifikatattribut enthält, aber die entsprechende Zertifikatsrichtlinienvariable in Ihrem Richtliniendokument verwendet wird, kann die Richtlinienbewertung zu unerwartetem Verhalten führen. Dies liegt daran, dass die fehlende Richtlinienvariable in der Richtlinienerklärung nicht bewertet wird.

SerialNumber Format des Zertifikats

AWS IoT Core behandelt die Seriennummer des Zertifikats als Zeichenkettendarstellung einer dezimalen Ganzzahl. Wenn eine Richtlinie beispielsweise nur Verbindungen zulässt, deren Client-ID mit der Seriennummer des Zertifikats übereinstimmt, muss die Client-ID die Seriennummer im Dezimalformat sein.

Platzhalter

Wenn Platzhalterzeichen in Zertifikatattributen vorhanden sind, wird die Richtlinienvariable nicht durch den Wert des Zertifikatsattributs ersetzt. Dadurch bleibt der `${policy-variable}` Text im Richtliniendokument erhalten. Dies kann zu einem Autorisierungsfehler führen. Die folgenden Platzhalterzeichen können verwendet werden: `*`, `$`, `+`, `?` und `#`.

Array-Felder

Arrays in Zertifikatattributen sind auf fünf Elemente beschränkt. Zusätzliche Elemente werden ignoriert.

Länge der Zeichenfolge

Alle Zeichenfolgenwerte sind auf maximal 1.024 Zeichen beschränkt. Wenn ein Zertifikatsattribut eine Zeichenfolge enthält, die länger als 1024 Zeichen ist, wird die Richtlinienvariable nicht durch den Wert des Zertifikatsattributs ersetzt. Dadurch bleibt das `${policy-variable}` im Richtliniendokument. Dies kann zu einem Autorisierungsfehler führen.

Sonderzeichen

Jedem Sonderzeichen, wie `,`, `'`, `\`, `+`, `=`, `<`, `>` und `;`, muss ein umgekehrter Schrägstrich (`\`) vorangestellt werden, wenn es in einer Richtlinienvariablen verwendet wird. Beispielsweise wird `Amazon Web Services O=Amazon.com Inc. L=Seattle ST=Washington C=US` zu `Amazon Web Service O\=Amazon.com Inc. L\=Seattle ST\=Washington C\=US`.

Beispielrichtlinien, die Zertifikatsrichtlinienvariablen verwenden

Das folgende Richtliniendokument ermöglicht Verbindungen mit einer Client-ID, die der Seriennummer des Zertifikats entspricht, und das Veröffentlichen zu dem Thema, das dem Muster entspricht:`${iot:Certificate.Subject.Organization}/device-stats/${iot:ClientId}/*`.

**Important**

Wenn Ihr X.509-Zertifikat kein bestimmtes Zertifikatattribut enthält, aber die entsprechende Zertifikatsrichtlinienvariable in Ihrem Richtliniendokument verwendet wird, kann die Richtlinienbewertung zu unerwartetem Verhalten führen. Dies liegt daran, dass die fehlende Richtlinienvariable in der Richtlinienerklärung nicht bewertet wird. Wenn Sie beispielsweise das folgende Richtliniendokument an ein Zertifikat anhängen, das das `iot:Certificate.Subject.Organization` Attribut nicht enthält, werden die `iot:Certificate.Subject.Organization` Zertifikatsrichtlinienvariablen bei der Richtlinienbewertung nicht aufgefüllt.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
```

```
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/${iot:Certificate.SerialNumber}"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Publish"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topic/${iot:Certificate.Subject.Organization}/
device-stats/${iot:ClientId}/*"
   ]
  }
 ]
}
```

Sie können auch den Bedingungsoperator Null verwenden, um sicherzustellen, dass die in einer Richtlinie verwendeten Zertifikatsrichtlinienvariablen bei der Richtlinienbewertung aufgefüllt werden. Im folgenden Richtliniendokument sind Zertifikate nur `iot:Connect` zulässig, wenn die Attribute Certificate Serial Number und Certificate Subject Common Name vorhanden sind.

Alle Variablen der Zertifikatsrichtlinie haben Zeichenkettenwerte, sodass alle Bedingungsoperatoren vom Typ „Zeichenfolge“ unterstützt werden.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/*"
   ],
   "Condition": {
    "Null": {
     "iot:Certificate.SerialNumber": "false",
     "iot:Certificate.Subject.CommonName": "false"
    }
```

```
    }
   }
  ]
}
```

## Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine Entität, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine Entität mit größeren Rechten zwingen kann, die Aktion auszuführen. In kann AWS ein dienstübergreifender Identitätswechsel zum Problem des verwirrten Stellvertreters führen. Ein serviceübergreifender Identitätswechsel kann auftreten, wenn ein Service (der Anruf-Service) einen anderen Service anruft (den aufgerufenen Service). Der Anruf-Service kann so manipuliert werden, dass er seine Berechtigungen verwendet, um auf die Ressourcen eines anderen Kunden zu reagieren, auf die er sonst nicht zugreifen dürfte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Um die Berechtigungen einzuschränken, die AWS IoT der Ressource einen anderen Dienst gewähren, empfehlen wir die Verwendung der Kontextschlüssel `aws:SourceArn`und der `aws:SourceAccount`globalen Bedingungsschlüssel in Ressourcenrichtlinien. Wenn Sie beide globalen Bedingungskontextschlüssel verwenden, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienanweisung verwendet werden.

Der effektivste Weg, um sich vor dem Verwirrter-Stellvertreter-Problem zu schützen, ist die Verwendung des `aws:SourceArn` globalen Bedingungskontextschlüssels mit dem vollständigen Amazon-Ressourcenname (ARN) der Ressource. Für AWS IoT`aws:SourceArn` müssen Sie das Format einhalten: `arn:aws:iot:region:account-id:resource-type/resource-id` für ressourcenspezifische Berechtigungen oder`arn:aws:iot:region:account-id:*`. Bei der Ressourcen-ID kann es sich um den Namen oder die ID der zugelassenen Ressource oder um eine Platzhalterangabe der zulässigen Ressource handeln. IDs Stellen Sie sicher, dass das *`region`* mit Ihrer AWS IoT Region und das mit Ihrer *`account-id`* Kundenkonto-ID übereinstimmt.

Das folgende Beispiel zeigt, wie Sie das Problem mit dem verwirrten Stellvertreter verhindern können, indem Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globale Bedingung in der AWS IoT Rollenvertrauensrichtlinie verwenden. Weitere Beispiele finden Sie unter Ausführliche Beispiele für die Prävention verwirrter Stellvertreter.

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"iot.amazonaws.com"
         },
         "Action":"sts:AssumeRole",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":"123456789012"
            },
            "ArnLike":{
               "aws:SourceArn":"arn:aws:iot:us-east-1:123456789012:*"
            }
         }
      }
   ]
}
```

> **Note**
>
> Wenn Sie die Fehlermeldung „Zugriff verweigert“ erhalten, kann dies daran liegen, dass die Dienstintegration mit AWS Security Token Service (STS) die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` Kontextschlüssel nicht unterstützt.

### Ausführliche Beispiele für die Prävention verwirrter Stellvertreter

Dieser Abschnitt enthält ausführliche Beispiele dafür, wie das Problem der verwirrten Stellvertreter verhindert werden kann, indem die Kontextschlüssel aws:SourceArn und die aws:SourceAccount globalen Bedingungsschlüssel in der AWS IoT Rollenvertrauensrichtlinie verwendet werden.

- Flottenbereitstellung
- JITP
- Anbieter von Anmeldeinformationen

#### Flottenbereitstellung

Sie können die Flottenbereitstellung mithilfe einer Provisioning-Vorlagenressource konfigurieren. Wenn eine Bereitstellungsvorlage auf eine Bereitstellungsrolle verweist, kann die Vertrauensrichtlinie

dieser Rolle die Bedingungsschlüssel und die `aws:SourceArn` Bedingungsschlüssel enthalten. `aws:SourceAccount` Diese Schlüssel begrenzen die Ressourcen, für die die Konfiguration die Anforderung aufrufen kann. `sts:AssumeRole`

Die Rolle mit der folgenden Vertrauensrichtlinie kann nur vom IoT-Prinzipal (`iot.amazonaws.com`) für die in der `SourceArn` angegebene Bereitstellungsvorlage übernommen werden.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"iot.amazonaws.com"
         },
         "Action":"sts:AssumeRole",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":"123456789012"
            },
            "ArnLike":{
               "aws:SourceArn":"arn:aws:iot:us-
east-1:123456789012:provisioningtemplate/example_template"
            }
         }
      }
   ]
}
```

JITP

Bei der just-in-time Bereitstellung (JITP) können Sie entweder die Bereitstellungsvorlage als separate Ressource von der CA verwenden oder den Vorlagentext und die Rolle als Teil der CA-Zertifikatskonfiguration definieren. Der Wert von `aws:SourceArn` in der AWS IoT Rollenvertrauensrichtlinie hängt davon ab, wie Sie die Bereitstellungsvorlage definieren.

Definieren Sie die Bereitstellungsvorlage als separate Ressource

Wenn Sie Ihre Bereitstellungsvorlage als separate Ressource definieren, `aws:SourceArn` kann der Wert von sein. "`arn:aws:iot:region:account-id:provisioningtemplate/example_template`" Sie können dasselbe Richtlinienbeispiel in Flottenbereitstellung verwenden.

Definieren einer Bereitstellungsvorlage in einem CA-Zertifikat

Wenn Sie Ihre Bereitstellungsvorlage innerhalb einer CA-Zertifikatsressource definieren, `aws:SourceArn` kann der Wert von oder sein`"arn:aws:iot:region:account-id:cacert/cert_id"`. `"arn:aws:iot:region:account-id:cacert/*"` Sie können einen Platzhalter verwenden, wenn die Ressourcenkennung, z. B. die ID eines CA-Zertifikats, zum Zeitpunkt der Erstellung unbekannt ist.

Die Rolle mit der folgenden Vertrauensrichtlinie kann nur vom IoT-Prinzipal (`iot.amazonaws.com`) für das in der angegebene CA-Zertifikat übernommen werden`SourceArn`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"iot.amazonaws.com"
         },
         "Action":"sts:AssumeRole",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":"123456789012"
            },
            "ArnLike":{
               "aws:SourceArn":"arn:aws:iot:us-
east-1:123456789012:cacert/
8ecde6884f3d87b1125ba31ac3fcb13d7016de7f57cc904fe1cb97c6ae98196e"
            }
         }
      }
   ]
}
```

Beim Erstellen eines CA-Zertifikats können Sie in der Registrierungskonfiguration auf eine Bereitstellungsrolle verweisen. Die Vertrauensrichtlinie der Bereitstellungsrolle kann verwendet werden`aws:SourceArn`, um einzuschränken, für welche Ressourcen die Rolle verwendet werden kann. Beim ersten CACertificateRegister-Aufruf zur Registrierung des CA-Zertifikats müssten Sie jedoch nicht den ARN des CA-Zertifikats in der `aws:SourceArn` Bedingung angeben.

Um dieses Problem zu umgehen, d. h. um die Vertrauensrichtlinie der Bereitstellungsrolle für das spezifische CA-Zertifikat anzugeben, mit dem registriert ist AWS IoT Core, können Sie wie folgt vorgehen:

- Rufen Sie zunächst Register auf, CACertificate ohne den `RegistrationConfig` Parameter anzugeben.
- Nachdem das CA-Zertifikat bei registriert wurde AWS IoT Core, rufen Sie Update CACertificate auf.

  Geben Sie im CACertificate Aktualisierungsaufruf eine `RegistrationConfig` an, die die Vertrauensrichtlinie für die Bereitstellungsrolle enthält und auf den ARN des neu registrierten CA-Zertifikats `aws:SourceArn` festgelegt ist.

Anbieter von Anmeldeinformationen

Verwenden Sie für AWS IoT Core Credential Provider dasselbe, das AWS-Konto Sie zum Erstellen des Rollenalias in verwenden`aws:SourceAccount`, und geben Sie eine Anweisung an, die dem Ressourcen-ARN des Rolealias-Ressourcentyps in entspricht. `aws:SourceArn` Wenn Sie eine IAM-Rolle für die Verwendung mit dem AWS IoT Core Anmeldeinformationsanbieter erstellen, müssen Sie alle Rollenaliase, die möglicherweise die Rolle übernehmen müssen, in die `aws:SourceArn` ARNs Bedingung aufnehmen, um so die dienstübergreifende Anfrage zu autorisieren. `sts:AssumeRole`

Die Rolle mit der folgenden Vertrauensrichtlinie kann nur vom Principal von AWS IoT Core Credential Provider (`credentials.iot.amazonaws.com`) für den in der angegebenen roleAlias übernommen werden. `SourceArn` Wenn ein Principal versucht, Anmeldeinformationen für einen anderen Rollenalias als den in der `aws:SourceArn` Bedingung angegebenen abzurufen, wird die Anfrage abgelehnt, auch wenn dieser andere Rollenalias auf dieselbe IAM-Rolle verweist.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "credentials.iot.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
```

```
        "ArnLike": {
          "aws:SourceArn": "arn:aws:iot:us-
east-1:123456789012:rolealias/example_rolealias"
        }
      }
    }
  ]
}
```

## AWS IoT Core Beispiele für Richtlinien

Die Beispielrichtlinien in diesem Abschnitt veranschaulichen die Richtliniendokumente, die zur Ausführung allgemeiner Aufgaben in AWS IoT Core verwendet werden. Sie können sie als Beispiele verwenden, um darauf aufbauend mit der Erstellung der Richtlinien für Ihre Lösungen zu beginnen.

Für die Beispiele in diesem Abschnitt werden die folgenden Richtlinienelemente verwendet:

- the section called “AWS IoT Core politische Maßnahmen”
- the section called “AWS IoT Core Ressourcen für Aktionen”
- the section called “Beispiele für identitätsbasierte Richtlinien”
- the section called “Grundlegende Richtlinienvariablen AWS IoT Core”
- the section called “AWS IoT Core X.509-Zertifikatsrichtlinienvariablen”

Richtlinienbeispiele in diesem Abschnitt:

- Beispiel für die Verbinden-Richtlinie
- Beispiele für Veröffentlichungs-/Abonnement-Richtlinien
- Beispiele zu den Verbinden- und Veröffentlichen-Richtlinien
- Beispielrichtlinien für beibehaltene Nachrichten
- Beispiele für die Zertifikatrichtlinie
- Beispiel für Objektrichtlinien
- Beispiel für grundlegende Auftragsrichtlinie

### Beispiel für die Verbinden-Richtlinie

Die folgende Richtlinie verweigert dem Client IDs `client1` und dem Herstellen einer `client2` Verbindung die Erlaubnis AWS IoT Core, Geräte können jedoch über eine Client-ID eine Verbindung

herstellen. Die Client-ID entspricht dem Namen einer Sache, die in der AWS IoT Core Registrierung registriert und dem Prinzipal zugeordnet ist, der für die Verbindung verwendet wird:

> **Note**
>
> Für registrierte Geräte empfehlen wir, Objektrichtlinienvariablen für `Connect`-Aktionen zu verwenden und das Objekt an den Prinzipal anzuhängen, der für die Verbindung verwendet wird.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Deny",
   "Action": [
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/client1",
    "arn:aws:iot:us-east-1:123456789012:client/client2"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/${iot:Connection.Thing.ThingName}"
   ],
   "Condition": {
    "Bool": {
     "iot:Connection.Thing.IsAttached": "true"
    }
   }
  }
 ]
}
```

Die folgende Richtlinie erteilt die Erlaubnis, eine Verbindung AWS IoT Core mit der Client-ID herzustellen`client1`. Dieses Richtlinienbeispiel bezieht sich auf nicht registrierte Geräte.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/client1"
   ]
  }
 ]
}
```

Richtlinienbeispiele für persistente MQTT-Sitzungen

`connectAttributes` ermöglichen es Ihnen, in Ihren IAM-Richtlinien `PersistentConnect` und `LastWill` anzugeben, welche Attribute Sie in Ihrer Connect-Meldung verwenden möchten. Weitere Informationen finden Sie unter ConnectAttributes verwenden.

Die folgende Richtlinie ermöglicht, eine Verbindung mit dem `PersistentConnect`-Feature herzustellen:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": "arn:aws:iot:us-east-1:123456789012:client/client1",
   "Condition": {
    "ForAllValues:StringEquals": {
     "iot:ConnectAttributes": [
      "PersistentConnect"
     ]
    }
```

```
    }
   }
  ]
}
```

Die folgende Richtlinie untersagt `PersistentConnect`, andere Features hingegen sind erlaubt:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": "arn:aws:iot:us-east-1:123456789012:client/client1",
   "Condition": {
    "ForAllValues:StringNotEquals": {
     "iot:ConnectAttributes": [
      "PersistentConnect"
     ]
    }
   }
  }
 ]
}
```

Die oben genannte Richtlinie kann auch mit `StringEquals` ausgedrückt werden, sodass alle anderen Features, einschließlich neuer Features, zulässig sind:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": "arn:aws:iot:us-east-1:123456789012:client/client1",
  },
  {
   "Effect": "Deny",
   "Action": [
```

```
    "iot:Connect"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "iot:ConnectAttributes": [
      "PersistentConnect"
     ]
    }
   }
  }
 ]
}
```

Die folgende Richtlinie erlaubt das Herstellen einer Verbindung über beide Methoden, `PersistentConnect` und `LastWill`. Alle anderen neue Features sind nicht erlaubt:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": "arn:aws:iot:us-east-1:123456789012:client/client1",
   "Condition": {
    "ForAllValues:StringEquals": {
     "iot:ConnectAttributes": [
      "PersistentConnect",
      "LastWill"
     ]
    }
   }
  }
 ]
}
```

Die folgende Richtlinie ermöglicht eine nahtlose Verbindung von Clients mit oder ohne `LastWill`. Andere anderen Features sind nicht zulässig:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": "arn:aws:iot:us-east-1:123456789012:client/client1",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "iot:ConnectAttributes": [
                        "LastWill"
                    ]
                }
            }
        }
    ]
}
```

Die folgende Richtlinie erlaubt nur Verbindungen unter Verwendung von Standardfeatures:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": "arn:aws:iot:us-east-1:123456789012:client/client1",
   "Condition": {
    "ForAllValues:StringEquals": {
     "iot:ConnectAttributes": []
    }
   }
  }
 ]
}
```

Die folgende Richtlinie erlaubt nur die Verbindung mit `PersistentConnect`. Jedes neue Feature ist zulässig, solange die Verbindung `PersistentConnect` verwendet:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": "arn:aws:iot:us-east-1:123456789012:client/client1",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "iot:ConnectAttributes": [
                        "PersistentConnect"
                    ]
                }
            }
        }
    ]
}
```

Die folgende Richtlinie besagt, dass die Verbindung sowohl `PersistentConnect` als auch `LastWill` verwendet werden muss. Neue Features sind nicht zulässig:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": "arn:aws:iot:us-east-1:123456789012:client/client1",
   "Condition": {
    "ForAllValues:StringEquals": {
     "iot:ConnectAttributes": [
      "PersistentConnect",
      "LastWill"
     ]
    }
   }
  },
  {
   "Effect": "Deny",
   "Action": [
```

```
    "iot:Connect"
   ],
   "Resource": "*",
   "Condition": {
    "ForAllValues:StringEquals": {
     "iot:ConnectAttributes": [
      "PersistentConnect"
     ]
    }
   }
  },
  {
   "Effect": "Deny",
   "Action": [
    "iot:Connect"
   ],
   "Resource": "*",
   "Condition": {
    "ForAllValues:StringEquals": {
     "iot:ConnectAttributes": [
      "LastWill"
     ]
    }
   }
  },
  {
   "Effect": "Deny",
   "Action": [
    "iot:Connect"
   ],
   "Resource": "*",
   "Condition": {
    "ForAllValues:StringEquals": {
     "iot:ConnectAttributes": []
    }
   }
  }
 ]
}
```

Die folgende Richtlinie darf `PersistentConnect` nicht verwenden, kann aber `LastWill` verwenden; alle anderen neuen Features sind nicht erlaubt:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "iot:Connect"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "iot:ConnectAttributes": [
                        "PersistentConnect"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": "arn:aws:iot:us-east-1:123456789012:client/client1",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "iot:ConnectAttributes": [
                        "LastWill"
                    ]
                }
            }
        }
    ]
}
```

Die folgende Richtlinie erlaubt Verbindungen nur für Clients, die einen `LastWill` mit dem Topic `"my/lastwill/topicName"` haben; alle anderen Features sind erlaubt, solange sie das Topic `LastWill` verwenden:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": "arn:aws:iot:us-east-1:123456789012:client/client1",
            "Condition": {
                "ArnEquals": {
                    "iot:LastWillTopic": "arn:aws:iot:region:account-id:topic/my/
lastwill/topicName"
                }
            }
        }
    ]
}
```

Die folgende Richtlinie erlaubt nur die Verbindung mit einem spezifischen `LastWillTopic`; andere Features sind zulässig, solange es das `LastWillTopic` verwendet:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": "arn:aws:iot:us-east-1:123456789012:client/client1",
            "Condition": {
                "ArnEquals": {
                    "iot:LastWillTopic": "arn:aws:iot:region:account-id:topic/my/
lastwill/topicName"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "iot:Connect"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "iot:ConnectAttributes": [
```

```
                    "PersistentConnect"
                ]
            }
        }
    }
]
}
```

Beispiele für Veröffentlichungs-/Abonnement-Richtlinien

Welche Richtlinie Sie verwenden, hängt davon ab, wie Sie eine Verbindung herstellen AWS IoT Core. Sie können eine Verbindung herstellen, AWS IoT Core indem Sie einen MQTT-Client, HTTP oder WebSocket verwenden. Wenn Sie sich über einen MQTT-Client verbinden, nutzen Sie für die Authentifizierung ein X.509-Zertifikat. Wenn Sie eine Verbindung über HTTP oder das WebSocket Protokoll herstellen, authentifizieren Sie sich mit Signature Version 4 und Amazon Cognito.

> **Note**
>
> Für registrierte Geräte empfehlen wir, Objektrichtlinienvariablen für `Connect`-Aktionen zu verwenden und das Objekt an den Prinzipal anzuhängen, der für die Verbindung verwendet wird.

In diesem Abschnitt:

- Verwenden von Platzhalterzeichen in MQTT und AWS IoT Core -Richtlinien
- Richtlinien zum Veröffentlichen, Abonnieren und Empfangen von Nachrichten zu to/from bestimmten Themen
- Richtlinien zum Veröffentlichen, Abonnieren und Empfangen von Nachrichten, Themen mit einem bestimmten Präfix to/from
- Richtlinien zum Veröffentlichen, Abonnieren und Empfangen von Nachrichten — Themen, die für jedes Gerät spezifisch sind to/from
- Richtlinien zum Veröffentlichen, Abonnieren und Empfangen von Nachrichten — to/from Themen, bei denen das Thing-Attribut im Themennamen enthalten ist
- Richtlinien, um die Veröffentlichung von Nachrichten zu untergeordneten Topics eines Topic-Namens zu verweigern
- Richtlinien, um den Empfang von Nachrichten von untergeordneten Topics eines Topic-Namens zu verweigern

- Richtlinien zum Abonnieren von Topics mit MQTT-Platzhalterzeichen
- Richtlinien für HTTP und Clients WebSocket

Verwenden von Platzhalterzeichen in MQTT und AWS IoT Core -Richtlinien

MQTT und AWS IoT Core Richtlinien haben unterschiedliche Platzhalterzeichen, und Sie sollten sie nach reiflicher Überlegung auswählen. In MQTT # werden die Platzhalterzeichen + und in MQTT-Themenfiltern verwendet, um mehrere Themennamen zu abonnieren. AWS IoT Core Richtlinien verwenden * und ? als Platzhalterzeichen und folgen den Konventionen der IAM-Richtlinien. In einem Richtliniendokument steht * für eine beliebige Kombination von mehreren Zeichen und ein Fragezeichen ? entspricht einem beliebigen einzelnen Zeichen. In Richtliniendokumenten werden die MQTT-Platzhalterzeichen + und # als Zeichen ohne besondere Bedeutung behandelt. Verwenden Sie die Platzhalterzeichen * und ? anstelle der MQTT-Platzhalterzeichen, um mehrere Topic-Namen und -Filter im `resource`-Attribut einer Richtlinie zu beschreiben,

Beachten Sie bei der Auswahl der Platzhalterzeichen für die Verwendung in einem Richtliniendokument, dass das * Zeichen nicht auf eine einzelne Themenebene beschränkt ist. Das + Zeichen ist in einem MQTT-Themenfilter auf eine einzelne Themenebene beschränkt. Ziehen Sie die Verwendung mehrerer ?-Zeichen in Betracht, um eine Platzhalterspezifikation auf eine einzige MQTT-Topic-Filterebene zu beschränken, Weitere Informationen zur Verwendung von Platzhalterzeichen in einer Richtlinienressource und weitere Beispiele für deren Übereinstimmung finden Sie unter Verwenden von Platzhaltern in Ressourcen. ARNs

Die folgende Tabelle zeigt die verschiedenen Platzhalterzeichen, die in MQTT und AWS IoT Core - Richtlinien für MQTT-Clients verwendet werden.

| Platzhalterzeichen | Ist ein MQTT-Platzhalterzeichen | Beispiel in MQTT | Ist ein Platzhalterzeichen AWS IoT Core für Richtlinien | Beispiel für AWS IoT Core Richtlinien für MQTT-Clients |
|---|---|---|---|---|
| # | Ja | `some/#` | Nein | N/A |
| + | Ja | `some/+/topic` | Nein | N/A |

| Platzhalterzeichen | Ist ein MQTT-Platzhalterzeichen | Beispiel in MQTT | Ist ein Platzhalterzeichen AWS IoT Core für Richtlinien | Beispiel für AWS IoT Core Richtlinien für MQTT-Clients |
|---|---|---|---|---|
| * | Nein | N/A | Ja | `topicfilter/some/*/topic`<br><br>`topicfilter/some/sensor*/topic` |
| ? | Nein | N/A | Ja | `topic/some/?????/topic`<br><br>`topicfilter/some/sensor???/topic` |

Richtlinien zum Veröffentlichen, Abonnieren und Empfangen von Nachrichten zu to/from bestimmten Themen

Im Folgenden finden Sie Beispiele für registrierte und nicht registrierte Geräte zum Veröffentlichen, Abonnieren und Empfangen von Nachrichten to/from zum Thema „some_specific_topic“. In diesen Beispielen wird ebenfalls hervorgehiben, dass `Publish` und `Receive` „topic“ als Ressource und `Subscribe` „topicfilter“ als Ressource verwenden.

Registered devices

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte eine Verbindung mit einer clientId herstellen, die dem Namen einer Sache in der Registrierung entspricht. Sie bietet auch `Publish`-, `Subscribe`- und `Receive`-Berechtigungen für das Topic namens „some_specific_topic“.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
```

```
    ],
    "Resource": [
     "arn:aws:iot:us-east-1:123456789012:client/${iot:Connection.Thing.ThingName}"
    ],
    "Condition": {
     "Bool": {
      "iot:Connection.Thing.IsAttached": "true"
     }
    }
   },
   {
    "Effect": "Allow",
    "Action": [
     "iot:Publish"
    ],
    "Resource": [
     "arn:aws:iot:us-east-1:123456789012:topic/some_specific_topic"
    ]
   },
   {
    "Effect": "Allow",
    "Action": [
     "iot:Subscribe"
    ],
    "Resource": [
     "arn:aws:iot:us-east-1:123456789012:topicfilter/some_specific_topic"
    ]
   },
   {
    "Effect": "Allow",
    "Action": [
     "iot:Receive"
    ],
    "Resource": [
     "arn:aws:iot:us-east-1:123456789012:topic/some_specific_topic"
    ]
   }
  ]
}
```

Unregistered devices

Für Geräte, die nicht in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte entweder über ClientID1, ClientID2 oder ClientID3 eine Verbindung

herstellen. Sie bietet auch `Publish`-, `Subscribe`- und `Receive`-Berechtigungen für das Topic namens „some_specific_topic“.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/clientId1",
                "arn:aws:iot:us-east-1:123456789012:client/clientId2",
                "arn:aws:iot:us-east-1:123456789012:client/clientId3"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/some_specific_topic"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topicfilter/some_specific_topic"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Receive"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/some_specific_topic"
            ]
```

```
        }
    ]
}
```

Richtlinien zum Veröffentlichen, Abonnieren und Empfangen von Nachrichten, Themen mit einem bestimmten Präfix to/from

Im Folgenden finden Sie Beispiele für registrierte und nicht registrierte Geräte zum Veröffentlichen, Abonnieren und Empfangen von to/from Nachrichtenthemen mit dem Präfix „topic_prefix“.

> **Note**
>
> Beachten Sie die Verwendung des Platzhalterzeichens in diesem Beispiel. * Es * ist zwar nützlich, Berechtigungen für mehrere Themennamen in einer einzigen Anweisung bereitzustellen, kann jedoch zu unbeabsichtigten Folgen führen, da Geräten mehr Rechte gewährt werden als erforderlich. Wir empfehlen daher, das Platzhalterzeichen nur * nach reiflicher Überlegung zu verwenden.

Registered devices

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte eine Verbindung mit einer clientId herstellen, die dem Namen einer Sache in der Registrierung entspricht. Sie bietet `Publish`-, `Subscribe`- and `Receive`-Berechtigungen für Topics mit dem Präfix „topic_prefix“.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/${iot:Connection.Thing.ThingName}"
   ],
   "Condition": {
    "Bool": {
     "iot:Connection.Thing.IsAttached": "true"
```

```
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Publish",
    "iot:Receive"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topic/topic_prefix*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Subscribe"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topicfilter/topic_prefix*"
   ]
  }
 ]
}
```

Unregistered devices

Für Geräte, die nicht in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte entweder über ClientID1, ClientID2 oder ClientID3 eine Verbindung herstellen. Sie bietet `Publish`-, `Subscribe`- and `Receive`-Berechtigungen für Topics mit dem Präfix „topic_prefix“.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/clientId1",
                "arn:aws:iot:us-east-1:123456789012:client/clientId2",
```

```
                "arn:aws:iot:us-east-1:123456789012:client/clientId3"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish",
                "iot:Receive"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/topic_prefix*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topicfilter/topic_prefix*"
            ]
        }
    ]
}
```

Richtlinien zum Veröffentlichen, Abonnieren und Empfangen von Nachrichten — Themen, die für jedes Gerät spezifisch sind to/from

Im Folgenden finden Sie Beispiele für registrierte und nicht registrierte Geräte zum Veröffentlichen, Abonnieren und Empfangen von Nachrichten to/from , die für das jeweilige Gerät spezifisch sind.

Registered devices

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte eine Verbindung mit einer clientId herstellen, die dem Namen einer Sache in der Registrierung entspricht. Sie berechtigt zum Veröffentlichen von Inhalten zum objektspezifischen Topic (`sensor/device/${iot:Connection.Thing.ThingName}`) sowie zum Abonnieren und Empfangen von Inhalten zum objektspezifischen Topic (`command/device/${iot:Connection.Thing.ThingName}`). Wenn der Name des Objekts in der Registrierung „thing1" lautet, kann das Gerät unter dem Thema" 1" veröffentlichen. sensor/device/thing1". The device will also be able to subscribe to and receive from the topic "command/device/thing

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/${iot:Connection.Thing.ThingName}"
   ],
   "Condition": {
    "Bool": {
     "iot:Connection.Thing.IsAttached": "true"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Publish"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topic/sensor/device/
${iot:Connection.Thing.ThingName}"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Subscribe"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topicfilter/command/device/
${iot:Connection.Thing.ThingName}"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Receive"
   ],
   "Resource": [
```

```
    "arn:aws:iot:us-east-1:123456789012:topic/command/device/
${iot:Connection.Thing.ThingName}"
   ]
  }
 ]
}
```

Unregistered devices

Für Geräte, die nicht in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte entweder über ClientID1, ClientID2 oder ClientID3 eine Verbindung herstellen. Sie berechtigt zum Veröffentlichen von Inhalten zum clientspezifischen Topic (`sensor/device/${iot:ClientId}`) sowie zum Abonnieren und Empfangen von Inhalten zum clientspezifischen Topic (`command/device/${iot:ClientId}`). Wenn das Gerät eine Verbindung mit clientId als ClientID1 herstellt, kann es zum Thema "1" veröffentlichen. sensor/device/clientId Das Gerät kann das Thema auch abonnieren und Inhalte empfangen. `device/clientId1/command`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/clientId1",
                "arn:aws:iot:us-east-1:123456789012:client/clientId2",
                "arn:aws:iot:us-east-1:123456789012:client/clientId3"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/sensor/device/
${iot:Connection.Thing.ThingName}"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "iot:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topicfilter/command/device/
${iot:Connection.Thing.ThingName}"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Receive"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/command/device/
${iot:Connection.Thing.ThingName}"
            ]
        }
    ]
}
```

Richtlinien zum Veröffentlichen, Abonnieren und Empfangen von Nachrichten — to/from Themen, bei denen das Thing-Attribut im Themennamen enthalten ist

Im Folgenden finden Sie ein Beispiel für registrierte Geräte zum Veröffentlichen, Abonnieren und Empfangen von Nachrichten. to/from Themen, deren Namen Ding-Attribute enthalten.

> **Note**
>
> Ding-Attribute existieren nur für Geräte, die in der AWS IoT Core Registrierung registriert sind. Es gibt kein entsprechendes Beispiel für nicht registrierte Geräte.

Registered devices

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte eine Verbindung mit einer clientId herstellen, die dem Namen einer Sache in der Registrierung entspricht. Sie berechtigt zum Veröffentlichen von Inhalten im Topic (`sensor/${iot:Connection.Thing.Attributes[version]}`)

sowie zum Abonnieren und Empfangen von Inhalten zum Topic (`command/${iot:Connection.Thing.Attributes[location]}`), wenn der Name des Topics Objektattribute enthält. Wenn der Name des Objekts in der Registrierung den `version=v1` Wert und hat`location=Seattle`, kann das Gerät Beiträge zum Thema "" sensor/v1", and subscribe to and receive from the topic "command/Seattle veröffentlichen.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/${iot:Connection.Thing.ThingName}"
   ],
   "Condition": {
    "Bool": {
     "iot:Connection.Thing.IsAttached": "true"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Publish"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topic/sensor/
${iot:Connection.Thing.Attributes[version]}"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Subscribe"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topicfilter/command/
${iot:Connection.Thing.Attributes[location]}"
   ]
  },
```

```
  {
   "Effect": "Allow",
   "Action": [
    "iot:Receive"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topic/command/
${iot:Connection.Thing.Attributes[location]}"
   ]
  }
 ]
}
```

Unregistered devices

Da Ding-Attribute nur für Geräte existieren, die in der AWS IoT Core Registrierung registriert sind, gibt es kein entsprechendes Beispiel für nicht registrierte Dinge.

Richtlinien, um die Veröffentlichung von Nachrichten zu untergeordneten Topics eines Topic-Namens zu verweigern

Im Folgenden finden Sie Beispiele für registrierte und nicht registrierte Geräte, mit denen Nachrichten zu allen Topics außer bestimmten untergeordneten Topics veröffentlicht werden können.

Registered devices

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte eine Verbindung mit einer clientId herstellen, die dem Namen einer Sache in der Registrierung entspricht. Sie berechtigt zur Veröffentlichung von Inhalten zu allen Topics mit dem Präfix „department/“, nicht jedoch zum untergeordneten Topic „department/admins“.

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

```
   "Condition": {
    "Bool": {
     "iot:Connection.Thing.IsAttached": "true"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Publish"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topic/department/*"
   ]
  },
  {
   "Effect": "Deny",
   "Action": [
    "iot:Publish"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topic/department/admins"
   ]
  }
 ]
}
```

Unregistered devices

Für Geräte, die nicht in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte entweder über ClientID1, ClientID2 oder ClientID3 eine Verbindung herstellen. Sie berechtigt zur Veröffentlichung von Inhalten zu allen Topics mit dem Präfix „department/“, nicht jedoch zum untergeordneten Topic „department/admins“.

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

```
                "arn:aws:iot:us-east-1:123456789012:client/clientId1",
                "arn:aws:iot:us-east-1:123456789012:client/clientId2",
                "arn:aws:iot:us-east-1:123456789012:client/clientId3"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/department/*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "iot:Publish"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/department/admins"
            ]
        }
    ]
}
```

Richtlinien, um den Empfang von Nachrichten von untergeordneten Topics eines Topic-Namens zu verweigern

Im Folgenden finden Sie Beispiele für registrierte und nicht registrierte Geräte, die Nachrichten von allen Topics mit bestimmten Präfixen außer gewissen untergeordneten Topics abonnieren und empfangen.

Registered devices

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte eine Verbindung mit einer clientId herstellen, die dem Namen einer Sache in der Registrierung entspricht. Die Richtlinie ermöglicht es Geräten, jedes Topic mit dem Präfix „topic_prefix“ zu abonnieren. Durch die Verwendung `NotResource` in der Anweisung for ermöglichen wir dem Gerät`iot:Receive`, Nachrichten zu allen Themen zu empfangen, die das Gerät abonniert hat, mit Ausnahme der Themen mit dem Präfix „topic_“. prefix/restricted". For

example, with this policy, devices can subscribe to "topic_prefix/topic1" and even "topic_prefix/restricted", however, they will only receive messages from the topic "topic_prefix/topic1" and no messages from the topic "topic_prefix/restricted

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/${iot:Connection.Thing.ThingName}"
   ],
   "Condition": {
    "Bool": {
     "iot:Connection.Thing.IsAttached": "true"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "iot:Subscribe",
   "Resource": "arn:aws:iot:us-east-1:123456789012:topicfilter/topic_prefix/*"
  },
  {
   "Effect": "Allow",
   "Action": "iot:Receive",
   "NotResource": "arn:aws:iot:us-east-1:123456789012:topic/topic_prefix/restricted/
*"
  }
 ]
}
```

Unregistered devices

Für Geräte, die nicht in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte entweder über ClientID1, ClientID2 oder ClientID3 eine Verbindung herstellen. Die Richtlinie ermöglicht es Geräten, jedes Topic mit dem Präfix „topic_prefix“ zu abonnieren. Durch die Verwendung `NotResource` in der Anweisung for ermöglichen wir dem Gerät`iot:Receive`, Nachrichten zu allen Themen zu empfangen, die das Gerät abonniert hat,

mit Ausnahme von Themen mit dem Präfix „topic_“. prefix/restricted". For example, with this policy, devices can subscribe to "topic_prefix/topic1" and even "topic_prefix/restricted". However, they will only receive messages from the topic "topic_prefix/topic1" and no messages from the topic "topic_prefix/restricted

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/clientId1",
                "arn:aws:iot:us-east-1:123456789012:client/clientId2",
                "arn:aws:iot:us-east-1:123456789012:client/clientId3"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iot:Subscribe",
            "Resource": "arn:aws:iot:us-east-1:123456789012:topicfilter/
topic_prefix/*"
        },
        {
            "Effect": "Allow",
            "Action": "iot:Receive",
            "NotResource": "arn:aws:iot:us-east-1:123456789012:topic/topic_prefix/
restricted/*"
        }
    ]
}
```

Richtlinien zum Abonnieren von Topics mit MQTT-Platzhalterzeichen

Die MQTT-Platzhalterzeichen + und # werden als Literalzeichenfolgen behandelt, aber sie werden nicht als Platzhalter behandelt, wenn sie in Richtlinien verwendet werden. AWS IoT Core In MQTT werden + und # nur als Platzhalter behandelt, wenn ein Topic-Filter abonniert wird. In anderen Zusammenhängen werden sie als wörtliche Zeichenfolge gehandhabt. Wir empfehlen, diese MQTT-Platzhalter nur nach sorgfältiger Prüfung als Teil von Richtlinien zu verwenden. AWS IoT Core

Im Folgenden finden Sie Beispiele für registrierte und nicht registrierte Dinge, die MQTT-Platzhalter in Richtlinien verwenden. AWS IoT Core Diese Platzhalter werden als Literalzeichenfolgen behandelt.

Registered devices

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte eine Verbindung mit einer clientId herstellen, die dem Namen einer Sache in der Registrierung entspricht. Die Richtlinie ermöglicht es Geräten, die Topics „department/+/employees“ und „location/#“ zu abonnieren. Da + und # in AWS IoT Core Richtlinien als wörtliche Zeichenketten behandelt werden, können Geräte das Thema „Abteilung/+/Mitarbeiter“ abonnieren, aber nicht auch das Thema "". department/engineering/employees". Similarly, devices can subscribe to the topic "location/#" but not to the topic "location/Seattle". However, once the device subscribes to the topic "department/+/employees", the policy will allow them to receive messages from the topic "department/engineering/employees". Similarly, once the device subscribes to the topic "location/#", they will receive messages from the topic "location/Seattle

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/${iot:Connection.Thing.ThingName}"
   ],
   "Condition": {
    "Bool": {
     "iot:Connection.Thing.IsAttached": "true"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "iot:Subscribe",
   "Resource": "arn:aws:iot:us-east-1:123456789012:topicfilter/department/+/
employees"
  },
  {
   "Effect": "Allow",
   "Action": "iot:Subscribe",
```

```
    "Resource": "arn:aws:iot:us-east-1:123456789012:topicfilter/location/#"
   },
   {
    "Effect": "Allow",
    "Action": "iot:Receive",
    "Resource": "arn:aws:iot:us-east-1:123456789012:topic/*"
   }
  ]
}
```

Unregistered devices

Für Geräte, die nicht in der AWS IoT Core Registrierung registriert sind, ermöglicht die folgende Richtlinie, dass Geräte entweder über ClientID1, ClientID2 oder ClientID3 eine Verbindung herstellen. Mit der Richtlinie können Geräte die Topics „department/+/employees“ und „location/#“ abonnieren. Da + und # in AWS IoT Core Richtlinien als wörtliche Zeichenketten behandelt werden, können Geräte das Thema „Abteilung/+/Mitarbeiter“ abonnieren, aber nicht auch das Thema "". department/engineering/employees". Similarly, devices can subscribe to the topic "location/#" but not "location/Seattle". However, once the device subscribes to the topic "department/+/employees", the policy will allow them to receive messages from the topic "department/engineering/employees". Similarly, once the device subscribes to the topic "location/#", they will receive messages from the topic "location/Seattle

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/clientId1",
                "arn:aws:iot:us-east-1:123456789012:client/clientId2",
                "arn:aws:iot:us-east-1:123456789012:client/clientId3"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iot:Subscribe",
            "Resource": "arn:aws:iot:us-east-1:123456789012:topicfilter/department/
+/employees"
```

```
        },
        {
            "Effect": "Allow",
            "Action": "iot:Subscribe",
            "Resource": "arn:aws:iot:us-east-1:123456789012:topicfilter/location/#"
        },
        {
            "Effect": "Allow",
            "Action": "iot:Receive",
            "Resource": "arn:aws:iot:us-east-1:123456789012:topic/*"
        }
    ]
}
```

### Richtlinien für HTTP und Clients WebSocket

Wenn Sie eine Verbindung über HTTP oder das WebSocket Protokoll herstellen, authentifizieren Sie sich mit Signature Version 4 und Amazon Cognito. Amazon-Cognito-Identitäten können authentifiziert oder nicht authentifiziert sein. Authentifizierte Identitäten gehören zu Benutzer, die von einem unterstützten Identitätsanbieter authentifiziert werden. Nicht authentifizierte Identitäten gehören in der Regel Gastbenutzern, die sich nicht bei einem Identitätsanbieter authentifizieren. Amazon Cognito bietet eine eindeutige Kennung und AWS Anmeldeinformationen zur Unterstützung nicht authentifizierter Identitäten. Weitere Informationen finden Sie unter the section called “Autorisierung mit Amazon-Cognito-Identitäten”.

AWS IoT Core Verwendet für die folgenden Operationen AWS IoT Core Richtlinien, die über die API an Amazon Cognito Cognito-Identitäten angehängt sind. `AttachPolicy` Dadurch werden die Berechtigungen, die dem Amazon Cognito Cognito-Identitätspool mit authentifizierten Identitäten zugewiesen sind, eingeschränkt.

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

Das bedeutet, dass eine Amazon Cognito Cognito-Identität die Genehmigung der IAM-Rollenrichtlinie und der AWS IoT Core Richtlinie benötigt. Sie fügen die IAM-Rollenrichtlinie über die API dem Pool und die AWS IoT Core Richtlinie der Amazon Cognito Identity hinzu. AWS IoT Core `AttachPolicy`

Authentifizierte und nicht authentifizierte Benutzer sind unterschiedliche Identitätstypen. Wenn Sie der Amazon Cognito Identity keine AWS IoT Richtlinie beifügen, schlägt ein authentifizierter Benutzer die Autorisierung fehl AWS IoT und hat keinen Zugriff auf AWS IoT Ressourcen und Aktionen.

> **Note**
>
> Bei anderen AWS IoT Core Vorgängen oder bei AWS IoT Core nicht authentifizierten Identitäten werden die mit der Amazon Cognito Cognito-Identitätspool-Rolle verbundenen Berechtigungen nicht eingeschränkt. Dies ist sowohl für authentifizierte als auch für nicht authentifizierte Identitäten die großzügigste Richtlinie, die Sie der Amazon-Cognito-Poolrolle hinzufügen sollten.

HTTP

Um nicht authentifizierten Amazon-Cognito-Identitäten zu ermöglichen, Nachrichten über HTTP zu einem für die Amazon-Cognito-Identität spezifischen Thema zu veröffentlichen, fügen Sie der Amazon-Cognito-Identitätspoolrolle die folgende IAM-Richtlinie an:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish",
            ],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/${cognito-
identity.amazonaws.com:sub}"]
        }
    ]
}
```

Um authentifizierte Benutzer zuzulassen, fügen Sie die obige Richtlinie der Amazon Cognito Identity-Pool-Rolle und der Amazon Cognito Identity mithilfe der API hinzu. AWS IoT Core AttachPolicy

> **Note**
>
> Bei der Autorisierung von Amazon Cognito Cognito-Identitäten werden beide Richtlinien AWS IoT Core berücksichtigt und die geringsten angegebenen Rechte gewährt. Eine Aktion ist nur zulässig, wenn beide Richtlinien die angeforderte Aktion zulassen. Wenn eine Richtlinie eine Aktion verbietet, wird diese Aktion nicht erlaubt.

MQTT

Um nicht authentifizierten Amazon Cognito Cognito-Identitäten die Veröffentlichung von MQTT-Nachrichten zu einem WebSocket Thema zu ermöglichen, das für die Amazon Cognito Cognito-Identität in Ihrem Konto spezifisch ist, fügen Sie der Amazon Cognito Cognito-Identitätspool-Rolle die folgende IAM-Richtlinie hinzu:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/${cognito-
identity.amazonaws.com:sub}"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:client/${cognito-
identity.amazonaws.com:sub}"]
        }
    ]
}
```

Um authentifizierte Benutzer zuzulassen, fügen Sie die obige Richtlinie der Amazon Cognito Identity-Pool-Rolle und der Amazon Cognito Identity mithilfe der API hinzu. AWS IoT Core AttachPolicy

> **Note**
>
> Bei der Autorisierung von Amazon Cognito Cognito-Identitäten werden beide AWS IoT Core berücksichtigt und die geringsten angegebenen Rechte gewährt. Eine Aktion ist nur zulässig, wenn beide Richtlinien die angeforderte Aktion zulassen. Wenn eine Richtlinie eine Aktion verbietet, wird diese Aktion nicht erlaubt.

Beispiele zu den Verbinden- und Veröffentlichen-Richtlinien

Für Geräte, die als Dinge in der AWS IoT Core Registrierung registriert sind, gewährt die folgende Richtlinie die Erlaubnis, eine Verbindung AWS IoT Core mit einer Client-ID herzustellen, die dem Ding-Namen entspricht, und beschränkt das Gerät auf die Veröffentlichung zu einem Client-ID- oder Dingnamen-spezifischen MQTT-Thema. Damit eine Verbindung erfolgreich hergestellt werden kann, muss der Name des Dings in der AWS IoT Core Registrierung registriert und mithilfe einer Identität oder eines Prinzipals authentifiziert werden, der dem Ding zugeordnet ist:

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

Für Geräte, die nicht als Dinge in der AWS IoT Core Registrierung registriert sind, gewährt die folgende Richtlinie die Erlaubnis, eine Verbindung AWS IoT Core mit einer Client-ID herzustellen, `client1` und beschränkt das Gerät auf die Veröffentlichung zu einem clientID-spezifischen MQTT-Thema:

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action":["iot:Publish"],
        "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/${iot:ClientId}"]
      },
      {
        "Effect": "Allow",
        "Action": ["iot:Connect"],
        "Resource": ["arn:aws:iot:us-east-1:123456789012:client/client1"]
      }
    ]
}
```

Beispielrichtlinien für beibehaltene Nachrichten

Die Verwendung beibehaltener Nachrichten erfordert spezielle Richtlinien. Aufbewahrte Nachrichten sind MQTT-Nachrichten, bei denen das RETAIN-Flag gesetzt und von gespeichert wurde. AWS IoT Core Dieser Abschnitt enthält Beispielrichtlinien, die die allgemeine Verwendung von beibehaltenen Nachrichten ermöglichen.

In diesem Abschnitt:

- Richtlinie zum Verbinden und Veröffentlichen von beibehaltenen Nachrichten
- Richtlinie zum Verbinden und Veröffentlichen von beibehaltenen Will-Nachrichten
- Richtlinie zum Auflisten und Abrufen von beibehaltenen Nachrichten

Richtlinie zum Verbinden und Veröffentlichen von beibehaltenen Nachrichten

Damit ein Gerät beibehaltene Nachrichten veröffentlichen kann, muss das Gerät in der Lage sein, eine Verbindung herzustellen, (jede MQTT-Nachricht) zu veröffentlichen und beibehaltene MQTT-Nachrichten zu veröffentlichen. Die folgende Richtlinie gewährt dem Client **`device1`** diese Berechtigungen für das Topic `device/sample/configuration`. Ein weiteres Beispiel für die Berechtigung zum Herstellen einer Verbindung finden Sie unter the section called “Beispiele zu den Verbinden- und Veröffentlichen-Richtlinien”.

```
{
 "Version": "2012-10-17",
```

```
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:Connect"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/device1"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Publish",
    "iot:RetainPublish"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topic/device/sample/configuration"
   ]
  }
 ]
}
```

Richtlinie zum Verbinden und Veröffentlichen von beibehaltenen Will-Nachrichten

Clients können eine Nachricht konfigurieren, die veröffentlicht AWS IoT Core wird, wenn der Client die Verbindung unerwartet trennt. Im MQTT werden solche Nachrichten als Will-Nachrichten bezeichnet. Die Verbindungsberechtigung eines Clients muss um eine zusätzliche Bedingung erweitert werden, damit sie einbezogen werden können.

Das folgende Richtliniendokument gewährt allen Clients die Berechtigung, eine Verbindung herzustellen und eine Will-Nachricht mit dem Topic `will` zu veröffentlichen, die auch von AWS IoT Core beibehalten wird.

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

```
    "arn:aws:iot:us-east-1:123456789012:client/device1"
   ],
   "Condition": {
    "ForAllValues:StringEquals": {
     "iot:ConnectAttributes": [
      "LastWill"
     ]
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "iot:Publish",
    "iot:RetainPublish"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topic/will"
   ]
  }
 ]
}
```

Richtlinie zum Auflisten und Abrufen von beibehaltenen Nachrichten

Services und Anwendungen können auf beibehaltene Nachrichten zugreifen, ohne einen MQTT-Client unterstützen zu müssen, indem sie `ListRetainedMessages` und `GetRetainedMessage` aufrufen. Die Services und Anwendungen, die diese Aktionen aufrufen, müssen mithilfe einer Richtlinie wie dem folgenden Beispiel autorisiert werden.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iot:ListRetainedMessages"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:client/device1"
   ],
  },
  {
```

```
   "Effect": "Allow",
   "Action": [
    "iot:GetRetainedMessage"
   ],
   "Resource": [
    "arn:aws:iot:us-east-1:123456789012:topic/foo"
   ]
  }
 ]
}
```

Beispiele für die Zertifikatrichtlinie

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, gewährt die folgende Richtlinie die Erlaubnis, eine Verbindung AWS IoT Core mit einer Client-ID herzustellen, die einem Ding-Namen entspricht, und zu einem Thema zu veröffentlichen, dessen Name dem `certificateId` des Zertifikats entspricht, mit dem sich das Gerät authentifiziert hat:

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

Für Geräte, die nicht in der AWS IoT Core Registrierung registriert sind, gewährt die folgende Richtlinie die Erlaubnis, eine Verbindung AWS IoT Core mit dem Client herzustellen IDs

`client1client2`, `client3` und zu einem Thema zu veröffentlichen, dessen Name dem `certificateId` des Zertifikats entspricht, mit dem sich das Gerät authentifiziert hat:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/
${iot:CertificateId}"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/client1",
                "arn:aws:iot:us-east-1:123456789012:client/client2",
                "arn:aws:iot:us-east-1:123456789012:client/client3"
            ]
        }
    ]
}
```

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, gewährt die folgende Richtlinie die Erlaubnis, eine Verbindung AWS IoT Core mit einer Client-ID herzustellen, die dem Namen des Dings entspricht, und zu einem Thema zu veröffentlichen, dessen Name dem `CommonName` Feld des Antragstellers des Zertifikats entspricht, mit dem sich das Gerät authentifiziert hat:

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

```
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/
${iot:Certificate.Subject.CommonName}"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:client/
${iot:Connection.Thing.ThingName}"]
        }
    ]
}
```

> **Note**
>
> In diesem Beispiel wird der Subject Common Name des Zertifikats als Topic-ID verwendet, mit der Annahme, dass der Subject Common Name für jedes registrierte Zertifikat eindeutig ist. Wenn die Zertifikate für mehrere Geräte gemeinsam genutzt werden, ist der gemeinsame Betreff-Name für alle Geräte, die dieses Zertifikat gemeinsam nutzen, identisch, sodass Veröffentlichungsrechte für dasselbe Thema von mehreren Geräten aus möglich sind (nicht empfohlen).

Für Geräte, die nicht in der AWS IoT Core Registrierung registriert sind, gewährt die folgende Richtlinie die Erlaubnis, eine Verbindung AWS IoT Core mit dem Client IDs `client1client2`,, `client3` und herzustellen und zu einem Thema zu veröffentlichen, dessen Name dem `CommonName` Feld des Antragstellers des Zertifikats entspricht, mit dem sich das Gerät authentifiziert hat:

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

```
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/client1",
                "arn:aws:iot:us-east-1:123456789012:client/client2",
                "arn:aws:iot:us-east-1:123456789012:client/client3"
            ]
        }
    ]
}
```

> **Note**
>
> In diesem Beispiel wird der Subject Common Name des Zertifikats als Topic-ID verwendet, mit der Annahme, dass der Subject Common Name für jedes registrierte Zertifikat eindeutig ist. Wenn die Zertifikate für mehrere Geräte gemeinsam genutzt werden, ist der gemeinsame Betreff-Name für alle Geräte, die dieses Zertifikat gemeinsam nutzen, identisch, sodass Veröffentlichungsrechte für dasselbe Thema von mehreren Geräten aus möglich sind (nicht empfohlen).

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, gewährt die folgende Richtlinie die Erlaubnis, eine Verbindung AWS IoT Core mit einer Client-ID herzustellen, die dem Namen des Dings entspricht, und zu einem Thema zu veröffentlichen, dessen Name mit einem Präfix versehen ist, `admin/` wenn das `Subject.CommonName.2` Feld für das Zertifikat, das zur Authentifizierung des Geräts verwendet wird, auf gesetzt ist`Administrator`:

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

```
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/admin/*"],
            "Condition": {
                "StringEquals": {
                    "iot:Certificate.Subject.CommonName.2": "Administrator"
                }
            }
        }
    ]
}
```

Für Geräte, die nicht in der AWS IoT Core Registrierung registriert sind, gewährt die folgende Richtlinie die Erlaubnis IDs `client1client2`, eine Verbindung AWS IoT Core mit dem Client herzustellen `client3` und zu einem Thema zu veröffentlichen, dessen Name mit dem Präfix versehen ist, `admin/` wenn das `Subject.CommonName.2` Feld für das Zertifikat, das zur Authentifizierung des Geräts verwendet wird, auf gesetzt ist`Administrator`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/client1",
                "arn:aws:iot:us-east-1:123456789012:client/client2",
                "arn:aws:iot:us-east-1:123456789012:client/client3"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/admin/*"],
            "Condition": {
                "StringEquals": {
                    "iot:Certificate.Subject.CommonName.2": "Administrator"
```

```
                }
            }
        }
    ]
}
```

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, erlaubt die folgende Richtlinie einem Gerät, seinen Ding-Namen für Veröffentlichungen zu einem bestimmten Thema zu verwenden, das aus `admin/` folgenden Optionen besteht`Subject.CommonName`: `ThingName` `Administrator`

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

Für Geräte, die nicht in der AWS IoT Core Registrierung registriert sind, gewährt die folgende Richtlinie die Erlaubnis IDs `client1client2`, eine Verbindung zum Client herzustellen `client3` und zum Thema zu veröffentlichen, `admin` wenn für das Zertifikat, AWS IoT Core mit dem das Gerät authentifiziert wurde, eines der `Subject.CommonName` Felder wie folgt gesetzt ist: `Administrator`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/client1",
                "arn:aws:iot:us-east-1:123456789012:client/client2",
                "arn:aws:iot:us-east-1:123456789012:client/client3"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/admin"],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "iot:Certificate.Subject.CommonName.List": "Administrator"
                }
            }
        }
    ]
}
```

Beispiel für Objektrichtlinien

Die folgende Richtlinie ermöglicht es einem Gerät, eine Verbindung herzustellen, wenn das zur Authentifizierung verwendete Zertifikat an das Objekt angehängt AWS IoT Core ist, für das die Richtlinie geprüft wird:

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

```
                "Bool": {
                    "iot:Connection.Thing.IsAttached": ["true"]
                }
            }
        }
    ]
}
```

Die folgende Richtlinie ermöglicht einem Gerät das Veröffentlichen von Inhalten, wenn das Zertifikat an ein Objekt mit einem bestimmten Objekttyp angehängt ist und das Objekt das Attribut `attributeName` mit dem Wert `attributeValue` hat. Weitere Informationen über Objektrichtlinienvariablen finden Sie unter Objektrichtlinienvariablen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish"
      ],
      "Resource": "arn:aws:iot:us-east-1:123456789012:topic/device/stats",
      "Condition": {
        "StringEquals": {
          "iot:Connection.Thing.Attributes[attributeName]": "attributeValue",
          "iot:Connection.Thing.ThingTypeName": "Thing_Type_Name"
        },
        "Bool": {
          "iot:Connection.Thing.IsAttached": "true"
        }
      }
    }
  ]
}
```

Mit der folgenden Richtlinie kann ein Gerät zu einem Topic veröffentlichen, das mit einem Attribut des Objekts beginnt. Wenn das Gerätezertifikat nicht mit dem Objekt verknüpft ist, wird diese Variable nicht aufgelöst und der Fehler „Zugriff verweigert“ wird angezeigt. Weitere Informationen über Objektrichtlinienvariablen finden Sie unter Objektrichtlinienvariablen.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish"
      ],
      "Resource": "arn:aws:iot:us-east-1:123456789012:topic/
${iot:Connection.Thing.Attributes[attributeName]}/*"
    }
  ]
}
```

Beispiel für grundlegende Auftragsrichtlinie

In diesem Beispiel werden die für ein Auftragsziel erforderlichen Richtlinienanweisungen gezeigt, bei dem es sich um ein einzelnes Gerät handelt, das eine Jobanfrage empfängt und dem AWS IoT den Status der Auftragsausführung mitteilt.

*us-west-2:57EXAMPLE833*Ersetzen Sie es durch Ihr AWS-Region, einen Doppelpunkt (:) und Ihre 12-stellige AWS-Konto Zahl und *uniqueThingName* ersetzen Sie es dann durch den Namen der Ding-Ressource, in der das Gerät steht. AWS IoT

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Connect"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:client/uniqueThingName"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/pubtopic",
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/events/job/*",
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/events/jobExecution/*",
```

```
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/things/uniqueThingName/jobs/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topicfilter/test/dc/subtopic",
        "arn:aws:iot:us-west-2:57EXAMPLE833:topicfilter/$aws/events/jobExecution/*",
        "arn:aws:iot:us-west-2:57EXAMPLE833:topicfilter/$aws/things/uniqueThingName/
jobs/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/subtopic",
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/things/uniqueThingName/jobs/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iotjobsdata:DescribeJobExecution",
        "iotjobsdata:GetPendingJobExecutions",
        "iotjobsdata:StartNextPendingJobExecution",
        "iotjobsdata:UpdateJobExecution"
      ],
      "Resource": [
        "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/things/uniqueThingName"
      ]
    }
  ]
}
```

## Autorisierung mit Amazon-Cognito-Identitäten

Es gibt zwei Arten von Amazon–Cognito-Identitäten: nicht authentifiziert und authentifiziert. Wenn Ihre App nicht authentifizierte Amazon-Cognito-Identitäten unterstützt, wird keine Authentifizierung durchgeführt, sodass Sie nicht wissen, wer der Benutzer:in ist.

Nicht authentifizierte Identitäten: Für nicht authentifizierte Amazon-Cognito-Identitäten gewähren Sie Berechtigungen, indem Sie eine IAM-Rolle an einen nicht authentifizierten Identitätspool anfügen. Wir empfehlen, nur jenen Ressourcen Zugriff gewähren, die Sie für unbekannte Benutzer verfügbar haben möchten.

> **Important**
>
> Für nicht authentifizierte Amazon Cognito Cognito-Benutzer, die eine Verbindung herstellen AWS IoT Core, empfehlen wir, in den IAM-Richtlinien Zugriff auf sehr begrenzte Ressourcen zu gewähren.

Authentifizierte Identitäten: Für authentifizierte Amazon-Cognito-Identitäten müssen Sie Berechtigungen an zwei Stellen angeben:

- Fügen Sie dem authentifizierten Amazon-Cognito-Identitätspool eine IAM-Richtlinie an und
- Hängen Sie der Amazon Cognito Identity (authentifizierter Benutzer) eine AWS IoT Core Richtlinie an.

Richtlinienbeispiele für nicht authentifizierte und authentifizierte Amazon-Cognito-Benutzer, die eine Verbindung zu AWS IoT Core herstellen

Das folgende Beispiel zeigt Berechtigungen sowohl in der IAM-Richtlinie als auch in der IoT-Richtlinie einer Amazon-Cognito-Identität. Der authentifizierte Benutzer möchte zu einem gerätespezifischen Thema veröffentlichen (z. B.). device/DEVICE_ID/status

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/Client_ID"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/device/Device_ID/status"
            ]
        }
    ]
}
```

Das folgende Beispiel zeigt Berechtigungen sowohl in der IAM-Richtlinie einer nicht authentifizierten Amazon-Cognito-Rolle. Der nicht authentifizierte Benutzer möchte Inhalte zu nicht gerätespezifischen Topics veröffentlichen, für die keine Authentifizierung erforderlich ist.

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

```
    ]
}
```

GitHub Beispiele

Die folgenden Beispiel-Webanwendungen GitHub zeigen, wie das Anhängen von Richtlinien an authentifizierte Benutzer in den Benutzeranmelde- und Authentifizierungsprozess integriert werden kann.

- Verwendung der MQTT publish/subscribe React-Webanwendung und AWS AmplifyAWS IoT Device SDK for JavaScript
- MQTT publish/subscribe React-Webanwendung mit AWS AmplifyAWS IoT Device SDK for JavaScript, der und einer Lambda-Funktion

Amplify ist eine Reihe von Tools und Diensten, mit denen Sie Web- und Mobilanwendungen erstellen können, die sich in AWS Dienste integrieren lassen. Weitere Informationen zu Amplify finden Sie in der Amplify-Framework-Dokumentation.

In beiden Beispielen werden die folgenden Schritte ausgeführt.

1. Wenn sich ein/e Benutzer:in für ein Konto anmeldet, erstellt die Anwendung einen Amazon-Cognito-Benutzerpool und eine Identität.
2. Wenn sich ein/e Benutzer:in authentifiziert, erstellt die Anwendung eine Richtlinie und fügt sie der Identität an. Dadurch erhält der/die Benutzer:in Veröffentlichungs- und Abonnementberechtigungen.
3. Der/Die Benutzer:in kann die Anwendung verwenden, um MQTT-Thopics zu veröffentlichen und zu abonnieren.

Im ersten Beispiel wird die `AttachPolicy`-API-Operation direkt in der Authentifizierungsoperation verwendet. Im folgenden Beispiel wird gezeigt, wie dieser API-Aufruf in einer React-Webanwendung implementiert wird, die Amplify und das AWS IoT Device SDK for JavaScript verwendet.

```
function attachPolicy(id, policyName) {
    var Iot = new AWS.Iot({region: AWSConfiguration.region, apiVersion:
 AWSConfiguration.apiVersion, endpoint: AWSConfiguration.endpoint});
    var params = {policyName: policyName, target: id};
```

```
    console.log("Attach IoT Policy: " + policyName + " with cognito identity id: " +
 id);
    Iot.attachPolicy(params, function(err, data) {
         if (err) {
               if (err.code !== 'ResourceAlreadyExistsException') {
                  console.log(err);
               }
          }
         else  {
            console.log("Successfully attached policy with the identity", data);
         }
     });
}
```

Dieser Code erscheint in der AuthDisplay.js-Datei.

Im zweiten Beispiel wird die `AttachPolicy`-API-Operation in einer Lambda-Funktion implementiert. Im folgenden Beispiel wird gezeigt, wie Lambda diesen API-Aufruf verwendet.

```
iot.attachPolicy(params, function(err, data) {
     if (err) {
           if (err.code !== 'ResourceAlreadyExistsException') {
              console.log(err);
              res.json({error: err, url: req.url, body: req.body});
           }
      }
     else  {
        console.log(data);
        res.json({success: 'Create and attach policy call succeed!', url: req.url,
 body: req.body});
     }
 });
```

Dieser Code erscheint in der `iot.GetPolicy`-Funktion in der Datei app.js.

> **Note**
>
> Wenn Sie die Funktion mit AWS Anmeldeinformationen aufrufen, die Sie über Amazon Cognito Identity-Pools erhalten, enthält das Kontextobjekt in Ihrer Lambda-Funktion einen

Wert für. `context.cognito_identity_id` Weitere Informationen finden Sie unter den folgenden Topics.

- AWS Lambda Kontextobjekt in Node.js
- AWS Lambda Kontextobjekt in Python
- AWS Lambda Kontextobjekt in Ruby
- AWS Lambda Kontextobjekt in Java
- AWS Lambda Kontextobjekt in Go
- AWS Lambda Kontextobjekt in C#
- AWS Lambda Kontextobjekt in PowerShell

## Autorisieren von direkten Aufrufen von AWS Diensten mithilfe des AWS IoT Core Credential Providers

Geräte können X.509-Zertifikate verwenden, um AWS IoT Core mithilfe von TLS-Protokollen für die gegenseitige Authentifizierung eine Verbindung herzustellen. Andere AWS Dienste unterstützen keine zertifikatsbasierte Authentifizierung, sie können jedoch mithilfe von AWS Anmeldeinformationen im AWS Signature Version 4-Format aufgerufen werden. Der Signature Version 4-Algorithmus erfordert normalerweise, dass der Anrufer über eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel verfügt. AWS IoT Core verfügt über einen Anbieter für Anmeldeinformationen, mit dem Sie das integrierte X.509-Zertifikat als eindeutige Geräteidentität zur Authentifizierung AWS von Anfragen verwenden können. Damit ist es nicht mehr erforderlich, eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel auf Ihrem Gerät zu speichern.

Der Anmeldeinformationsanbieter authentifiziert ein Anrufer unter Verwendung eines X.509-Zertifikats und stellt ein temporäres Sicherheits-Token mit eingeschränkten Berechtigungen aus. Das Token kann verwendet werden, um jede Anfrage zu signieren und zu authentifizieren. AWS Für diese Art der Authentifizierung Ihrer AWS Anfragen müssen Sie eine AWS Identity and Access Management (IAM-) Rolle erstellen und konfigurieren und der Rolle entsprechende IAM-Richtlinien zuordnen, damit der Anbieter der Anmeldeinformationen die Rolle in Ihrem Namen übernehmen kann. Weitere Informationen zu AWS IoT Core und IAM finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT.

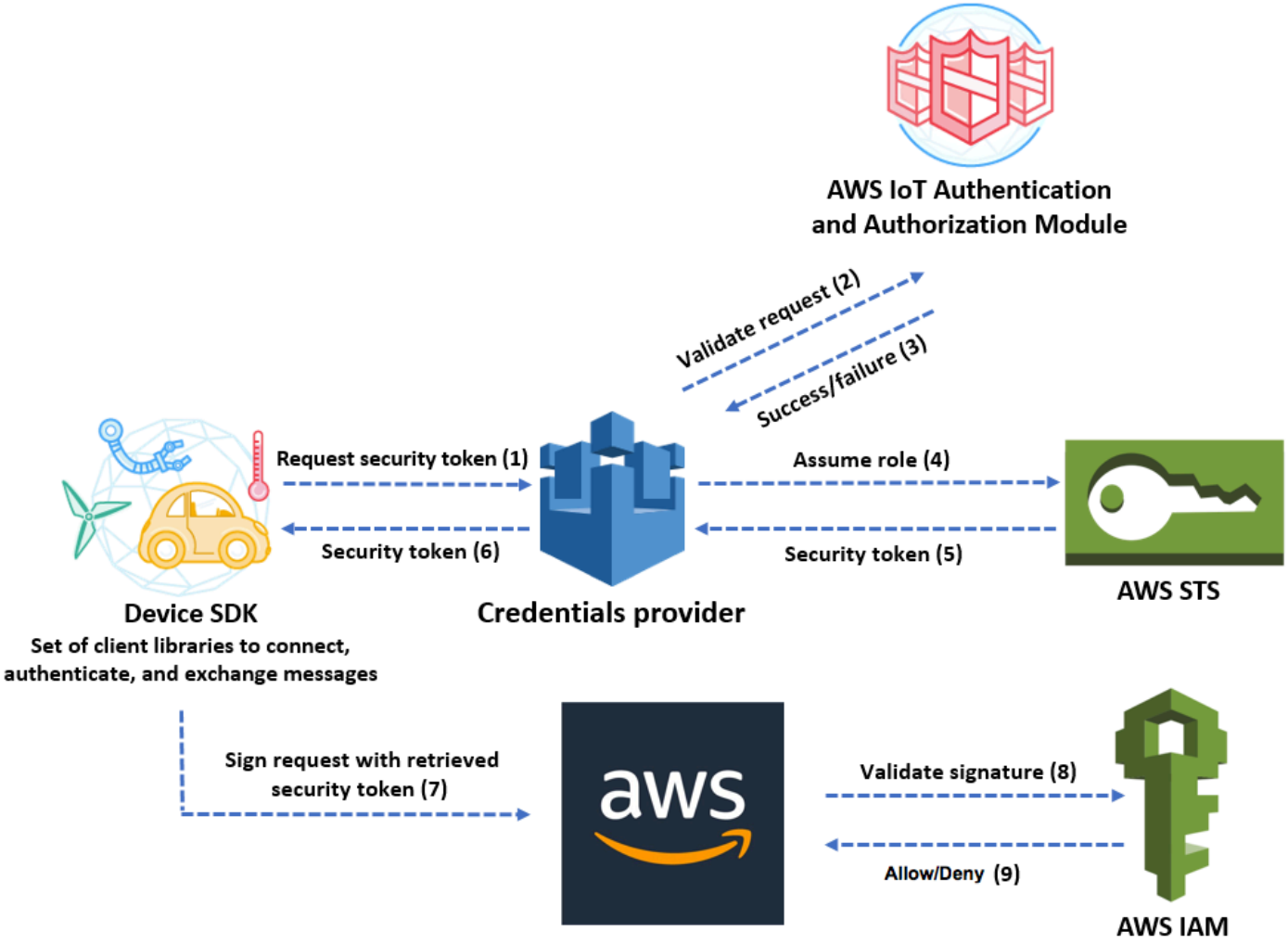
AWS IoT erfordert, dass Geräte die Server Name Indication (SNI) -Erweiterung an das Transport Layer Security (TLS) -Protokoll senden und die vollständige Endpunktadresse vor Ort angeben.

`host_name` Im Feld `host_name`muss der Endpunkt angegeben sein. Dabei muss es sich um Folgendes handeln:

- Die von `aws iot describe-endpoint --endpoint-type iot:CredentialProvider` zurückgegebene `endpointAddress`.

Verbindungsversuche von Geräten ohne den richtigen Wert für `host_name` werden fehlschlagen.

Das folgende Diagramm veranschaulicht den Workflow des Anmeldeinformationsanbieters.




1. Das AWS IoT Core Gerät sendet eine HTTPS-Anfrage an den Anbieter für Anmeldeinformationen nach einem Sicherheitstoken. Die Anfrage enthält das X.509-Zertifikat des Geräts für die Authentifizierung.

2. Der Anbieter für Anmeldeinformationen leitet die Anfrage an das AWS IoT Core Authentifizierungs- und Autorisierungsmodul weiter, um das Zertifikat zu validieren und zu überprüfen, ob das Gerät berechtigt ist, das Sicherheitstoken anzufordern.
3. Wenn das Zertifikat gültig ist und berechtigt ist, ein Sicherheitstoken anzufordern, meldet das AWS IoT Core Authentifizierungs- und Autorisierungsmodul Erfolg. Andernfalls sendet es eine Ausnahme an das Gerät.
4. Nach der erfolgreichen Validierung des Zertifikats ruft der Anmeldeinformationsanbieter AWS Security Token Service (AWS STS) auf, um die IAM-Rolle anzunehmen, die Sie für ihn erstellt haben.
5. AWS STS gibt ein temporäres Sicherheitstoken mit eingeschränkten Rechten an den Anmeldeinformationsanbieter zurück.
6. Der Anmeldeinformationsanbieter gibt das Sicherheits-Token an das Gerät zurück.
7. Das Gerät verwendet das Sicherheitstoken, um eine AWS Anfrage mit AWS Signature Version 4 zu signieren.
8. Der angeforderte Service ruft IAM auf, um die Signatur zu validieren und die Anforderung anhand der Zugriffsrichtlinien zu autorisieren, die der IAM-Rolle zugeordnet sind, die Sie für den Anmeldeinformationsanbieter erstellt haben.
9. Wenn IAM die Signatur erfolgreich validiert und die Anforderung autorisiert, ist die Anforderung erfolgreich. Andernfalls sendet IAM eine Ausnahme.

Im folgenden Abschnitt wird beschrieben, wie Sie ein Zertifikat verwenden, um ein Sicherheits-Token abzurufen. Es ist in der Annahme geschrieben, dass Sie bereits ein Gerät registriert haben und für es ein eigenes Zertifikat erstellt und aktiviert haben.

## So verwenden Sie ein Zertifikat zum Abrufen eines Sicherheits-Tokens

1. Konfigurieren Sie die IAM-Rolle, die der Anmeldeinformationsanbieter im Namen Ihres Geräts annimmt. Fügen Sie der Rolle die folgende Vertrauensrichtlinie hinzu.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {"Service": "credentials.iot.amazonaws.com"},
        "Action": "sts:AssumeRole"
    }
```

```
}
```

Fügen Sie der Rolle für jeden AWS Dienst, den Sie aufrufen möchten, eine Zugriffsrichtlinie hinzu. Der Anmeldeinformationsanbieter unterstützt die folgenden Richtlinienvariablen:

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

Wenn das Gerät den Objektnamen in seiner Anforderung an einen AWS -Service bereitstellt, fügt der Anmeldeinformationsanbieter dem Sicherheits-Token `credentials-iot:ThingName` und `credentials-iot:ThingTypeName` als Kontextvariablen hinzu. Der Anmeldeinformationsanbieter stellt `credentials-iot:AwsCertificateId` als Kontextvariable bereit, auch wenn das Gerät den Dingnamen nicht in der Anfrage angibt. Sie übergeben den Dingnamen als Wert des `x-amzn-iot-thingname` HTTP-Anfrage-Headers.

Diese drei Variablen funktionieren nur für IAM-Richtlinien, nicht für AWS IoT Core -Richtlinien.

2. Stellen Sie sicher, dass der Benutzer, der den nächsten Schritt ausführt (Anlegen eines Rollenalias), die Berechtigung hat, die neu erstellte Rolle an AWS IoT Core zu übergeben. Die folgende Richtlinie gewährt einem AWS Benutzer `iam:GetRole` sowohl `iam:PassRole` Berechtigungen als auch Berechtigungen. Die `iam:GetRole`-Berechtigung ermöglicht es dem Benutzer, Informationen über die Rolle zu abzurufen, die Sie gerade erstellt haben. Die `iam:PassRole` Berechtigung ermöglicht es dem Benutzer, die Rolle an einen anderen AWS Dienst zu übergeben.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iam:GetRole",
            "iam:PassRole"
        ],
        "Resource": "arn:aws:iam::your AWS-Konto id:role/your role name"
    }
}
```

3. Erstellen Sie einen AWS IoT Core Rollenalias. Das Gerät, das direkte Anrufe an AWS Dienste tätigen soll, muss wissen, zu welcher Rolle der ARN für die Verbindung verwendet AWS IoT Core werden soll. Eine Hartcodierung des Rollen-ARN stellt jedoch keine gute Lösung dar, da Sie das Gerät bei jeder Änderung des Rollen-ARN aktualisieren müssten. Eine bessere Lösung ist es, mit der `CreateRoleAlias`-API einen Rollenalias zu erstellen, der auf den Rollen-ARN verweist. Wenn sich der Rollen-ARN ändert, können Sie einfach den Rollenalias aktualisieren. Auf dem Gerät ist keine Änderung erforderlich. Diese API verwendet die folgenden Parameter:

   `roleAlias`

   Erforderlich Eine beliebige Zeichenfolge, die den Rollenalias identifiziert. Sie dient als Primärschlüssel im Rollenalias-Datenmodell. Sie hat 1-128 Zeichen und darf nur alphanumerische Zeichen und die Symbole =, @ und - enthalten. Großbuchstaben und Kleinbuchstaben sind zulässig. Bei Rollenaliasnamen wird zwischen Groß- und Kleinschreibung unterschieden.

   `roleArn`

   Erforderlich Der ARN der Rolle, auf den sich der Rollenalias bezieht.

   `credentialDurationSeconds`

   Optional. Die Gültigkeitsdauer (in Sekunden) der Anmeldeinformationen. Die Mindestwert beträgt 900 Sekunden (15 Minuten). Der Höchstwert beträgt 43.200 Sekunden (12 Stunden). Der Standardwert ist 3.600 Sekunden (1 Stunde).

   > **Important**
   >
   > Der AWS IoT Core Credential Provider kann Anmeldeinformationen mit einer maximalen Lebensdauer von 43.200 Sekunden (12 Stunden) ausstellen. Wenn die Anmeldeinformationen bis zu 12 Stunden gültig sind, kann die Anzahl der Anrufe beim Anmeldeinformationsanbieter reduziert werden, da die Anmeldeinformationen länger zwischengespeichert werden.
   > Der `credentialDurationSeconds`-Wert muss kleiner oder gleich der maximalen Sitzungsdauer der IAM-Rolle sein, auf die der Rollenalias verweist. Weitere Informationen finden Sie unter Ändern der maximalen Sitzungsdauer (AWS API) einer Rolle im AWS Identity and Access Management-Benutzerhandbuch.

   Weitere Informationen über diese API finden Sie unter CreateRoleAlias.

4. Anfügen einer Richtlinie an das Gerätezertifikat. Die an das Gerätezertifikat angefügte Richtlinie muss dem Gerät die Berechtigung erteilen, die Rolle zu übernehmen. Dies erreichen Sie, indem Sie dem Rollenalias die Berechtigung für die Aktion `iot:AssumeRoleWithCertificate` erteilen, wie im folgenden Beispiel gezeigt.

```
{
   "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. Stellen Sie eine HTTPS-Anfrage an den Anmeldeinformationsanbieter, um ein Sicherheits-Token zu erhalten. Geben Sie die folgenden Informationen an:

   - Zertifikat: Da es sich um eine HTTP-Anfrage zur gegenseitigen TLS-Authentifizierung handelt, müssen Sie Ihrem Client bei der Anfrage das Zertifikat und den privaten Schlüssel zur Verfügung stellen. Verwenden Sie dasselbe Zertifikat und denselben privaten Schlüssel, mit dem Sie Ihr Zertifikat registriert haben AWS IoT Core.

     Um sicherzustellen, dass Ihr Gerät mit AWS IoT Core (und nicht mit einem Dienst, der sich als solches ausgibt) kommuniziert, finden Sie weitere Informationen unter Serverauthentifizierung. Folgen Sie den Links, um die entsprechenden CA-Zertifikate herunterzuladen, und kopieren Sie sie dann auf Ihr Gerät.
   - RoleAlias: Der Name des Rollenalias, den Sie für den Anbieter für Anmeldeinformationen erstellt haben. Bei Rollenaliasnamen wird zwischen Groß- und Kleinschreibung unterschieden und sie müssen mit dem Rollenalias übereinstimmen, der in erstellt wurde AWS IoT Core.
   - ThingName: Der Name des Dings, den Sie bei der Registrierung Ihres Dings erstellt AWS IoT Core haben. Dieser wird als Wert des `x-amzn-iot-thingname` HTTP-Headers übergeben. Dieser Wert ist nur erforderlich, wenn Sie Ding-Attribute als Richtlinienvariablen in AWS IoT Core oder IAM-Richtlinien verwenden.

> **Note**
>
> Der Wert ThingName, den Sie angeben, `x-amzn-iot-thingname` muss mit dem Namen der Dingressource AWS IoT übereinstimmen, die einem Zertifikat zugewiesen ist. Wenn sie nicht übereinstimmen, wird ein 403-Fehler zurückgegeben.

Führen Sie den folgenden Befehl in der aus AWS CLI , um den Endpunkt des Anmeldeinformationsanbieters für Ihren AWS-Konto zu erhalten. Weitere Informationen über diese API finden Sie unter DescribeEndpoint. Informationen zu FIPS-fähigen Endpunkten finden Sie unter. AWS IoT Core- Endpunkte des Anmeldeinformationsanbieters

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

Das folgende JSON-Objekt ist die Beispielausgabe des describe-endpoint-Befehls. Es enthält die `endpointAddress` , die Sie verwenden, um ein Sicherheits-Token anzufordern.

```
{
    "endpointAddress": "your_aws_account_specific_prefix.credentials.iot.your
 region.amazonaws.com"
}
```

Verwenden Sie den Endpunkt, um eine HTTPS-Anfrage an den Anmeldeinformationsanbieter zu stellen, ein Sicherheits-Token zurückzugeben. Der folgende Beispielbefehl verwendet `curl`, aber Sie können jeden beliebigen HTTP-Client verwenden.

> **Note**
>
> Beim Namen roleAlias wird zwischen Groß- und Kleinschreibung unterschieden und er muss mit dem Rollenalias übereinstimmen, der in erstellt wurde. AWS IoT

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

Dieser Befehl gibt ein Sicherheits-Token-Objekt zurück, das einen `accessKeyId`, einen `secretAccessKey`, ein `sessionToken`, und einen Ablaufzeitpunkt enthält. Das folgende JSON-Objekt ist die Beispielausgabe des `curl`-Befehls.

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

Anschließend können Sie die `sessionToken` Werte, und verwenden `accessKeyIdsecretAccessKey`, um Anfragen an Dienste zu signieren. AWS Eine end-to-end Demonstration finden Sie im Blogbeitrag So vermeiden Sie fest codierte AWS Anmeldeinformationen auf Geräten mithilfe des AWS IoT Credential Providers im AWS Security Blog.

## Kontenübergreifender Zugriff mit IAM

AWS IoT Core ermöglicht es Ihnen, einem Prinzipal die Möglichkeit zu geben, ein Thema zu veröffentlichen oder zu abonnieren, das AWS-Konto nicht dem Prinzipal gehört. Den kontoübergreifenden Zugriff konfigurieren Sie durch Erstellung einer IAM-Richtlinie und einer IAM-Rolle und das anschließende Anfügen der Richtlinie an die Rolle.

Erstellen Sie zunächst eine kundenseitig verwaltete IAM-Richtlinie wie in Erstellen von IAM-Richtlinien beschrieben, genauso wie für andere Benutzer und Zertifikate in Ihrem AWS-Konto.

Für Geräte, die in der AWS IoT Core Registrierung registriert sind, gewährt die folgende Richtlinie Geräten die Erlaubnis, eine Verbindung herzustellen, indem sie eine Client-ID AWS IoT Core verwenden, die dem Ding-Namen des Geräts entspricht, und dass sie dort veröffentlichen, `my/topic/thing-name` wo *thing-name* sich der Ding-Name des Geräts befindet:

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

```
            "Resource": ["arn:aws:iot:us-east-1:123456789012:client/
${iot:Connection.Thing.ThingName}"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/my/topic/
${iot:Connection.Thing.ThingName}"],
        }
    ]
}
```

Für Geräte, die nicht in der AWS IoT Core Registrierung registriert sind, erteilt die folgende Richtlinie einem Gerät die Erlaubnis, den in der AWS IoT Core Registrierung Ihres Kontos (123456789012) `client1` registrierten Dingnamen zu verwenden, um eine Verbindung zu einem Client-ID-spezifischen Thema herzustellen AWS IoT Core und dort zu veröffentlichen, dessen Name mit einem Präfix versehen ist: `my/topic/`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/client1"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/my/topic/${iot:ClientId}"
            ]
        }
    ]
```

```
}
```

Führen Sie als Nächstes die unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer beschriebenen Schritte aus. Geben Sie die ID des AWS-Konto ein, für das gemeinsamer Zugriff gewährt werden soll. Fügen Sie dann im letzten Schritt die gerade erstellte Richtlinie an die Rolle an. Wenn Sie später die AWS -Konto-ID ändern müssen, auf die Sie den Zugriff gewährt haben, können Sie das folgende Vertrauensrichtlinienformat nutzen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam:us-east-1:567890123456:user/MyUser"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

# Datenschutz in AWS IoT Core

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS IoT Core. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).

- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der AWS IoT API oder auf andere AWS-Services Weise arbeiten oder diese verwenden. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Weitere Informationen zum Datenschutz enthält der Blog-Beitrag AWS Shared Responsibility Model and GDPR im AWS -Sicherheitsblog.

AWS IoT Geräte sammeln Daten, manipulieren diese Daten und senden diese Daten dann an einen anderen Webdienst. Sie können einige Daten für einen kurzen Zeitraum auf Ihrem Gerät speichern. Sie sind dafür verantwortlich, den Datenschutz für diese Daten im Ruhezustand zu gewährleisten. Wenn Ihr Gerät Daten an sendet AWS IoT, geschieht dies über eine TLS-Verbindung, wie später in diesem Abschnitt beschrieben wird. AWS IoT Geräte können Daten an jeden AWS Dienst senden. Weitere Informationen zur Datensicherheit der einzelnen Dienste finden Sie in der Dokumentation zu diesem Dienst. AWS IoT kann so konfiguriert werden, dass CloudWatch Protokolle in Logs geschrieben und AWS IoT API-Aufrufe protokolliert werden AWS CloudTrail. Weitere Informationen zur Datensicherheit für diese Dienste finden Sie unter Authentifizierung und Zugriffskontrolle für

Amazon CloudWatch und Verschlüsseln von CloudTrail Protokolldateien mit AWS KMS-verwalteten Schlüsseln.

## Datenverschlüsselung in AWS IoT

Standardmäßig sind alle AWS IoT Daten während der Übertragung und Speicherung verschlüsselt. Übertragene Daten werden mit TLS verschlüsselt, und Daten im Ruhezustand werden mit AWS eigenen Schlüsseln verschlüsselt. AWS IoT unterstützt derzeit keine vom Kunden verwalteten AWS KMS keys (KMS-Schlüssel) über den AWS Key Management Service (AWS KMS). Device Advisor und AWS IoT Wireless verwenden jedoch nur an, um AWS-eigener Schlüssel Kundendaten zu verschlüsseln.

## Transportsicherheit in AWS IoT Core

TLS (Transport Layer Security) ist ein kryptografisches Protokoll, das für die sichere Kommunikation über ein Computernetzwerk ausgelegt ist. Beim AWS IoT Core Device Gateway müssen Kunden die gesamte Kommunikation während der Übertragung verschlüsseln, indem sie TLS für Verbindungen zwischen Geräten und dem Gateway verwenden. TLS wird verwendet, um die Vertraulichkeit der Anwendungsprotokolle (MQTT, HTTP und WebSocket) zu gewährleisten, die von unterstützt werden. AWS IoT Core TLS unterstützt verschiedene Programmiersprachen und Betriebssysteme. Die AWS darin enthaltenen Daten werden durch den jeweiligen AWS Dienst verschlüsselt. Weitere Informationen zur Datenverschlüsselung bei anderen AWS Diensten finden Sie in der Sicherheitsdokumentation für diesen Dienst.

Inhalt


- TLS-Protokolle
- Sicherheitsrichtlinien
- Wichtige Hinweise zur Transportsicherheit in AWS IoT Core
- Transportsicherheit für LoRa WAN-Wireless-Geräte


### TLS-Protokolle

AWS IoT Core unterstützt die folgenden Versionen des TLS-Protokolls:

- TLS 1.3
- TLS 1.2

Mit AWS IoT Core können Sie die TLS-Einstellungen (für TLS 1.2 und TLS 1.3) in Domänenkonfigurationen konfigurieren. Weitere Informationen finden Sie unter ???.

## Sicherheitsrichtlinien

Eine Sicherheitsrichtlinie ist eine Kombination aus TLS-Protokollen und ihren Verschlüsselungen, die bestimmen, welche Protokolle und Verschlüsselungen bei TLS-Verhandlungen zwischen einem Client und einem Server unterstützt werden. Sie können Ihre Geräte so konfigurieren, dass sie je nach Bedarf vordefinierte Sicherheitsrichtlinien verwenden. Beachten Sie, dass benutzerdefinierte Sicherheitsrichtlinien AWS IoT Core nicht unterstützt werden.

Sie können eine der vordefinierten Sicherheitsrichtlinien für Ihre Geräte auswählen, wenn Sie eine Verbindung herstellen AWS IoT Core. Die Namen der neuesten vordefinierten Sicherheitsrichtlinien AWS IoT Core enthalten Versionsinformationen, die auf dem Jahr und Monat basieren, in dem sie veröffentlicht wurden. Die vordefinierte Standardsicherheitsrichtlinie ist beispielsweise `IoTSecurityPolicy_TLS13_1_2_2022_10`. Um eine Sicherheitsrichtlinie anzugeben, können Sie die AWS IoT Konsole oder die verwenden AWS CLI. Weitere Informationen finden Sie unter ???.

In der folgenden Tabelle werden die aktuellen vordefinierten Sicherheitsrichtlinien beschrieben, die von AWS IoT Core unterstützt werden. Die `IotSecurityPolicy_` wurde aus Richtliniennamen in der Überschriftenzeile entfernt, sodass sie passen.

| Sicherheitsrichtlinie | TLS13_1_3_2022_10 | TLS13_1_2_2022_10 | TLS12_1_2_2022_10 | TLS12_1_0_2016_01* | | TLS12_1_0_2015_01* | |
|---|---|---|---|---|---|---|---|
| TCP-Port | 443/8443/8883 | 443/8443/8883 | 443/8443/8883 | 443 | 8443/8883 | 443 | 8443/8883 |
| TLS-Protokolle | | | | | | | |
| TLS 1.2 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| TLS 1.3 | ✓ | ✓ | | | | | |
| TLS-Verschlüsselungsverfahren | | | | | | | |

| Sicherheitsrichtlinie | TLS13_1_3_2022_10 | TLS13_1_2_2022_10 | TLS12_1_2_2022_10 | TLS12_1_0_2016_01* | | TLS12_1_0_2015_01* | |
|---|---|---|---|---|---|---|---|
| TLS AES 128 GCM SHA256 | ✓ | ✓ | | | | | |
| TLS AES 256 GCM SHA384 | ✓ | ✓ | | | | | |
| TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 | ✓ | ✓ | | | | | |
| ECDHE-RSA- - GCM-AES128 SHA256 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ECDHE-RSA-AES128 - SHA256 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ECDHE-RSA-AES128 - SHA | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Sicherheitsrichtlinie | TLS13_1_3_2022_10 | TLS13_1_2_2022_10 | TLS12_1_2_2022_10 | TLS12_1_0_2016_01* | | TLS12_1_0_2015_01* | |
|---|---|---|---|---|---|---|---|
| ECDHE-RSA-AES256-GCM-SHA384 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ECDHE-RSA-AES256 - SHA384 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ECDHE-RSA-AES256 - SHA | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| AES128-GCM-SHA256 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| AES128-SHA256 | | ✓ | ✓ | ✓ | | ✓ | ✓ |
| AES128-SCHA | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| AES256-GCM-SHA384 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| AES256-SHA256 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| AES256-SCHA | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Sicherheitsrichtlinie | TLS13_1_3_2022_10 | TLS13_1_2_2022_10 | TLS12_1_2_2022_10 | TLS12_1_0_2016_01* | | TLS12_1_0_2015_01* | |
|---|---|---|---|---|---|---|---|
| DHE-RSA-SHA AES256 | | | | | | ✓ | ✓ |
| ECDHE-ECDSA-AES128-GCM-SHA256 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ECDHE-ECDSA- - AES128 SHA256 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ECDHE-ECDSA--SHA AES128 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ECDHE-ECDSA--GCM-AES256 SHA384 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ECDHE-ECDSA- - AES256 SHA384 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Sicherheitsrichtlinie | TLS13_1_3_2022_10 | TLS13_1_2_2022_10 | TLS12_1_2_2022_10 | TLS12_1_0_2016_01* | | TLS12_1_0_2015_01* | |
|---|---|---|---|---|---|---|---|
| ECDHE-ECDSA--SHA AES256 | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

> **Note**
>
> `TLS12_1_0_2016_01`ist nur in den folgenden Sprachen verfügbar AWS-Regionen: ap-east-1, ap-northeast-2, ap-south-1, ap-southeast-2, ca-central-1, cn-north-1, cn-northwest-1, eu-north-1, eu-west-2, eu-west-3, me-south-1, sa-east-1, us-east-2, -1, -2, us-west-1. us-gov-west us-gov-west
> `TLS12_1_0_2015_01`ist nur in den folgenden Ländern verfügbar AWS-Regionen: ap-northeast-1, ap-southeast-1, eu-central-1, eu-west-1, us-east-1, us-west-2.

## Wichtige Hinweise zur Transportsicherheit in AWS IoT Core

Bei Geräten, die AWS IoT Core über MQTT eine Verbindung herstellen, verschlüsselt TLS die Verbindung zwischen den Geräten und dem Broker und verwendet die TLS-Client-Authentifizierung, um Geräte zu identifizieren. AWS IoT Core Weitere Informationen finden Sie unter Client-Authentifizierung. Bei Geräten, die AWS IoT Core über HTTP eine Verbindung herstellen, verschlüsselt TLS die Verbindung zwischen den Geräten und dem Broker, und die Authentifizierung wird an AWS Signature Version 4 delegiert. Weitere Informationen finden Sie unter Signieren von Anforderungen mit Signature Version 4 in der Allgemeinen Referenz zu AWS .

Wenn Sie Geräte mit verbinden AWS IoT Core, ist das Senden der SNI-Erweiterung (Server Name Indication) nicht erforderlich, wird aber dringend empfohlen. Um Funktionen wie die Registrierung mehrerer Konten, benutzerdefinierte Domänen, VPC-Endpunkte und konfigurierte TLS-Richtlinien zu verwenden, müssen Sie die SNI-Erweiterung verwenden und die vollständige Endpunktadresse in das Feld eingeben. `host_name` Im Feld `host_name` muss der Endpunkt angegeben sein, den Sie aufrufen. Dieser Endpunkt muss einer der folgenden sein:

- den von `aws iot describe-endpoint --endpoint-type iot:Data-ATS` zurückgegebenen `endpointAddress`
- den von `aws iot describe-domain-configuration --domain-configuration-name "domain_configuration_name"` zurückgegebenen `domainName`

Verbindungsversuche von Geräten mit dem falschen oder `host_name` ungültigen Wert schlagen fehl. AWS IoT Core protokolliert Fehler CloudWatch für den Authentifizierungstyp Benutzerdefinierte Authentifizierung.

AWS IoT Core unterstützt die SessionTicket TLS-Erweiterung nicht.

### Transportsicherheit für LoRa WAN-Wireless-Geräte

LoRaWAN-Geräte folgen den in LoRaWAN™ SECURITY: A White Paper Prepared for the LoRa Alliance™ von Gemalto, Actility und Semtech beschriebenen Sicherheitspraktiken.

Weitere Informationen zur Transportsicherheit mit LoRa WAN-Geräten finden Sie unter LoRaWAN-Daten und Transportsicherheit.

## Datenverschlüsselung in AWS IoT

Datenschutz bezieht sich auf den Schutz von Daten während der Übertragung (beim Hin- und Hersenden AWS IoT) und im Ruhezustand (während sie auf Geräten oder von anderen AWS Diensten gespeichert werden). Alle an AWS IoT gesendeten Daten werden über eine TLS-Verbindung unter Verwendung von MQTT, HTTPS und WebSocket Protokollen gesendet, sodass sie während der Übertragung standardmäßig sicher sind. AWS IoT Geräte sammeln Daten und senden sie dann zur weiteren Verarbeitung an andere AWS Dienste. Weitere Informationen zur Datenverschlüsselung für andere AWS -Services finden Sie in der Sicherheitsdokumentation des Services.

FreeRTOS bietet eine PKCS#11-Bibliothek, die Schlüsselspeicher abstrahiert, auf kryptografische Objekte zugreift und Sitzungen verwaltet. Es liegt in Ihrer Verantwortung, diese Bibliothek zu verwenden, um Daten im Ruhezustand auf Ihren Geräten zu verschlüsseln. Weitere Informationen finden Sie unter FreeRTOS#11-Bibliothek (Public Key Cryptography Standard).

### Device Advisor

Verschlüsselung während der Übertragung

Daten, die an und von Device Advisor gesendet werden, werden während der Übertragung verschlüsselt. Alle Daten, die bei der Verwendung des Device Advisor APIs an und von dem Dienst gesendet werden, werden mit Signature Version 4 verschlüsselt. Weitere Informationen darüber, wie AWS API-Anfragen signiert werden, finden Sie unter Signieren von AWS API-Anfragen. Alle Daten, die von Ihren Testgeräten an Ihren Device-Advisor-Testendpunkt gesendet werden, werden über eine TLS-Verbindung gesendet, sodass sie während der Übertragung standardmäßig sicher sind.

### Schlüsselverwaltung in AWS IoT

Alle Verbindungen zu AWS IoT werden mit TLS hergestellt, sodass für die erste TLS-Verbindung keine clientseitigen Verschlüsselungsschlüssel erforderlich sind.

Die Geräte müssen sich mit einem X.509-Zertifikat oder einer Amazon-Cognito-Identität authentifizieren. Sie können ein Zertifikat für Sie AWS IoT generieren lassen. In diesem Fall wird ein public/private key pair generiert. Wenn Sie die AWS IoT Konsole verwenden, werden Sie aufgefordert, das Zertifikat und die Schlüssel herunterzuladen. Wenn Sie den `create-keys-and-certificate`-CLI-Befehl verwenden, werden das Zertifikat und die Schlüssel vom CLI-Befehl zurückgegeben. Sie sind dafür verantwortlich, das Zertifikat und den privaten Schlüssel auf Ihr Gerät zu kopieren und sicher aufzubewahren.

AWS IoT unterstützt derzeit keine vom Kunden verwalteten AWS KMS keys (KMS-Schlüssel) von AWS Key Management Service (AWS KMS). Device Advisor und AWS IoT Wireless verwenden jedoch nur an, um AWS-eigener Schlüssel Kundendaten zu verschlüsseln.

Device Advisor

Alle Daten, die bei der Verwendung von an Device Advisor gesendet werden, werden im AWS APIs Ruhezustand verschlüsselt. Device Advisor verschlüsselt alle Ihre Daten im Ruhezustand mithilfe von KMS-Schlüsseln, die in AWS Key Management Service gespeichert und verwaltet werden. Device Advisor verschlüsselt Ihre Daten mit AWS-eigene Schlüssel. Weitere Informationen zu finden Sie AWS-eigene Schlüssel unter AWS-eigene Schlüssel.

## Identitäts- und Zugriffsmanagement für AWS IoT

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert

(angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS IoT IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen


- Zielgruppe
- Authentifizierung mit IAM-Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Wie AWS IoT funktioniert mit IAM
- AWS IoT Beispiele für identitätsbasierte Richtlinien
- AWS verwaltete Richtlinien für AWS IoT
- Fehlerbehebung bei AWS IoT Identität und Zugriff


## Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. AWS IoT

Dienstbenutzer — Wenn Sie den AWS IoT Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS IoT Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Unter Fehlerbehebung bei AWS IoT Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in AWS IoT haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS IoT Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS IoT. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS IoT Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann AWS IoT, finden Sie unterWie AWS IoT funktioniert mit IAM.

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS IoT verfassen können. Beispiele für AWS IoT

identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. AWS IoT Beispiele für identitätsbasierte Richtlinien

## Authentifizierung mit IAM-Identitäten

In AWS IoT Identitäten können Gerätezertifikate (X.509), Amazon Cognito Cognito-Identitäten oder IAM-Benutzer oder -Gruppen enthalten sein. In diesem Thema werden nur IAM-Identitäten behandelt. Weitere Informationen zu den anderen Identitäten, die unterstützt werden, finden Sie unter. AWS IoT Client-Authentifizierung

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

## AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

## IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb von Ihnen AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

## IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten

Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Methoden für die Übernahme einer Rolle im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen

werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

## Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

## Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

## Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein

bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

### Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

### Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen

zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.

- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

### Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

## Wie AWS IoT funktioniert mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf zu verwalten AWS IoT, sollten Sie wissen, mit welchen IAM-Funktionen Sie verwenden können. AWS IoTEinen allgemeinen Überblick darüber, wie AWS IoT und andere AWS Dienste mit IAM funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Services That Work with IAM.

Themen

- Identitätsbasierte AWS IoT -Richtlinien
- Ressourcenbasierte AWS IoT -Richtlinien
- Autorisierung auf der Basis von AWS IoT -Tags

- AWS IoT IAM-Rollen

## Identitätsbasierte AWS IoT -Richtlinien

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen erteilt oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. AWS IoT unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

In der folgenden Tabelle sind die IAM-IoT-Aktionen, die zugehörige AWS IoT API und die Ressource aufgeführt, die durch die Aktion manipuliert wird.

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: AcceptCertificateTransfer | AcceptCertificateTransfer | `arn:aws:iot:` *`region`*`:`*`account-id`* `:cert/`*`cert-id`* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| | | **Note**<br>Das im ARN AWS-Konto angegebene Konto muss das Konto sein, auf das das Zertifikat übertragen wird. |
| IoT: AddThingToThingGroup | AddThingToThingGroup | `arn:aws:iot:` *region*`:`*account-id* `:thinggroup/` *thing-group-name*<br><br>`arn:aws:iot:` *region*`:`*account-id* `:thing/`*thing-name* |
| IoT: AssociateTargetsWithJob | AssociateTargetsWithJob | Keine |
| IoT: AttachPolicy | AttachPolicy | `arn:aws:iot:` *region*`:`*account-id* `:thinggroup/` *thing-group-name*<br><br>or<br><br>`arn:aws:iot:` *region*`:`*account-id* `:cert/`*cert-id* |
| IoT: AttachPrincipalPolicy | AttachPrincipalPolicy | `arn:aws:iot:` *region*`:`*account-id* `:cert/`*cert-id* |
| IoT: AttachSecurityProfile | AttachSecurityProfile | `arn:aws:iot:` *region*`:`*account-id* `:securityprofile/` *security-profile-name*<br><br>`arn:aws:iot:` *region*`:`*account-id* `:dimension/` *dimension-name* |
| IoT: AttachThingPrincipal | AttachThingPrincipal | `arn:aws:iot:` *region*`:`*account-id* `:cert/`*cert-id* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: CancelCertificateTransfer | CancelCertificateTransfer | `arn:aws:iot:` *region*`:`*account-id* `:cert/`*cert-id*<br><br>**Note**<br>Das im ARN AWS-Konto angegebene Konto muss das Konto sein, auf das das Zertifikat übertragen wird. |
| IoT: CancelJob | CancelJob | `arn:aws:iot:` *region*`:`*account-id* `:job/`*job-id* |
| IoT: CancelJobExecution | CancelJobExecution | `arn:aws:iot:` *region*`:`*account-id* `:job/`*job-id*<br><br>`arn:aws:iot:` *region*`:`*account-id* `:thing/`*thing-name* |
| IoT: ClearDefaultAuthorizer | ClearDefaultAuthorizer | Keine |
| IoT: CreateAuthorizer | CreateAuthorizer | `arn:aws:iot:` *region*`:`*account-id* `:authorizer/` *authorizer-function-name* |
| IoT: CreateCertificateFromCsr | CreateCertificateFromCsr | * |
| IoT: CreateDimension | CreateDimension | `arn:aws:iot:` *region*`:`*account-id* `:dimension/` *dimension-name* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: CreateJob | CreateJob | `arn:aws:iot:` *region*`:`*account-id* `:job/`*job-id*<br><br>`arn:aws:iot:` *region*`:`*account-id* `:thinggroup/` *thing-group-name*<br><br>`arn:aws:iot:` *region*`:`*account-id* `:thing/`*thing-name*<br><br>`arn:aws:iot:` *region*`:`*account-id* `:jobtemplate/` *job-template-id* |
| IoT: CreateJobTemplate | CreateJobTemplate | `arn:aws:iot:` *region*`:`*account-id* `:job/`*job-id*<br><br>`arn:aws:iot:` *region*`:`*account-id* `:jobtemplate/` *job-template-id* |
| IoT: CreateKeysAndCertificate | CreateKeysAndCertificate | * |
| IoT: CreatePolicy | CreatePolicy | `arn:aws:iot:` *region*`:`*account-id* `:policy/`*policy-name* |
| IoT: CreatePolicyVersion | CreatePolicyVersion | `arn:aws:iot:` *region*`:`*account-id* `:policy/`*policy-name*<br><br>**Note**<br>Dies muss eine AWS IoT Richtlinie sein, keine IAM-Richtlinie. |
| IoT: CreateRoleAlias | CreateRoleAlias | (Parameter: roleAlias)<br><br>`arn:aws:iot:` *region*`:`*account-id* `:rolealias/` *role-alias-name* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: CreateSecurityProfile | CreateSecurityProfile | arn:aws:iot: *region*:*account-id* :securityprofile/ *security-profile-name*<br><br>arn:aws:iot: *region*:*account-id* :dimension/ *dimension-name* |
| IoT: CreateThing | CreateThing | arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: CreateThingGroup | CreateThingGroup | arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name*<br><br>für die Gruppe, die erstellt wird, und für die übergeordnete Gruppe, sofern verwendet |
| IoT: CreateThingType | CreateThingType | arn:aws:iot: *region*:*account-id* :thingtype/ *thing-type-name* |
| IoT: CreateTopicRule | CreateTopicRule | arn:aws:iot: *region*:*account-id* :rule/*rule-name* |
| IoT: DeleteAuthorizer | DeleteAuthorizer | arn:aws:iot: *region*:*account-id* :authorizer/ *authorizer-name* |
| IoT: löschen CACertificate | Löschen CACertificate | arn:aws:iot: *region*:*account-id* :cacert/*cert-id* |
| IoT: DeleteCertificate | DeleteCertificate | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |
| IoT: DeleteDimension | DeleteDimension | arn:aws:iot: *region*:*account-id* :dimension/ *dimension-name* |
| IoT: DeleteJob | DeleteJob | arn:aws:iot: *region*:*account-id* :job/*job-id* |
| IoT: DeleteJobTemplate | DeleteJobTemplate | arn:aws:iot: *region*:*account-id* :job/*job-template-id* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: DeleteJobExecution | DeleteJobExecution | arn:aws:iot: *region*:*account-id* :job/*job-id*<br><br>arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: DeletePolicy | DeletePolicy | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: DeletePolicyVersion | DeletePolicyVersion | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: DeleteRegistrationCode | DeleteRegistrationCode | * |
| IoT: DeleteRoleAlias | DeleteRoleAlias | arn:aws:iot: *region*:*account-id* :rolealias/ *role-alias-name* |
| IoT: DeleteSecurityProfile | DeleteSecurityProfile | arn:aws:iot: *region*:*account-id* :securityprofile/ *security-profile-name*<br><br>arn:aws:iot: *region*:*account-id* :dimension/ *dimension-name* |
| IoT: DeleteThing | DeleteThing | arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: DeleteThingGroup | DeleteThingGroup | arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name* |
| IoT: DeleteThingType | DeleteThingType | arn:aws:iot: *region*:*account-id* :thingtype/ *thing-type-name* |
| IoT: DeleteTopicRule | DeleteTopicRule | arn:aws:iot: *region*:*account-id* :rule/*rule-name* |
| IoT: V2 löschen LoggingLevel | Lösche V2 LoggingLevel | arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: DeprecateThingType | DeprecateThingType | `arn:aws:iot:` *`region`*`:`*`account-id`* `:thingtype/` *`thing-type-name`* |
| IoT: DescribeAuthorizer | DescribeAuthorizer | `arn:aws:iot:` *`region`*`:`*`account-id`* `:authorizer/` *`authorizer-function-name`*<br><br>(Parameter: authorizerName)<br>Keine |
| IoT: BeschreibenCACertificate | BeschreibenCACertificate | `arn:aws:iot:` *`region`*`:`*`account-id`* `:cacert/`*`cert-id`* |
| IoT: DescribeCertificate | DescribeCertificate | `arn:aws:iot:` *`region`*`:`*`account-id`* `:cert/`*`cert-id`* |
| IoT: DescribeDefaultAuthorizer | DescribeDefaultAuthorizer | Keine |
| IoT: DescribeEndpoint | DescribeEndpoint | * |
| IoT: DescribeEventConfigurations | DescribeEventConfigurations | Keine |
| IoT: DescribeIndex | DescribeIndex | `arn:aws:iot:` *`region`*`:`*`account-id`* `:index/`*`index-name`* |
| IoT: DescribeJob | DescribeJob | `arn:aws:iot:` *`region`*`:`*`account-id`* `:job/`*`job-id`* |
| IoT: DescribeJobExecution | DescribeJobExecution | Keine |
| IoT: DescribeJobTemplate | DescribeJobTemplate | `arn:aws:iot:` *`region`*`:`*`account-id`* `:job/`*`job-template-id`* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: DescribeRoleAlias | DescribeRoleAlias | arn:aws:iot: *region*:*account-id* :rolealias/ *role-alias-name* |
| IoT: DescribeThing | DescribeThing | arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: DescribeThingGroup | DescribeThingGroup | arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name* |
| IoT: DescribeThingRegistrationTask | DescribeThingRegistrationTask | Keine |
| IoT: DescribeThingType | DescribeThingType | arn:aws:iot: *region*:*account-id* :thingtype/ *thing-type-name* |
| IoT: DetachPolicy | DetachPolicy | arn:aws:iot: *region*:*account-id* :cert/*cert-id*<br><br>or<br><br>arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name* |
| IoT: DetachPrincipalPolicy | DetachPrincipalPolicy | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |
| IoT: DetachSecurityProfile | DetachSecurityProfile | arn:aws:iot: *region*:*account-id* :securityprofile/ *security-profile-name*<br><br>arn:aws:iot: *region*:*account-id* :dimension/ *dimension-name* |
| IoT: DetachThingPrincipal | DetachThingPrincipal | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: DisableTopicRule | DisableTopicRule | arn:aws:iot: *region*:*account-id* :rule/*rule-name* |
| IoT: EnableTopicRule | EnableTopicRule | arn:aws:iot: *region*:*account-id* :rule/*rule-name* |
| IoT: GetEffectivePolicies | GetEffectivePolicies | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |
| IoT: GetIndexingConfiguration | GetIndexingConfiguration | Keine |
| IoT: GetJobDocument | GetJobDocument | arn:aws:iot: *region*:*account-id* :job/*job-id* |
| IoT: GetLoggingOptions | GetLoggingOptions | * |
| IoT: GetPolicy | GetPolicy | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: GetPolicyVersion | GetPolicyVersion | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: GetRegistrationCode | GetRegistrationCode | * |
| IoT: GetTopicRule | GetTopicRule | arn:aws:iot: *region*:*account-id* :rule/*rule-name* |
| IoT: ListAttachedPolicies | ListAttachedPolicies | arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name*<br>or<br>arn:aws:iot: *region*:*account-id* :cert/*cert-id* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: ListAuthorizers | ListAuthorizers | Keine |
| IoT: ListeCACertificates | ListeCACertificates | * |
| IoT: ListCertificates | ListCertificates | * |
| IoT: ListCertificatesByKanada | ListCertificatesByCA | * |
| IoT: ListIndices | ListIndices | Keine |
| IoT: ListJobExecutionsForJob | ListJobExecutionsForJob | Keine |
| IoT: ListJobExecutionsForThing | ListJobExecutionsForThing | Keine |
| IoT: ListJobs | ListJobs | `arn:aws:iot:` *`region`*`:`*`account-id`* `:thinggroup/` *`thing-group-name`*<br><br>wenn der thingGroupName Parameter verwendet wird |
| iot: ListJobTemplates | ListJobs | Keine |
| IoT: ListOutgoingCertificates | ListOutgoingCertificates | * |
| IoT: ListPolicies | ListPolicies | * |
| IoT: ListPolicyPrincipals | ListPolicyPrincipals | * |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: ListPolicyVersions | ListPolicyVersions | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: ListPrincipalPolicies | ListPrincipalPolicies | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |
| IoT: ListPrincipalThings | ListPrincipalThings | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |
| IoT: ListRoleAliases | ListRoleAliases | Keine |
| IoT: ListTargetsForPolicy | ListTargetsForPolicy | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: ListThingGroups | ListThingGroups | Keine |
| IoT: ListThingGroupsForThing | ListThingGroupsForThing | arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: ListThingPrincipals | ListThingPrincipals | arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: ListThingRegistrationTaskReports | ListThingRegistrationTaskReports | Keine |
| IoT: ListThingRegistrationTasks | ListThingRegistrationTasks | Keine |
| IoT: ListThingTypes | ListThingTypes | * |
| IoT: ListThings | ListThings | * |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: ListThingsInThingGroup | ListThingsInThingGroup | arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name* |
| IoT: ListTopicRules | ListTopicRules | * |
| IoT: Liste V2 LoggingLevels | Liste V2 LoggingLevels | Keine |
| IoT: registrierenCACertificate | RegistrierenCACertificate | * |
| IoT: RegisterCertificate | RegisterCertificate | * |
| IoT: RegisterThing | RegisterThing | Keine |
| IoT: RejectCertificateTransfer | RejectCertificateTransfer | arn:aws:iot: *region*:*account-id* :cert/*certificate-id* |
| IoT: RemoveThingFromThingGroup | RemoveThingFromThingGroup | arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name*<br><br>arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: ReplaceTopicRule | ReplaceTopicRule | arn:aws:iot: *region*:*account-id* :rule/*rule-name* |
| IoT: SearchIndex | SearchIndex | arn:aws:iot: *region*:*account-id* :index/*index-id* |
| IoT: SetDefaultAuthorizer | SetDefaultAuthorizer | arn:aws:iot: *region*:*account-id* :authorizer/ *authorizer-function-name* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: SetDefaultPolicyVersion | SetDefaultPolicyVersion | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: SetLoggingOptions | SetLoggingOptions | arn:aws:iot: *region*:*account-id* :role/*role-name* |
| IoT: SETv2LoggingLevel | SETv2LoggingLevel | arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name* |
| IoT: SETV2LoggingOptions | SETv2LoggingOptions | arn:aws:iot: *region*:*account-id* :role/*role-name* |
| IoT: StartThingRegistrationTask | StartThingRegistrationTask | Keine |
| IoT: StopThingRegistrationTask | StopThingRegistrationTask | Keine |
| IoT: TestAuthorization | TestAuthorization | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |
| IoT: TestInvokeAuthorizer | TestInvokeAuthorizer | Keine |
| IoT: TransferCertificate | TransferCertificate | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |
| IoT: UpdateAuthorizer | UpdateAuthorizer | arn:aws:iot: *region*:*account-id* :authorizerfunction/ *authorizer-function-name* |
| IoT: aktualisierenCACertificate | AktualisierenCACertificate | arn:aws:iot: *region*:*account-id* :cacert/*cert-id* |
| IoT: UpdateCertificate | UpdateCertificate | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: UpdateDimension | UpdateDimension | arn:aws:iot: *region*:*account-id* :dimension/ *dimension-name* |
| IoT: UpdateEventConfigurations | UpdateEventConfigurations | Keine |
| IoT: UpdateIndexingConfiguration | UpdateIndexingConfiguration | Keine |
| IoT: UpdateRoleAlias | UpdateRoleAlias | arn:aws:iot: *region*:*account-id* :rolealias/ *role-alias-name* |
| IoT: UpdateSecurityProfile | UpdateSecurityProfile | arn:aws:iot: *region*:*account-id* :securityprofile/ *security-profile-name*<br><br>arn:aws:iot: *region*:*account-id* :dimension/ *dimension-name* |
| IoT: UpdateThing | UpdateThing | arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: UpdateThingGroup | UpdateThingGroup | arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name* |
| IoT: UpdateThingGroupsForThing | UpdateThingGroupsForThing | arn:aws:iot: *region*:*account-id* :thing/*thing-name*<br><br>arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name* |

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS IoT verwendet:`iot:`. Um beispielsweise jemandem die Erlaubnis zu erteilen, alle IoT-Dinge aufzulisten, die in seiner AWS-Konto `ListThings` API registriert sind, nehmen Sie die `iot:ListThings` Aktion in seine Richtlinie auf. Richtlinienerklärungen müssen `Action` entweder ein `NotAction` Oder-Element enthalten. AWS

IoT definiert einen eigenen Satz von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "iot:Describe*"
```

Eine Liste der AWS IoT Aktionen finden Sie AWS IoT im IAM-Benutzerhandbuch unter Definierte Aktionen von.

Device-Advisor-Aktionen

Die folgende Tabelle listet die Device-Advisor-Aktionen im IAM-IoT, die zugehörige AWS IoT -Device-Advisor-API und die Ressource auf, die die Aktion bearbeitet.

| Richtlinienaktionen | AWS IoT API | Ressourcen |
|---|---|---|
| Berater für IoT-Geräte: CreateSuiteDefinition | CreateSuiteDefinition | Keine |
| iotdeviceadvisor: DeleteSuiteDefinition | DeleteSuiteDefinition | `arn:aws:iotdeviceadvisor:region:account-id:suitedefinition/suite-definition-id` |
| iotdeviceadvisor: GetSuiteDefinition | GetSuiteDefinition | `arn:aws:iotdeviceadvisor:region:account-id:suitedefinition/suite-definition-id` |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| iotdeviceadvisor:GetSuiteRun | GetSuiteRun | arn:aws:iotdeviceadvisor:*region*:*account-id*:suitedefinition/*suite-run-id* |
| iotdeviceadvisor:GetSuiteRunReport | GetSuiteRunReport | arn:aws:iotdeviceadvisor:*region*:*account-id*:suiterun/*suite-definition-id*/*suite-run-id* |
| iotdeviceadvisor:ListSuiteDefinitions | ListSuiteDefinitions | Keine |
| iotdeviceadvisor:ListSuiteRuns | ListSuiteRuns | arn:aws:iotdeviceadvisor:*region*:*account-id*:suitedefinition/*suite-definition-id* |
| iotdeviceadvisor:ListTagsForResource | ListTagsForResource | arn:aws:iotdeviceadvisor:*region*:*account-id*:suitedefinition/*suite-definition-id*<br><br>arn:aws:iotdeviceadvisor:*region*:*account-id*:suiterun/suite-definition-id/*suite-run-id* |
| iotdeviceadvisor:StartSuiteRun | StartSuiteRun | arn:aws:iotdeviceadvisor:*region*:*account-id*:suitedefinition/*suite-definition-id* |
| iotdeviceadvisor:TagResource | TagResource | arn:aws:iotdeviceadvisor:*region*:*account-id*:suitedefinition/*suite-definition-id*<br><br>arn:aws:iotdeviceadvisor:*region*:*account-id*:suiterun/suite-definition-id/*suite-run-id* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| iotdeviceadvisor:UntagResource | UntagResource | arn:aws:iotdeviceadvisor:*region*:*account-id*:suitedefinition/*suite-definition-id*<br><br>arn:aws:iotdeviceadvisor:*region*:*account-id*:suiterun/suite-definition-id/*suite-run-id* |
| iotdeviceadvisor:UpdateSuiteDefinition | UpdateSuiteDefinition | arn:aws:iotdeviceadvisor:*region*:*account-id*:suitedefinition/*suite-definition-id* |
| iotdeviceadvisor:StopSuiteRun | StopSuiteRun | arn:aws:iotdeviceadvisor:*region*:*account-id*:suiterun/suite-definition-id/*suite-run-id* |

Richtlinienaktionen in AWS IoT Device Advisor verwenden vor der Aktion das folgende Präfix:. `iotdeviceadvisor:` Um beispielsweise jemandem die Erlaubnis zu erteilen, alle in seiner AWS-Konto ListSuiteDefinitions API registrierten Suite-Definitionen aufzulisten, nehmen Sie die `iotdeviceadvisor:ListSuiteDefinitions` Aktion in seine Richtlinie auf.

Ressourcen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

AWS IoT Ressourcen

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: AcceptCertificateTransfer | AcceptCertificateTransfer | `arn:aws:iot:` *region*`:`*account-id*` :cert/`*cert-id*<br><br>**Note**<br>Das im ARN AWS-Konto angegebene Konto muss das Konto sein, auf das das Zertifikat übertragen wird. |
| IoT: AddThingToThingGroup | AddThingToThingGroup | `arn:aws:iot:` *region*`:`*account-id*` :thinggroup/` *thing-group-name*<br><br>`arn:aws:iot:` *region*`:`*account-id*` :thing/`*thing-name* |
| IoT: AssociateTargetsWithJob | AssociateTargetsWithJob | Keine |
| IoT: AttachPolicy | AttachPolicy | `arn:aws:iot:` *region*`:`*account-id*` :thinggroup/` *thing-group-name*<br><br>or<br><br>`arn:aws:iot:` *region*`:`*account-id*` :cert/`*cert-id* |
| IoT: AttachPrincipalPolicy | AttachPrincipalPolicy | `arn:aws:iot:` *region*`:`*account-id*` :cert/`*cert-id* |
| IoT: AttachThingPrincipal | AttachThingPrincipal | `arn:aws:iot:` *region*`:`*account-id*` :cert/`*cert-id* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: CancelCertificateTransfer | CancelCertificateTransfer | `arn:aws:iot:` *region*`:`*account-id* `:cert/`*cert-id*<br><br>**Note**<br>Das im ARN AWS-Konto angegebene Konto muss das Konto sein, auf das das Zertifikat übertragen wird. |
| IoT: CancelJob | CancelJob | `arn:aws:iot:` *region*`:`*account-id* `:job/`*job-id* |
| IoT: CancelJobExecution | CancelJobExecution | `arn:aws:iot:` *region*`:`*account-id* `:job/`*job-id*<br><br>`arn:aws:iot:` *region*`:`*account-id* `:thing/`*thing-name* |
| IoT: ClearDefaultAuthorizer | ClearDefaultAuthorizer | Keine |
| IoT: CreateAuthorizer | CreateAuthorizer | `arn:aws:iot:` *region*`:`*account-id* `:authorizer/` *authorizer-function-name* |
| IoT: CreateCertificateFromCsr | CreateCertificateFromCsr | * |
| IoT: CreateJob | CreateJob | `arn:aws:iot:` *region*`:`*account-id* `:job/`*job-id*<br><br>`arn:aws:iot:` *region*`:`*account-id* `:thinggroup/` *thing-group-name*<br><br>`arn:aws:iot:` *region*`:`*account-id* `:thing/`*thing-name*<br><br>`arn:aws:iot:` *region*`:`*account-id* `:jobtemplate/` *job-template-id* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: CreateJobTemplate | CreateJobTemplate | `arn:aws:iot:` *region*`:`*account-id*` :job/`*job-id*<br><br>`arn:aws:iot:` *region*`:`*account-id*` :jobtemplate/` *job-template-id* |
| IoT: CreateKeysAndCertificate | CreateKeysAndCertificate | * |
| IoT: CreatePolicy | CreatePolicy | `arn:aws:iot:` *region*`:`*account-id*` :policy/`*policy-name* |
| CreatePolicyVersion | IoT: CreatePolicyVersion | `arn:aws:iot:` *region*`:`*account-id*` :policy/`*policy-name*<br><br>**Note**<br>Dies muss eine AWS IoT Richtlinie sein, keine IAM-Richtlinie. |
| IoT: CreateRoleAlias | CreateRoleAlias | (Parameter: roleAlias)<br><br>`arn:aws:iot:` *region*`:`*account-id*` :rolealias/` *role-alias-name* |
| IoT: CreateThing | CreateThing | `arn:aws:iot:` *region*`:`*account-id*` :thing/`*thing-name* |
| IoT: CreateThingGroup | CreateThingGroup | `arn:aws:iot:` *region*`:`*account-id*` :thinggroup/` *thing-group-name*<br><br>für die Gruppe, die erstellt wird, und für die übergeordnete Gruppe, sofern verwendet |
| IoT: CreateThingType | CreateThingType | `arn:aws:iot:` *region*`:`*account-id*` :thingtype/` *thing-type-name* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: CreateTopicRule | CreateTopicRule | arn:aws:iot: *region*:*account-id* :rule/*rule-name* |
| IoT: DeleteAuthorizer | DeleteAuthorizer | arn:aws:iot: *region*:*account-id* :authorizer/ *authorizer-name* |
| IoT: löschen CACertificate | Löschen CACertificate | arn:aws:iot: *region*:*account-id* :cacert/*cert-id* |
| IoT: DeleteCertificate | DeleteCertificate | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |
| IoT: DeleteJob | DeleteJob | arn:aws:iot: *region*:*account-id* :job/*job-id* |
| IoT: DeleteJobExecution | DeleteJobExecution | arn:aws:iot: *region*:*account-id* :job/*job-id*<br>arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: DeleteJobTemplate | DeleteJobTemplate | arn:aws:iot: *region*:*account-id* :jobtemplate/ *job-template-id* |
| IoT: DeletePolicy | DeletePolicy | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: DeletePolicyVersion | DeletePolicyVersion | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: DeleteRegistrationCode | DeleteRegistrationCode | * |
| IoT: DeleteRoleAlias | DeleteRoleAlias | arn:aws:iot: *region*:*account-id* :rolealias/ *role-alias-name* |
| IoT: DeleteThing | DeleteThing | arn:aws:iot: *region*:*account-id* :thing/*thing-name* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: DeleteThingGroup | DeleteThingGroup | `arn:aws:iot:` *region*`:`*account-id* `:thinggroup/` *thing-group-name* |
| IoT: DeleteThingType | DeleteThingType | `arn:aws:iot:` *region*`:`*account-id* `:thingtype/` *thing-type-name* |
| IoT: DeleteTopicRule | DeleteTopicRule | `arn:aws:iot:` *region*`:`*account-id* `:rule/`*rule-name* |
| IoT: V2 löschen LoggingLevel | Lösche V2 LoggingLevel | `arn:aws:iot:` *region*`:`*account-id* `:thinggroup/` *thing-group-name* |
| IoT: DeprecateThingType | DeprecateThingType | `arn:aws:iot:` *region*`:`*account-id* `:thingtype/` *thing-type-name* |
| IoT: DescribeAuthorizer | DescribeAuthorizer | `arn:aws:iot:` *region*`:`*account-id* `:authorizer/` *authorizer-function-name*<br><br>(Parameter: authorizerName)<br>Keine |
| IoT: BeschreibenCACertificate | BeschreibenCACertificate | `arn:aws:iot:` *region*`:`*account-id* `:cacert/`*cert-id* |
| IoT: DescribeCertificate | DescribeCertificate | `arn:aws:iot:` *region*`:`*account-id* `:cert/`*cert-id* |
| IoT: DescribeDefaultAuthorizer | DescribeDefaultAuthorizer | Keine |
| IoT: DescribeEndpoint | DescribeEndpoint | * |
| IoT: DescribeEventConfigurations | DescribeEventConfigurations | Keine |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: DescribeIndex | DescribeIndex | arn:aws:iot: *region*:*account-id* :index/*index-name* |
| IoT: DescribeJob | DescribeJob | arn:aws:iot: *region*:*account-id* :job/*job-id* |
| IoT: DescribeJobExecution | DescribeJobExecution | Keine |
| IoT: DescribeJobTemplate | DescribeJobTemplate | arn:aws:iot: *region*:*account-id* :jobtemplate/ *job-template-id* |
| IoT: DescribeRoleAlias | DescribeRoleAlias | arn:aws:iot: *region*:*account-id* :rolealias/ *role-alias-name* |
| IoT: DescribeThing | DescribeThing | arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: DescribeThingGroup | DescribeThingGroup | arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name* |
| IoT: DescribeThingRegistrationTask | DescribeThingRegistrationTask | Keine |
| IoT: DescribeThingType | DescribeThingType | arn:aws:iot: *region*:*account-id* :thingtype/ *thing-type-name* |
| IoT: DetachPolicy | DetachPolicy | arn:aws:iot: *region*:*account-id* :cert/*cert-id*<br><br>or<br><br>arn:aws:iot: *region*:*account-id* :thinggroup/ *thing-group-name* |
| IoT: DetachPrincipalPolicy | DetachPrincipalPolicy | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: DetachThingPrincipal | DetachThingPrincipal | `arn:aws:iot:` *region*`:`*account-id* `:cert/`*cert-id* |
| IoT: DisableTopicRule | DisableTopicRule | `arn:aws:iot:` *region*`:`*account-id* `:rule/`*rule-name* |
| IoT: EnableTopicRule | EnableTopicRule | `arn:aws:iot:` *region*`:`*account-id* `:rule/`*rule-name* |
| IoT: GetEffectivePolicies | GetEffectivePolicies | `arn:aws:iot:` *region*`:`*account-id* `:cert/`*cert-id* |
| IoT: GetIndexingConfiguration | GetIndexingConfiguration | Keine |
| IoT: GetJobDocument | GetJobDocument | `arn:aws:iot:` *region*`:`*account-id* `:job/`*job-id* |
| IoT: GetLoggingOptions | GetLoggingOptions | * |
| IoT: GetPolicy | GetPolicy | `arn:aws:iot:` *region*`:`*account-id* `:policy/`*policy-name* |
| IoT: GetPolicyVersion | GetPolicyVersion | `arn:aws:iot:` *region*`:`*account-id* `:policy/`*policy-name* |
| IoT: GetRegistrationCode | GetRegistrationCode | * |
| IoT: GetTopicRule | GetTopicRule | `arn:aws:iot:` *region*`:`*account-id* `:rule/`*rule-name* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: ListAttachedPolicies | ListAttachedPolicies | `arn:aws:iot:` *`region`*`:`*`account-id`* `:thinggroup/`*`thing-group-name`*<br>or<br>`arn:aws:iot:` *`region`*`:`*`account-id`* `:cert/`*`cert-id`* |
| IoT: ListAuthorizers | ListAuthorizers | Keine |
| IoT: ListCACertificates | ListCACertificates | * |
| IoT: ListCertificates | ListCertificates | * |
| IoT: ListCertificatesByKanada | ListCertificatesByCA | * |
| IoT: ListIndices | ListIndices | Keine |
| IoT: ListJobExecutionsForJob | ListJobExecutionsForJob | Keine |
| IoT: ListJobExecutionsForThing | ListJobExecutionsForThing | Keine |
| IoT: ListJobs | ListJobs | `arn:aws:iot:` *`region`*`:`*`account-id`* `:thinggroup/`*`thing-group-name`*<br>wenn der thingGroupName Parameter verwendet wird |
| iot: ListJobTemplates | ListJobTemplates | Keine |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: ListOutgoingCertificates | ListOutgoingCertificates | * |
| IoT: ListPolicies | ListPolicies | * |
| IoT: ListPolicyPrincipals | ListPolicyPrincipals | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: ListPolicyVersions | ListPolicyVersions | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: ListPrincipalPolicies | ListPrincipalPolicies | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |
| IoT: ListPrincipalThings | ListPrincipalThings | arn:aws:iot: *region*:*account-id* :cert/*cert-id* |
| IoT: ListRoleAliases | ListRoleAliases | Keine |
| IoT: ListTargetsForPolicy | ListTargetsForPolicy | arn:aws:iot: *region*:*account-id* :policy/*policy-name* |
| IoT: ListThingGroups | ListThingGroups | Keine |
| IoT: ListThingGroupsForThing | ListThingGroupsForThing | arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: ListThingPrincipals | ListThingPrincipals | arn:aws:iot: *region*:*account-id* :thing/*thing-name* |
| IoT: ListThingRegistrationTaskReports | ListThingRegistrationTaskReports | Keine |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: ListThingRegistrationTasks | ListThingRegistrationTasks | Keine |
| IoT: ListThingTypes | ListThingTypes | * |
| IoT: ListThings | ListThings | * |
| IoT: ListThingsInThingGroup | ListThingsInThingGroup | `arn:aws:iot:` *`region`*`:`*`account-id`* `:thinggroup/` *`thing-group-name`* |
| IoT: ListTopicRules | ListTopicRules | * |
| IoT: ListV2LoggingLevels | ListV2LoggingLevels | Keine |
| IoT: registrierenCACertificate | RegistrierenCACertificate | * |
| IoT: RegisterCertificate | RegisterCertificate | * |
| IoT: RegisterThing | RegisterThing | Keine |
| IoT: RejectCertificateTransfer | RejectCertificateTransfer | `arn:aws:iot:` *`region`*`:`*`account-id`* `:cert/`*`cert-id`* |
| IoT: RemoveThingFromThingGroup | RemoveThingFromThingGroup | `arn:aws:iot:` *`region`*`:`*`account-id`* `:thinggroup/` *`thing-group-name`*<br><br>`arn:aws:iot:` *`region`*`:`*`account-id`* `:thing/`*`thing-name`* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: ReplaceTopicRule | ReplaceTopicRule | `arn:aws:iot:` *region*`:`*account-id* `:rule/`*rule-name* |
| IoT: SearchIndex | SearchIndex | `arn:aws:iot:` *region*`:`*account-id* `:index/`*index-id* |
| IoT: SetDefaultAuthorizer | SetDefaultAuthorizer | `arn:aws:iot:` *region*`:`*account-id* `:authorizer/` *authorizer-function-name* |
| IoT: SetDefaultPolicyVersion | SetDefaultPolicyVersion | `arn:aws:iot:` *region*`:`*account-id* `:policy/`*policy-name* |
| IoT: SetLoggingOptions | SetLoggingOptions | * |
| IoT: SETv2LoggingLevel | SETv2LoggingLevel | * |
| IoT: SETV2LoggingOptions | SETv2LoggingOptions | * |
| IoT: StartThingRegistrationTask | StartThingRegistrationTask | Keine |
| IoT: StopThingRegistrationTask | StopThingRegistrationTask | Keine |
| IoT: TestAuthorization | TestAuthorization | `arn:aws:iot:` *region*`:`*account-id* `:cert/`*cert-id* |
| IoT: TestInvokeAuthorizer | TestInvokeAuthorizer | Keine |
| IoT: TransferCertificate | TransferCertificate | `arn:aws:iot:` *region*`:`*account-id* `:cert/`*cert-id* |

| Richtlinienaktionen | AWS IoT API | Ressourcen |
| --- | --- | --- |
| IoT: UpdateAuthorizer | UpdateAuthorizer | `arn:aws:iot:region:account-id :authorizerfunction/ authorizer-function-name` |
| IoT: aktualisierenCACertificate | AktualisierenCACertificate | `arn:aws:iot:region:account-id :cacert/cert-id` |
| IoT: UpdateCertificate | UpdateCertificate | `arn:aws:iot:region:account-id :cert/cert-id` |
| IoT: UpdateEventConfigurations | UpdateEventConfigurations | Keine |
| IoT: UpdateIndexingConfiguration | UpdateIndexingConfiguration | Keine |
| IoT: UpdateRoleAlias | UpdateRoleAlias | `arn:aws:iot:region:account-id :rolealias/ role-alias-name` |
| IoT: UpdateThing | UpdateThing | `arn:aws:iot:region:account-id :thing/thing-name` |
| IoT: UpdateThingGroup | UpdateThingGroup | `arn:aws:iot:region:account-id :thinggroup/ thing-group-name` |
| IoT: UpdateThingGroupsForThing | UpdateThingGroupsForThing | `arn:aws:iot:region:account-id :thing/thing-name` |

Weitere Informationen zum Format von ARNs finden Sie unter Amazon Resource Names (ARNs) und AWS Service Namespaces.

Einige AWS IoT Aktionen, wie z. B. die zum Erstellen von Ressourcen, können nicht für eine bestimmte Ressource ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

```
"Resource": "*"
```

Eine Liste der AWS IoT Ressourcentypen und ihrer ARNs Eigenschaften finden Sie AWS IoT im IAM-Benutzerhandbuch unter Defined by (Ressourcen definiert von). Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS IoT definierte Aktionen.

Device-Advisor-Ressourcen

Verwenden Sie die folgenden Ressourcen-ARN-Formate für Suite-Definitionen und Suite-Läufe, um Einschränkungen auf Ressourcenebene für AWS IoT Device Advisor IAM-Richtlinien zu definieren.

ARN–Format der Suite-Definitionsressource

```
arn:aws:iotdeviceadvisor:region:account-id:suitedefinition/suite-definition-id
```

ARN–Format der Suite-Ausführungsressource

```
arn:aws:iotdeviceadvisor:region:account-id:suiterun/suite-definition-id/suite-run-id
```

Bedingungsschlüssel

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann

gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

AWS IoT definiert seinen eigenen Satz von Bedingungsschlüsseln und unterstützt auch die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

AWS IoT Bedingungsschlüssel

| AWS IoT Zustandsschlüssel | Beschreibung | Typ |
|---|---|---|
| `aws:RequestTag/${tag-key}` | Ein Tag-Schlüssel, der in der Anforderung vorhanden ist, die der Benutzer an AWS IoT stellt. | String |
| `aws:ResourceTag/${tag-key}` | Die Schlüsselkomponente eines Tags, das an eine AWS IoT Ressource angehängt ist. | String |
| `aws:TagKeys` | Liste aller Tag-Schlüsselnamen, die der Ressource in der Anforderung zugeordnet sind | String |

Eine Liste der AWS IoT Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS IoT im IAM-Benutzerhandbuch. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Definierte Aktionen von AWS IoT.

Beispiele

Beispiele für AWS IoT identitätsbasierte Richtlinien finden Sie unter. AWS IoT Beispiele für identitätsbasierte Richtlinien

## Ressourcenbasierte AWS IoT -Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die angeben, welche Aktionen ein bestimmter Principal unter welchen Bedingungen auf der AWS IoT Ressource ausführen kann.

AWS IoT unterstützt keine ressourcenbasierten IAM-Richtlinien. Es unterstützt AWS IoT jedoch ressourcenbasierte Richtlinien. Weitere Informationen finden Sie unter AWS IoT Core Richtlinien.

## Autorisierung auf der Basis von AWS IoT -Tags

Sie können Tags an AWS IoT Ressourcen anhängen oder Tags in einer Anfrage an übergeben. AWS IoT Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `iot:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden. Weitere Informationen finden Sie unter Verwenden von Tags mit IAM-Richtlinien. Weitere Informationen zum Markieren von AWS IoT Ressourcen finden Sie unterVerschlagworten Sie Ihre Ressourcen AWS IoT.

Ein Beispiel für eine identitätsbasierte Richtlinie zur Einschränkung des Zugriffs auf eine Ressource auf der Grundlage der Markierungen dieser Ressource finden Sie unter Anzeigen von AWS IoT - Ressourcen basierend auf Tags.

## AWS IoT IAM-Rollen

Eine IAM-Rolle ist eine Entität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt.

Verwenden temporärer Anmeldeinformationen mit AWS IoT

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie AssumeRoleoder aufrufen GetFederationToken.

AWS IoT unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit dienstbezogenen Rollen können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

AWS IoT unterstützt keine dienstbezogenen Rollen.

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

## AWS IoT Beispiele für identitätsbasierte Richtlinien

IAM-Benutzer besitzen keine Berechtigungen zum Erstellen oder Ändern von AWS IoT -Ressourcen. Sie können auch keine Aufgaben mit der AWS Management Console AWS CLI, oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den -Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der AWS IoT -Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Anzeigen von AWS IoT -Ressourcen basierend auf Tags
- AWS IoT Device Advisor-Ressourcen anhand von Stichwörtern anzeigen

## Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS IoT Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

## Verwenden der AWS IoT -Konsole

Um auf die AWS IoT Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS IoT Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Um sicherzustellen, dass diese Entitäten die AWS IoT Konsole weiterhin verwenden können, fügen Sie den Entitäten außerdem die folgende AWS verwaltete Richtlinie hinzu:`AWSIoTFullAccess`. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die Sie ausführen möchten.

## Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## Anzeigen von AWS IoT -Ressourcen basierend auf Tags

Sie können in Ihrer identitätsbasierten Richtlinie Bedingungen für die Steuerung des Zugriffs auf AWS IoT -Ressourcen auf der Basis von Tags verwenden. Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen können, die das Anzeigen eines Things ermöglicht. Die Berechtigung wird jedoch nur erteilt, wenn das Things-Tag `Owner` den Wert des Benutzernamens dieses Benutzers hat. Diese Richtlinie gewährt auch die Berechtigungen, die für die Ausführung dieser Aktion auf der Konsole erforderlich sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListBillingGroupsInConsole",
            "Effect": "Allow",
```

```
            "Action": "iot:ListBillingGroups",
            "Resource": "*"
        },
        {
            "Sid": "ViewBillingGroupsIfOwner",
            "Effect": "Allow",
           "Action": "iot:DescribeBillingGroup",
            "Resource": "arn:aws:iot:*:*:billinggroup/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Sie können diese Richtlinie den IAM-Benutzern in Ihrem Konto anfügen. Wenn ein benannter Benutzer `richard-roe` versucht, eine AWS IoT Abrechnungsgruppe aufzurufen, muss die Abrechnungsgruppe mit oder gekennzeichnet `0wner=richard-roe` werden. `owner=richard-roe` Andernfalls wird der Zugriff abgelehnt. Der Tag-Schlüssel `0wner` der Bedingung stimmt sowohl mit `0wner` als auch mit `owner` überein, da die Namen von Bedingungsschlüsseln nicht zwischen Groß- und Kleinschreibung unterscheiden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

## AWS IoT Device Advisor-Ressourcen anhand von Stichwörtern anzeigen

Sie können in Ihrer identitätsbasierten Richtlinie Bedingungen für die Steuerung des Zugriffs auf AWS IoT -Device-Advisor-Ressourcen auf der Basis von Tags verwenden. Im folgenden Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen können, mit der eine bestimmte Suite-Definition angezeigt werden kann. Die Berechtigung wird jedoch nur erteilt, wenn `SuiteType` im Suite-Definitions-Tag auf den Wert von `MQTT` gesetzt ist. Diese Richtlinie gewährt auch die Berechtigungen, die für die Ausführung dieser Aktion auf der Konsole erforderlich sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewSuiteDefinition",
            "Effect": "Allow",
            "Action": "iotdeviceadvisor:GetSuiteDefinition",
            "Resource": "arn:aws:iotdeviceadvisor:*:*:suitedefinition/*",
            "Condition": {
```

```
                "StringEquals": {"aws:ResourceTag/SuiteType": "MQTT"}
            }
        }
    ]
}
```

# AWS verwaltete Richtlinien für AWS IoT

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Service ein neues Feature startet, fügt AWS schreibgeschützte Berechtigungen für neue Vorgänge und Ressourcen hinzu. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

> **Note**
>
> AWS IoT funktioniert sowohl mit IAM-Richtlinien als auch mit AWS IoT IAM-Richtlinien. In diesem Thema werden nur IAM-Richtlinien behandelt, die eine Richtlinienaktion für

API-Operationen auf der Steuer- und Datenebene definieren. Siehe auch AWS IoT Core Richtlinien.

## AWS verwaltete Richtlinie: Zugriff AWSIo TConfig

Sie können die `AWSIoTConfigAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie erteilt die zugehörigen Identitätsberechtigungen, die Zugriff auf alle AWS IoT -Konfigurationsoperationen gewähren. Diese Richtlinie kann sich auf Datenverarbeitung und Speicher auswirken. Informationen zu dieser Richtlinie finden Sie AWS Management Console unter AWSIoTConfigAccess.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `iot`— Rufen Sie AWS IoT Daten ab und führen Sie IoT-Konfigurationsaktionen durch.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:AcceptCertificateTransfer",
                "iot:AddThingToThingGroup",
                "iot:AssociateTargetsWithJob",
                "iot:AttachPolicy",
                "iot:AttachPrincipalPolicy",
                "iot:AttachThingPrincipal",
                "iot:CancelCertificateTransfer",
                "iot:CancelJob",
                "iot:CancelJobExecution",
                "iot:ClearDefaultAuthorizer",
```

```
                "iot:CreateAuthorizer",
                "iot:CreateCertificateFromCsr",
                "iot:CreateJob",
                "iot:CreateKeysAndCertificate",
                "iot:CreateOTAUpdate",
                "iot:CreatePolicy",
                "iot:CreatePolicyVersion",
                "iot:CreateRoleAlias",
                "iot:CreateStream",
                "iot:CreateThing",
                "iot:CreateThingGroup",
                "iot:CreateThingType",
                "iot:CreateTopicRule",
                "iot:DeleteAuthorizer",
                "iot:DeleteCACertificate",
                "iot:DeleteCertificate",
                "iot:DeleteJob",
                "iot:DeleteJobExecution",
                "iot:DeleteOTAUpdate",
                "iot:DeletePolicy",
                "iot:DeletePolicyVersion",
                "iot:DeleteRegistrationCode",
                "iot:DeleteRoleAlias",
                "iot:DeleteStream",
                "iot:DeleteThing",
                "iot:DeleteThingGroup",
                "iot:DeleteThingType",
                "iot:DeleteTopicRule",
                "iot:DeleteV2LoggingLevel",
                "iot:DeprecateThingType",
                "iot:DescribeAuthorizer",
                "iot:DescribeCACertificate",
                "iot:DescribeCertificate",
                "iot:DescribeDefaultAuthorizer",
                "iot:DescribeEndpoint",
                "iot:DescribeEventConfigurations",
                "iot:DescribeIndex",
                "iot:DescribeJob",
                "iot:DescribeJobExecution",
                "iot:DescribeRoleAlias",
                "iot:DescribeStream",
                "iot:DescribeThing",
                "iot:DescribeThingGroup",
                "iot:DescribeThingRegistrationTask",
```

```
                "iot:DescribeThingType",
                "iot:DetachPolicy",
                "iot:DetachPrincipalPolicy",
                "iot:DetachThingPrincipal",
                "iot:DisableTopicRule",
                "iot:EnableTopicRule",
                "iot:GetEffectivePolicies",
                "iot:GetIndexingConfiguration",
                "iot:GetJobDocument",
                "iot:GetLoggingOptions",
                "iot:GetOTAUpdate",
                "iot:GetPolicy",
                "iot:GetPolicyVersion",
                "iot:GetRegistrationCode",
                "iot:GetTopicRule",
                "iot:GetV2LoggingOptions",
                "iot:ListAttachedPolicies",
                "iot:ListAuthorizers",
                "iot:ListCACertificates",
                "iot:ListCertificates",
                "iot:ListCertificatesByCA",
                "iot:ListIndices",
                "iot:ListJobExecutionsForJob",
                "iot:ListJobExecutionsForThing",
                "iot:ListJobs",
                "iot:ListOTAUpdates",
                "iot:ListOutgoingCertificates",
                "iot:ListPolicies",
                "iot:ListPolicyPrincipals",
                "iot:ListPolicyVersions",
                "iot:ListPrincipalPolicies",
                "iot:ListPrincipalThings",
                "iot:ListRoleAliases",
                "iot:ListStreams",
                "iot:ListTargetsForPolicy",
                "iot:ListThingGroups",
                "iot:ListThingGroupsForThing",
                "iot:ListThingPrincipals",
                "iot:ListThingRegistrationTaskReports",
                "iot:ListThingRegistrationTasks",
                "iot:ListThings",
                "iot:ListThingsInThingGroup",
                "iot:ListThingTypes",
                "iot:ListTopicRules",
```

```
                "iot:ListV2LoggingLevels",
                "iot:RegisterCACertificate",
                "iot:RegisterCertificate",
                "iot:RegisterThing",
                "iot:RejectCertificateTransfer",
                "iot:RemoveThingFromThingGroup",
                "iot:ReplaceTopicRule",
                "iot:SearchIndex",
                "iot:SetDefaultAuthorizer",
                "iot:SetDefaultPolicyVersion",
                "iot:SetLoggingOptions",
                "iot:SetV2LoggingLevel",
                "iot:SetV2LoggingOptions",
                "iot:StartThingRegistrationTask",
                "iot:StopThingRegistrationTask",
                "iot:TestAuthorization",
                "iot:TestInvokeAuthorizer",
                "iot:TransferCertificate",
                "iot:UpdateAuthorizer",
                "iot:UpdateCACertificate",
                "iot:UpdateCertificate",
                "iot:UpdateEventConfigurations",
                "iot:UpdateIndexingConfiguration",
                "iot:UpdateRoleAlias",
                "iot:UpdateStream",
                "iot:UpdateThing",
                "iot:UpdateThingGroup",
                "iot:UpdateThingGroupsForThing",
                "iot:UpdateAccountAuditConfiguration",
                "iot:DescribeAccountAuditConfiguration",
                "iot:DeleteAccountAuditConfiguration",
                "iot:StartOnDemandAuditTask",
                "iot:CancelAuditTask",
                "iot:DescribeAuditTask",
                "iot:ListAuditTasks",
                "iot:CreateScheduledAudit",
                "iot:UpdateScheduledAudit",
                "iot:DeleteScheduledAudit",
                "iot:DescribeScheduledAudit",
                "iot:ListScheduledAudits",
                "iot:ListAuditFindings",
                "iot:CreateSecurityProfile",
                "iot:DescribeSecurityProfile",
                "iot:UpdateSecurityProfile",
```

```
                "iot:DeleteSecurityProfile",
                "iot:AttachSecurityProfile",
                "iot:DetachSecurityProfile",
                "iot:ListSecurityProfiles",
                "iot:ListSecurityProfilesForTarget",
                "iot:ListTargetsForSecurityProfile",
                "iot:ListActiveViolations",
                "iot:ListViolationEvents",
                "iot:ValidateSecurityProfileBehaviors"
            ],
            "Resource": "*"
        }
    ]
}
```

## AWS verwaltete Richtlinie: AWSIo TConfig ReadOnlyAccess

Sie können die `AWSIoTConfigReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie erteilt die zugehörigen Identitätsberechtigungen, die schreibgeschützten Zugriff auf alle AWS IoT -Konfigurationsoperationen gewähren. Informationen zu dieser Richtlinie finden Sie AWS Management Console unter AWSIoTConfigReadOnlyAccess.

### Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `iot`: Führen Sie schreibgeschützte Operationen von IoT-Konfigurationsaktionen durch.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:DescribeAuthorizer",
                "iot:DescribeCACertificate",
                "iot:DescribeCertificate",
```

```
                "iot:DescribeDefaultAuthorizer",
                "iot:DescribeEndpoint",
                "iot:DescribeEventConfigurations",
                "iot:DescribeIndex",
                "iot:DescribeJob",
                "iot:DescribeJobExecution",
                "iot:DescribeRoleAlias",
                "iot:DescribeStream",
                "iot:DescribeThing",
                "iot:DescribeThingGroup",
                "iot:DescribeThingRegistrationTask",
                "iot:DescribeThingType",
                "iot:GetEffectivePolicies",
                "iot:GetIndexingConfiguration",
                "iot:GetJobDocument",
                "iot:GetLoggingOptions",
                "iot:GetOTAUpdate",
                "iot:GetPolicy",
                "iot:GetPolicyVersion",
                "iot:GetRegistrationCode",
                "iot:GetTopicRule",
                "iot:GetV2LoggingOptions",
                "iot:ListAttachedPolicies",
                "iot:ListAuthorizers",
                "iot:ListCACertificates",
                "iot:ListCertificates",
                "iot:ListCertificatesByCA",
                "iot:ListIndices",
                "iot:ListJobExecutionsForJob",
                "iot:ListJobExecutionsForThing",
                "iot:ListJobs",
                "iot:ListOTAUpdates",
                "iot:ListOutgoingCertificates",
                "iot:ListPolicies",
                "iot:ListPolicyPrincipals",
                "iot:ListPolicyVersions",
                "iot:ListPrincipalPolicies",
                "iot:ListPrincipalThings",
                "iot:ListRoleAliases",
                "iot:ListStreams",
                "iot:ListTargetsForPolicy",
                "iot:ListThingGroups",
                "iot:ListThingGroupsForThing",
                "iot:ListThingPrincipals",
```

```
                "iot:ListThingRegistrationTaskReports",
                "iot:ListThingRegistrationTasks",
                "iot:ListThings",
                "iot:ListThingsInThingGroup",
                "iot:ListThingTypes",
                "iot:ListTopicRules",
                "iot:ListV2LoggingLevels",
                "iot:SearchIndex",
                "iot:TestAuthorization",
                "iot:TestInvokeAuthorizer",
                "iot:DescribeAccountAuditConfiguration",
                "iot:DescribeAuditTask",
                "iot:ListAuditTasks",
                "iot:DescribeScheduledAudit",
                "iot:ListScheduledAudits",
                "iot:ListAuditFindings",
                "iot:DescribeSecurityProfile",
                "iot:ListSecurityProfiles",
                "iot:ListSecurityProfilesForTarget",
                "iot:ListTargetsForSecurityProfile",
                "iot:ListActiveViolations",
                "iot:ListViolationEvents",
                "iot:ValidateSecurityProfileBehaviors"
            ],
            "Resource": "*"
        }
    ]
}
```

## AWS verwaltete Richtlinie: AWSIo TData Zugriff

Sie können die `AWSIoTDataAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt den zugehörigen Identitätsberechtigungen, die den Zugriff auf alle AWS IoT Datenoperationen ermöglichen. Bei den Datenoperationen werden Daten über das MQTT- oder HTTP-Protokoll gesendet. Informationen zum Anzeigen dieser Richtlinie in der AWS Management Console finden Sie unter `AWSIoTDataAccess`.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `iot`— Rufen Sie AWS IoT Daten ab und gewähren Sie vollen Zugriff auf AWS IoT Messaging-Aktionen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect",
                "iot:Publish",
                "iot:Subscribe",
                "iot:Receive",
                "iot:GetThingShadow",
                "iot:UpdateThingShadow",
                "iot:DeleteThingShadow",
                "iot:ListNamedShadowsForThing"
            ],
            "Resource": "*"
        }
    ]
}
```

## AWS verwaltete Richtlinie: AWSIo TFull Zugriff

Sie können die `AWSIoTFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie erteilt die zugehörigen Identitätsberechtigungen, die Zugriff auf alle AWS IoT -Konfigurations- und Messaging-Operationen gewähren. Informationen zu dieser Richtlinie finden Sie AWS Management Console unter `AWSIoTFullAccess`.

### Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `iot`— Rufen Sie AWS IoT Daten ab und gewähren Sie vollen Zugriff auf AWS IoT Konfiguration und Nachrichtenaktionen.
- `iotjobsdata`— Rufen Sie AWS IoT Jobs-Daten ab und ermöglichen Sie den vollen Zugriff auf die API-Operationen auf der AWS IoT Jobs-Datenebene.

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

## AWS verwaltete Richtlinie: AWSIo TLogging

Sie können die `AWSIoTLogging`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt die zugehörigen Identitätsberechtigungen, die den Zugriff auf die Erstellung von Amazon CloudWatch Logs-Gruppen und das Streamen von Protokollen an die Gruppen ermöglichen. Diese Richtlinie ist mit Ihrer CloudWatch Logging-Rolle verknüpft. Informationen zu dieser Richtlinie finden Sie AWS Management Console unter `AWSIoTLogging`.

### Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `logs`— CloudWatch Protokolle abrufen. Ermöglicht auch die Erstellung von CloudWatch Protokollgruppen und das Streamen von Protokollen an die Gruppen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutMetricFilter",
                "logs:PutRetentionPolicy",
                "logs:GetLogEvents",
                "logs:DeleteLogStream"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

## AWS verwaltete Richtlinie: AWSIo TOTAUpdate

Sie können die `AWSIoTOTAUpdate`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt die zugehörigen Identitätsberechtigungen, die den Zugriff auf das Erstellen von AWS IoT Aufträgen und das Beschreiben von AWS IoT AWS Codesignaturaufträgen ermöglichen. Informationen zu dieser Richtlinie finden Sie AWS Management Console unter`AWSIoTOTAUpdate`.

### Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `iot`— AWS IoT Jobs und Codesignatur-Jobs erstellen.
- `signer`— Führen Sie die Erstellung von AWS Codesigner-Jobs durch.

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

## AWS verwaltete Richtlinie: Aktionen AWSIo TRule

Sie können die `AWSIoTRuleActions`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt den zugehörigen Identitätsberechtigungen, die den Zugriff auf alle AWS-Service in AWS IoT der Regel unterstützten Aktionen ermöglichen. Informationen zu dieser Richtlinie in der AWS Management Console finden Sie unter `AWSIoTRuleActions`.

### Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `iot`: Führen Sie Aktionen zum Veröffentlichen von Regelaktionsmeldungen durch.
- `dynamodb`: Fügen Sie eine Nachricht in eine DynamoDB-Tabelle ein oder teilen Sie eine Nachricht in mehrere Spalten einer DynamoDB-Tabelle auf.
- `s3`: Speichern Sie ein Objekt zu einem Amazon-S3-Bucket.
- `kinesis`: Senden Sie eine Nachricht an ein Amazon-Kinesis-Streamingobjekt.
- `firehose`- Fügt einen Datensatz in ein Firehose-Stream-Objekt ein.
- `cloudwatch`- Ändern Sie den CloudWatch Alarmstatus oder senden Sie Nachrichtendaten an die CloudWatch Metrik.
- `sns`: Führen Sie die Operation durch, um eine Benachrichtigung mit Amazon SNS zu veröffentlichen. Dieser Vorgang ist auf SNS-Themen beschränkt AWS IoT .

- `sqs`: Fügen Sie eine Nachricht ein, die der SQS-Warteschlange hinzugefügt werden soll.
- `es`- Senden Sie eine Nachricht an den OpenSearch Servicedienst.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "dynamodb:PutItem",
            "kinesis:PutRecord",
            "iot:Publish",
            "s3:PutObject",
            "sns:Publish",
            "sqs:SendMessage*",
            "cloudwatch:SetAlarmState",
            "cloudwatch:PutMetricData",
            "es:ESHttpPut",
            "firehose:PutRecord"
        ],
        "Resource": "*"
    }
}
```

## AWS verwaltete Richtlinie: AWSIo TThings Registrierung

Sie können die `AWSIoTThingsRegistration`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt die zugehörigen Identitätsberechtigungen, die die Massenregistrierung von Objekten mithilfe der `StartThingRegistrationTask`-API ermöglichen. Diese Richtlinie kann sich auf Datenverarbeitung und Speicher auswirken. Informationen zu dieser Richtlinie finden Sie AWS Management Console unter `AWSIoTThingsRegistration`.

### Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `iot`: Führen Sie bei der Massenregistrierung Aktionen zum Erstellen von Objekten und zum Anhängen von Richtlinien und Zertifikaten durch.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:AddThingToThingGroup",
                "iot:AttachPolicy",
                "iot:AttachPrincipalPolicy",
                "iot:AttachThingPrincipal",
                "iot:CreateCertificateFromCsr",
                "iot:CreatePolicy",
                "iot:CreateThing",
                "iot:DescribeCertificate",
                "iot:DescribeThing",
                "iot:DescribeThingGroup",
                "iot:DescribeThingType",
                "iot:DetachPolicy",
                "iot:DetachThingPrincipal",
                "iot:GetPolicy",
                "iot:ListAttachedPolicies",
                "iot:ListPolicyPrincipals",
                "iot:ListPrincipalPolicies",
                "iot:ListPrincipalThings",
                "iot:ListTargetsForPolicy",
                "iot:ListThingGroupsForThing",
                "iot:ListThingPrincipals",
                "iot:RegisterCertificate",
                "iot:RegisterThing",
                "iot:RemoveThingFromThingGroup",
                "iot:UpdateCertificate",
                "iot:UpdateThing",
                "iot:UpdateThingGroupsForThing",
                "iot:AddThingToBillingGroup",
                "iot:DescribeBillingGroup",
                "iot:RemoveThingFromBillingGroup"
            ],
            "Resource": [
                "*"
```

```
            ]
        }
    ]
}
```

## AWS IoT Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AWS IoT seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite AWS IoT Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

| Änderung | Beschreibung | Datum |
| --- | --- | --- |
| AWSIoTFullZugriff — Aktualisierung einer bestehenden Richtlinie | AWS IoT Es wurden neue Berechtigungen hinzugefügt, um Benutzern den Zugriff auf API-Operationen auf AWS IoT Jobs-Datenebene mithilfe des HTTP-Protokolls zu ermöglichen.<br><br>Ein neues IAM-Richtlinienpräfix,`iotjobsdata:` , bietet Ihnen eine detailliertere Zugriffskontrolle für den Zugriff auf Endpunkte der AWS IoT Jobs-Datenebene. Für API-Operationen auf der Steuerebene verwenden Sie weiterhin das Präfix `iot:`. Weitere Informationen finden Sie unter AWS IoT Core Richtlinien für HTTPS das Protokoll. | 11. Mai 2022 |

| Änderung | Beschreibung | Datum |
| --- | --- | --- |
| AWS IoT hat begonnen, Änderungen zu verfolgen | AWS IoT hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen. | 11. Mai 2022 |

# Fehlerbehebung bei AWS IoT Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS IoT und IAM auftreten können.

Themen


- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS IoT
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS IoT Ressourcen ermöglichen


## Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS IoT

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der/die IAM-Benutzer:in `mateojackson` versucht, über die Konsole Details zu einer Objektressource anzuzeigen, jedoch nicht über `iot:DescribeThing`-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iot:DescribeThing on resource: MyIoTThing
```

In diesem Fall muss die Richtlinie für den/die Benutzer:in `mateojackson` aktualisiert werden, damit er/sie mit der `iot:DescribeThing`-Aktion auf die Objektressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Verwenden von AWS IoT Device Advisor

Wenn Sie AWS IoT Device Advisor verwenden, tritt der folgende Beispielfehler auf, wenn der Benutzer `mateojackson` versucht, die Konsole zu verwenden, um Details zu einer Suite-Definition anzuzeigen, aber nicht über die `iotdeviceadvisor:`*`GetSuiteDefinition`* entsprechenden Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iotdeviceadvisor:GetSuiteDefinition on resource: MySuiteDefinition
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `iotdeviceadvisor:`*`GetSuiteDefinition`*-Aktion auf die *`MySuiteDefinition`*-Ressource zugreifen kann.

## Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS IoTübergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS IoT auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

### Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS IoT Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS IoT unterstützt werden, finden Sie unter. Wie AWS IoT funktioniert mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

## Protokollieren und Überwachen

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS IoT AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. Informationen zu Protokollierungs- und Überwachungsverfahren finden Sie unter Überwachung AWS IoT

# Überwachungstools

AWS stellt Tools bereit, die Sie zur Überwachung verwenden können AWS IoT. Sie können einige dieser Tools für die Überwachung konfigurieren. Einige der Tools erfordern manuelle Eingriffe. Wir empfehlen, dass Sie die Überwachungsaufgaben möglichst automatisieren.

## Automatisierte Überwachungstools

Sie können die folgenden automatisierten Überwachungstools verwenden, um zu beobachten AWS IoT und zu melden, wenn etwas nicht stimmt:

- Amazon CloudWatch Alarms — Überwachen Sie eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum und führen Sie eine oder mehrere Aktionen aus, die auf dem Wert der Metrik im Verhältnis zu einem bestimmten Schwellenwert über mehrere Zeiträume basieren. Die Aktion ist eine Benachrichtigung, die an ein Amazon Simple Notification Service (Amazon SNS) -Thema oder eine Amazon EC2 Auto Scaling Scaling-Richtlinie gesendet wird. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Status befinden. Der Status muss sich geändert haben und für eine festgelegte Anzahl an Zeiträumen aufrechterhalten worden sein. Weitere Informationen finden Sie unter Überwachen Sie AWS IoT Alarme und Messwerte mit Amazon CloudWatch.
- Amazon CloudWatch Logs — Überwachen, speichern und greifen Sie auf Ihre Protokolldateien aus AWS CloudTrail oder anderen Quellen zu. Mit Amazon CloudWatch Logs können Sie auch wichtige Schritte, die AWS IoT Device Advisor-Testfälle ausführen, generierte Ereignisse und MQTT-Nachrichten sehen, die von Ihren Geräten oder AWS IoT Core während der Testausführung gesendet wurden. Mit diesen Protokollen können Sie Geräte debuggen und Korrekturmaßnahmen auf Ihren Geräten ergreifen. Weitere Informationen finden Sie unter Überwachung AWS IoT mithilfe von Protokollen CloudWatch Weitere Informationen zur Verwendung von Amazon CloudWatch finden Sie unter Überwachung von Protokolldateien im CloudWatch Amazon-Benutzerhandbuch.
- Amazon CloudWatch Events — Ordnen Sie Ereignisse zu und leiten Sie sie an eine oder mehrere Zielfunktionen oder Streams weiter, um Änderungen vorzunehmen, Statusinformationen zu erfassen und Korrekturmaßnahmen zu ergreifen. Weitere Informationen finden Sie unter Was ist Amazon CloudWatch Events im CloudWatch Amazon-Benutzerhandbuch.
- AWS CloudTrail Protokollüberwachung — Teilen Sie Protokolldateien zwischen Konten, überwachen CloudTrail Sie Protokolldateien in Echtzeit, indem Sie sie an CloudWatch Logs senden, schreiben Sie Protokollverarbeitungsanwendungen in Java und überprüfen Sie, ob sich Ihre Protokolldateien nach der Lieferung von nicht geändert haben CloudTrail. Weitere

Informationen finden Sie unter Protokollieren von AWS IoT API-Aufrufen mit AWS CloudTrail und auch Arbeiten mit CloudTrail Protokolldateien im AWS CloudTrail Benutzerhandbuch.

### Manuelle Überwachungstools

Ein weiterer wichtiger Teil der Überwachung ist AWS IoT die manuelle Überwachung der Elemente, die von den CloudWatch Alarmen nicht abgedeckt werden. Die Dashboards AWS IoT CloudWatch, und andere AWS Servicekonsolen-Dashboards bieten einen at-a-glance Überblick über den Zustand Ihrer AWS Umgebung. Wir empfehlen, dass Sie auch die Protokolldateien unter AWS IoTüberprüfen.

- AWS IoT Das Dashboard zeigt:
  - CA-Zertifikate
  - Zertifikate
  - Richtlinien
  - Regeln
  - Elemente
- CloudWatch Die Startseite zeigt:
  - Aktuelle Alarme und Status.
  - Diagramme mit Alarmen und Ressourcen.
  - Servicestatus.

  Sie können verwenden CloudWatch , um Folgendes zu tun:
  - Erstellen von benutzerdefinierten Dashboards zur Überwachung des gewünschten Services.
  - Aufzeichnen von Metrikdaten, um Probleme zu beheben und Trends zu erkennen.
  - Suchen und durchsuchen Sie alle Ihre AWS Ressourcenmetriken.
  - Erstellen und Bearbeiten von Alarmen, um über Probleme benachrichtigt zu werden.

## Überprüfung der Einhaltung der Vorschriften für AWS IoT Core

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.

- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

## Resilienz im AWS IoT-Kern

Die AWS globale Infrastruktur basiert auf AWS-Region s und Availability Zones. AWS-Region s bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS-Region s und Availability Zones finden Sie unter AWS Globale Infrastruktur.

AWS IoT Core speichert Informationen zu Ihren Geräten in der Geräteregistrierung. Der Service speichert auch CA-Zertifikate, Gerätezertifikate und Geräteschattendaten. Diese Daten werden bei Hardware- oder Netzwerkausfällen automatisch in Availability Zones, nicht jedoch in Regionen repliziert.

AWS IoT Core veröffentlicht MQTT-Ereignisse, wenn die Geräteregistrierung aktualisiert wird. Sie können diese Nachrichten verwenden, um Ihre Registrierungsdaten zu sichern und sie irgendwo zu speichern (z. B. in einer DynamoDB-Tabelle). Sie sind dafür verantwortlich, Zertifikate zu speichern, AWS IoT Core die Sie für Sie oder die Sie selbst erstellen. Device Shadow speichert Statusdaten zu Ihren Geräten und kann erneut gesendet werden, wenn ein Gerät wieder online ist. AWS IoT Device Advisor speichert Informationen über Ihre Testsuite-Konfiguration. Diese Daten werden bei Hardware- oder Netzwerkausfällen automatisch repliziert.

AWS IoT Core Ressourcen sind regionsspezifisch und werden nur dann repliziert, AWS-Regionen wenn Sie dies ausdrücklich tun.

Weitere Informationen zu bewährten Methoden für die Sicherheit finden Sie unter Bewährte Sicherheitsmethoden in AWS IoT Core.

# Verwendung AWS IoT Core mit VPC-Endpunkten mit Schnittstelle

Mit AWS IoT Core können Sie IoT-Datenendpunkte in Ihrer Virtual Private Cloud (VPC) mithilfe von Schnittstellen-VPC-Endpunkten erstellen. Schnittstellen-VPC-Endpoints basieren auf einer AWS Technologie AWS PrivateLink, mit der Sie mithilfe AWS von privaten IP-Adressen auf Dienste zugreifen können, auf denen sie ausgeführt werden. Weitere Informationen finden Sie unter Amazon Virtual Private Cloud.

Informationen zum Verbinden von Geräten vor Ort in Remote-Netzwerken, z. B. einem Unternehmensnetzwerk, mit Ihrer Amazon VPC, finden Sie in den Optionen, die in der Network-to-Amazon VPC-Konnektivitätsmatrix aufgeführt sind.

Inhalt


- VPC-Endpunkte für AWS IoT Core die Datenebene erstellen
- Erstellen von VPC-Endpunkten für den AWS IoT Core -Anmeldeinformationsanbieter
- Erstellen eines Amazon-VPC-Schnittstellenendpunkts
- Konfigurieren einer privat gehosteten Zone
- Steuerung des Zugriffs auf AWS IoT Core über VPC-Endpunkte
- Einschränkungen
- Skalierung von VPC-Endpunkten mit AWS IoT Core
- Verwenden von benutzerdefinierten Domains mit VPC-Endpunkten
- Verfügbarkeit von VPC-Endpunkten für AWS IoT Core


## VPC-Endpunkte für AWS IoT Core die Datenebene erstellen

Sie können einen VPC-Endpunkt für die AWS IoT Core Datenebene-API erstellen, um Ihre Geräte mit AWS IoT Diensten und anderen AWS Diensten zu verbinden. Um mit VPC-Endpunkten zu beginnen, erstellen Sie einen VPC-Schnittstellen-Endpunkt und wählen Sie ihn AWS IoT Core als Dienst aus. AWS Wenn Sie die CLI verwenden, rufen Sie zuerst an, describe-vpc-endpoint-servicesum sicherzustellen, dass Sie eine Availability Zone auswählen, die in Ihrer Region vorhanden AWS IoT Core ist AWS-Region. In us-east-1 sähe dieser Befehl zum Beispiel wie folgt aus:

```
aws ec2 describe-vpc-endpoint-services --service-name com.amazonaws.us-east-1.iot.data
```

> **Note**
>
> Die VPC-Funktion zum automatischen Erstellen eines DNS-Eintrags ist deaktiviert. Erstellen Sie manuell einen privaten DNS-Eintrag, um eine Verbindung zu diesen Endpunkten herzustellen. Weitere Informationen über DNA-Einträge von privaten VPC finden Sie unter Private DNS für Schnittstellenendpunkte. Weitere Informationen zu AWS IoT Core VPC-Einschränkungen finden Sie unterEinschränkungen.

So verbinden Sie MQTT-Clients mit den VPC-Endpunktschnittstellen:

- Sie müssen manuell DNS-Einträge in einer privat gehosteten Zone erstellen, die an Ihre VPC angehängt ist. Informationen zu den ersten Schritten finden Sie unter Erstellen einer privat gehosteten Zone.

- Erstellen Sie in Ihrer privaten gehosteten Zone einen Alias-Datensatz für jede IP-Adresse der elastischen Netzwerkschnittstelle für den VPC-Endpunkt. Wenn Sie mehrere Netzwerkschnittstellen IPs für mehrere VPC-Endpunkte haben, erstellen Sie gewichtete DNS-Einträge mit gleicher Gewichtung für alle gewichteten Datensätze. Diese IP-Adressen sind im DescribeNetworkInterfacesAPI-Aufruf verfügbar, wenn sie nach der VPC-Endpunkt-ID im Beschreibungsfeld gefiltert werden.

Sehen Sie sich die detaillierten Anweisungen unten an, um einen Amazon VPC-Schnittstellenendpunkt zu erstellen und eine private gehostete Zone für die AWS IoT Core Datenebene zu konfigurieren.

## Erstellen von VPC-Endpunkten für den AWS IoT Core - Anmeldeinformationsanbieter

Sie können einen VPC-Endpunkt für den AWS IoT Core Anmeldeinformationsanbieter erstellen, um Geräte mithilfe der auf Client-Zertifikaten basierenden Authentifizierung zu verbinden und temporäre AWS Anmeldeinformationen im AWS Signature Version 4-Format abzurufen. Um mit VPC-Endpunkten für AWS IoT Core Credential Provider zu beginnen, führen Sie den create-vpc-endpointCLI-Befehl aus, um einen VPC-Schnittstellen-Endpunkt zu erstellen, und wählen Sie AWS IoT Core Credential Provider als Dienst aus. AWS Um sicherzustellen, dass Sie eine Availability Zone auswählen, in der sich Ihre Availability Zone AWS IoT Core befindet AWS-Region, führen

Sie zunächst den Befehl aus. describe-vpc-endpoint-services In us-east-1 sähe dieser Befehl zum Beispiel wie folgt aus:

```
aws ec2 describe-vpc-endpoint-services --service-name com.amazonaws.us-
east-1.iot.credentials
```

> **Note**
>
> Die VPC-Funktion zum automatischen Erstellen eines DNS-Eintrags ist deaktiviert. Erstellen Sie manuell einen privaten DNS-Eintrag, um eine Verbindung zu diesen Endpunkten herzustellen. Weitere Informationen über DNA-Einträge von privaten VPC finden Sie unter Private DNS für Schnittstellenendpunkte. Weitere Informationen zu AWS IoT Core VPC-Einschränkungen finden Sie unterEinschränkungen.

So verbinden Sie HTTP-Clients mit den VPC-Endpunktschnittstellen:

- Sie müssen manuell DNS-Einträge in einer privat gehosteten Zone erstellen, die an Ihre VPC angehängt ist. Informationen zu den ersten Schritten finden Sie unter Eine private gehostete Zone erstellen.

- Erstellen Sie in Ihrer privaten gehosteten Zone einen Alias-Datensatz für jede IP-Adresse der elastischen Netzwerkschnittstelle für den VPC-Endpunkt. Wenn Sie mehrere Netzwerkschnittstellen IPs für mehrere VPC-Endpunkte haben, erstellen Sie gewichtete DNS-Einträge mit gleicher Gewichtung für alle gewichteten Datensätze. Diese IP-Adressen sind im DescribeNetworkInterfacesAPI-Aufruf verfügbar, wenn sie nach der VPC-Endpunkt-ID im Beschreibungsfeld gefiltert werden.

Sehen Sie sich die detaillierten Anweisungen unten an, um einen Amazon VPC-Schnittstellenendpunkt zu erstellen und eine private gehostete Zone für den AWS IoT Core Anmeldeinformationsanbieter zu konfigurieren.

## Erstellen eines Amazon-VPC-Schnittstellenendpunkts

Sie können einen VPC-Schnittstellen-Endpunkt erstellen, um eine Verbindung zu AWS Diensten herzustellen, von AWS PrivateLink denen unterstützt wird. Gehen Sie wie folgt vor, um einen VPC-Schnittstellen-Endpunkt zu erstellen, der eine Verbindung zur AWS IoT Core Datenebene oder

zum AWS IoT Core Anmeldeinformationsanbieter herstellt. Weitere Informationen finden Sie unter Zugreifen auf einen AWS Dienst über einen Schnittstellen-VPC-Endpunkt.

> **Note**
>
> Die Prozesse zum Erstellen eines Amazon VPC-Schnittstellenendpunkts für AWS IoT Core Datenebene und AWS IoT Core Anmeldeinformationsanbieter sind ähnlich, aber Sie müssen endpunktspezifische Änderungen vornehmen, damit die Verbindung funktioniert.

So erstellen Sie einen Schnittstellen-VPC-Endpunkt mit der VPC-Endpunkte-Konsole

1. Navigieren Sie zur VPC-Endpunkte-Konsole, wählen Sie im linken Menü unter Virtual Private Cloud die Option Endpunkte und dann Endpunkt erstellen aus.
2. Geben Sie auf der Seite Endpunkt erstellen die folgenden Informationen an:
   - Wählen Sie AWS-Service s als Servicekategorie aus.
   - Suchen Sie nach dem Servicenamen, indem Sie das Schlüsselwort `iot` eingeben. Wählen Sie in der Liste der angezeigten `iot`-Services den Endpunkt aus.

     Wenn Sie einen VPC-Endpunkt für die AWS IoT Core Datenebene erstellen, wählen Sie den AWS IoT Core Datenebenen-API-Endpunkt für Ihre Region aus. Der Endpunkt wird das Format `com.amazonaws.`*`region`*`.iot.data` haben.

     Wenn Sie einen VPC-Endpunkt für den AWS IoT Core Credential Provider erstellen, wählen Sie den AWS IoT Core Credential Provider-Endpunkt für Ihre Region aus. Der Endpunkt wird das Format `com.amazonaws.`*`region`*`.iot.credentials` haben.

     > **Note**
     >
     > Der Dienstname für die AWS IoT Core Datenebene in der Region China wird das folgende Format haben`cn.com.amazonaws.`*`region`*`.iot.data`. Das Erstellen von VPC-Endpunkten für den AWS IoT Core Anmeldeinformationsanbieter wird in der Region China nicht unterstützt.

   - Wählen Sie für VPC und Subnetze die VPC aus, in der Sie den Endpunkt erstellen möchten, und die Availability Zones (AZs), in denen Sie das Endpunktnetzwerk erstellen möchten.

- Wählen Sie für DNS-Namen aktivieren die Option Für diesen Endpunkt aktivieren. Weder die AWS IoT Core Datenebene noch der AWS IoT Core Anmeldeinformationsanbieter unterstützen bisher private DNS-Namen.
- Wählen Sie für Sicherheitsgruppe die Sicherheitsgruppen aus, die Sie den Endpunktnetzwerkschnittstellen zuordnen möchten.
- Optional können Sie Tags hinzufügen oder entfernen. Tags sind Name-Wert-Paare, die Sie verwenden, um sie Ihrem Endpunkt zuzuordnen.

3. Wählen Sie VPC-Endpunkt erstellen, um den Schnittstellenendpunkt zu erstellen.

Nachdem Sie den AWS PrivateLink Endpunkt erstellt haben, sehen Sie auf der Registerkarte „Details“ Ihres Endpunkts eine Liste mit DNS-Namen. Sie können einen dieser DNS-Namen verwenden, die Sie in diesem Abschnitt erstellt haben, um Ihre private gehostete Zone zu konfigurieren.

## Konfigurieren einer privat gehosteten Zone

Sie können einen dieser DNS-Namen verwenden, die Sie im vorigen Abschnitt erstellt haben, um Ihre private gehostete Zone zu konfigurieren.

Für die AWS IoT Core Datenebene

Der DNS-Name muss der Name Ihrer Domainkonfiguration oder Ihr `IoT:Data-ATS`-Endpunkt sein. Ein mögliches Beispiel für einen DNS-Namen ist: *`xxx`*`-ats.data.iot.`*`region`*`.amazonaws.com`.

Für den AWS IoT Core Anbieter von Anmeldeinformationen

Der DNS-Name muss Ihr `iot:CredentialProvider`-Endpunkt sein. Ein möglicher DNS-Name ist: *`xxxx`*`.credentials.iot.`*`region`*`.amazonaws.com`.

> **Note**
>
> Die Verfahren zur Konfiguration der privaten gehosteten Zone für die AWS IoT Core Datenebene und den AWS IoT Core Anmeldeinformationsanbieter sind ähnlich, aber Sie müssen endpunktspezifische Änderungen vornehmen, damit die Verbindung funktioniert.

### Erstellen einer privaten gehosteten Zone

So erstellen Sie eine privat gehostete Zone mit der Route-53-Konsole

1. Navigieren Sie zur Konsole Route 53 Gehostete Zonen und wählen Sie Gehostete Zone erstellen.
2. Geben Sie auf der Seite Gehostete Zone erstellen die folgenden Informationen an.
   - Geben Sie Domainname die Endpunktadresse für Ihren `iot:Data-ATS` oder `iot:CredentialProvider`-Endpunkt ein. Der folgende AWS -CLI-Befehl zeigt, wie der Endpunkt über ein öffentliches Netzwerk abgerufen wird: `aws iot describe-endpoint --endpoint-type iot:Data-ATS` oder `aws iot describe-endpoint --endpoint-type iot:CredentialProvider`.

     > **Note**
     >
     > Wenn Sie benutzerdefinierte Domains verwenden, finden Sie weitere Informationen unter Verwenden von benutzerdefinierten Domains mit VPC-Endpunkten. Benutzerdefinierte Domänen werden für den AWS IoT Core Anmeldeinformationsanbieter nicht unterstützt.

   - Wählen Sie in der Liste Typ die Option Privat gehostete Zone.
   - Optional können Sie Tags hinzufügen oder entfernen, um sie Ihrer gehosteten Zone zuzuordnen.
3. Wählen Sie Gehostete Zone erstellen, um Ihre private gehostete Zone zu erstellen.

Weitere Informationen finden Sie unter Erstellen einer privat gehosteten Zone.

## Erstellen eines Datensatzes

Nachdem Sie eine private gehostete Zone eingerichtet haben, können Sie einen Eintrag erstellen, der dem DNS mitteilt, wie der Datenverkehr zu dieser Domain weitergeleitet werden soll.

So erstellen Sie einen Datensatz

1. Klicken Sie in der angezeigten Liste der gehosteten Zonen auf die privat gehostete Zone aus, die Sie zuvor erstellt haben, und wählen Sie Datensatz erstellen.
2. Erstellen Sie den Datensatz mithilfe des Assistenten. Wenn Ihnen in der Konsole die Methode Schnelle Erstellung angezeigt wird, wählen Sie Zum Assistenten wechseln aus.
3. Wählen Sie Einfaches Routing für Routing-Richtlinie und klicken Sie auf Weiter.
4. Wählen Sie unter Datensätze konfigurieren die Option Einfachen Datensatz definieren.
5. Gehen Sie auf der Seite Einfachen Datensatz definieren wie folgt vor:

- Geben Sie als Datensatzname `iot:Data-ATS`-Endpunkt oder `iot:CredentialProvider`-Endpunkt ein. Dieser muss mit dem Namen der privaten gehosteten Zone übereinstimmen.
- Behalten Sie für Datensatztyp den Wert `A - Routes traffic to an IPv4 address and some AWS resources` bei.
- Wählen Sie unter Wert/Weiterleiten von Datenverkehr an die Option Alias zu VPC-Endpunkt. Wählen Sie wie unter ??? beschrieben Ihre Region und dann den Endpunkt aus, den Sie zuvor erstellt haben, aus der angezeigten Liste der Endpunkte aus.

6. Wählen Sie Einfachen Datensatz definieren, um Ihren Datensatz zu erstellen.

## Steuerung des Zugriffs auf AWS IoT Core über VPC-Endpunkte

Sie können den Gerätezugriff so einschränken, dass er nur über AWS IoT Core den VPC-Endpunkt erlaubt ist, indem Sie VPC-Bedingungskontextschlüssel verwenden. AWS IoT Core unterstützt die folgenden VPC-bezogenen Kontextschlüssel:

- SourceVpc
- SourceVpce
- VPCSourceIp

> **Note**
>
> AWS IoT Core unterstützt keine Endpunktrichtlinien für VPC-Endpunkte.

Die folgende Richtlinie gewährt beispielsweise die Erlaubnis, eine Verbindung AWS IoT Core mit einer Client-ID herzustellen, die dem Ding-Namen entspricht, und die Veröffentlichung zu einem beliebigen Thema mit dem Ding-Namen, vorausgesetzt, dass das Gerät eine Verbindung zu einem VPC-Endpunkt mit einer bestimmten VPC-Endpunkt-ID herstellt. Diese Richtlinie verweigert Verbindungsversuche zu Ihrem öffentlichen IoT-Datenendpunkt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/
${iot:Connection.Thing.ThingName}"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceVpce": "vpce-1a2b3c4d"
                }
            }

        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/
${iot:Connection.Thing.ThingName}/*"
            ]
        }
    ]
}
```

## Einschränkungen

VPC-Endpunkte werden derzeit nur für AWS IoT Core -Datenendpunkte und Endpunkte von AWS IoT Core -Anmeldeinformationsanbietern unterstützt. VPC-Endpunkte werden für FIPS-Endpunkte (Federal Information Processing Standard) nicht unterstützt.

### Einschränkungen von VPC-Endpunkten für IoT-Daten

In diesem Abschnitt werden die Einschränkungen von VPC-Endpunkten für IoT-Daten behandelt.

- Die Keep-Alive-Zeiträume von MQTT sind auf 230 Sekunden begrenzt. Längere Keep-Alive-Zeiträume werden automatisch auf 230 Sekunden reduziert.
- Jeder VPC-Endpunkt unterstützt insgesamt 100.000 gleichzeitig verbundene Geräte. Wenn Sie mehr Verbindungen benötigen, finden Sie weitere Informationen unter Skalierung von VPC-Endpunkten mit AWS IoT Core.

- VPC-Endpunkte unterstützen nur IPv4 Datenverkehr.
- VPC-Endpunkte stellen nur ATS-Zertifikate bereit, mit Ausnahme von benutzerdefinierten Domains.
- VPC-Endpunktrichtlinien werden nicht unterstützt.
- Für VPC-Endpoints, die für die AWS IoT Core Datenebene erstellt wurden, unterstützt AWS IoT Core nicht die Verwendung zonaler oder regionaler öffentlicher DNS-Einträge.

### Einschränkungen der Endpunkte von Anmeldeinformationsanbietern

In diesem Abschnitt werden die Einschränkungen von VPC-Endpunkten für Anmeldeinformationsanbieter behandelt.

- VPC-Endpunkte unterstützen nur IPv4 Datenverkehr.
- VPC-Endpunkte stellen nur ATS-Zertifikate bereit.
- VPC-Endpunktrichtlinien werden nicht unterstützt.
- Benutzerdefinierte Domains werden für die Endpunkte von Anmeldeinformationsanbietern nicht unterstützt.
- Für VPC-Endpoints, die für den AWS IoT Core Anmeldeinformationsanbieter erstellt wurden, unterstützt die Verwendung zonaler oder regionaler öffentlicher DNS-Einträge AWS IoT Core nicht.

## Skalierung von VPC-Endpunkten mit AWS IoT Core

AWS IoT Core Schnittstellen-VPC-Endpunkte sind auf 100.000 verbundene Geräte über einen einzigen Schnittstellenendpunkt begrenzt. Wenn Ihr Anwendungsfall mehr gleichzeitige Verbindungen zum Broker erfordert, empfehlen wir, mehrere VPC-Endpunkte zu verwenden und Ihre Geräte manuell über Ihre Schnittstellenendpunkte zu routen. Achten Sie beim Erstellen von privaten DNS-Datensätzen für die Weiterleitung von Datenverkehr zu Ihren VPC-Endpunkten darauf, so viele gewichtete Datensätze zu erstellen, wie Sie VPC-Endpunkte haben, um den Verkehr auf Ihre verschiedenen Endpunkte zu verteilen.

## Verwenden von benutzerdefinierten Domains mit VPC-Endpunkten

Wenn Sie benutzerdefinierte Domains mit VPC-Endpunkten verwenden möchten, müssen Sie Ihre benutzerdefinierten Domainnameneinträge in einer privaten gehosteten Zone und Routing-Datensätze in Route53 erstellen. Weitere Informationen finden Sie unter Erstellen einer privat gehosteten Zone.

> **Note**
>
> Benutzerdefinierte Domänen werden nur für AWS IoT Core Datenendpunkte unterstützt.

### Verfügbarkeit von VPC-Endpunkten für AWS IoT Core

AWS IoT Core Schnittstellen-VPC-Endpunkte sind in allen AWS IoT Core unterstützten Regionen verfügbar. AWS IoT Core VPC-Schnittstellen-Endpunkte für den AWS IoT Core Anmeldeinformationsanbieter werden in der Region China und nicht unterstützt. AWS GovCloud (US) Regions

## Sicherheit der Infrastruktur in AWS IoT

Als Sammlung verwalteter Services AWS IoT ist sie durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Sie verwenden AWS veröffentlichte API-Aufrufe, um AWS IoT über das Netzwerk darauf zuzugreifen. Clients müssen Transport Layer Security (TLS) 1.2 oder höher unterstützen. Clients müssen außerdem Cipher-Suites mit Perfect Forward Secrecy (PFS) wie Ephemeral Diffie-Hellman (DHE) oder Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) unterstützen. Die meisten modernen Systeme, z. B. Java 7 und höher, unterstützen diese Modi. Weitere Informationen finden Sie unter Transportsicherheit in AWS IoT Core.

Anforderungen müssen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der mit einem IAM-Prinzipal verknüpft ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

## Sicherheitsüberwachung von Produktionsflotten oder Geräten mit Core AWS IoT

IoT-Flotten können aus einer großen Anzahl von Geräten mit unterschiedlichsten Funktionen bestehen, sind langlebig und geografisch verteilt. Aufgrund dieser Merkmale ist die Flotteneinrichtung komplex und fehleranfällig. Und da Geräte bezüglich Rechenleistung, Arbeitsspeicher und Speicherkapazitäten eingeschränkt sind, können Verschlüsselung und andere Formen der Sicherheit auf den Geräten selbst nur limitiert eingesetzt werden. Außerdem verwenden Geräte häufig Software

mit bekannten Schwachstellen. Diese Faktoren machen IoT-Flotten zu einem attraktiven Ziel für Hacker und erschweren die kontinuierliche Sicherung Ihrer Geräteflotte.

AWS IoT Device Defender begegnet diesen Herausforderungen durch die Bereitstellung von Tools zur Identifizierung von Sicherheitsproblemen und Abweichungen von bewährten Verfahren. Sie können AWS IoT Device Defender verwenden, um verbundene Geräte zu analysieren, zu prüfen und zu überwachen, um ungewöhnliches Verhalten zu erkennen und Sicherheitsrisiken zu minimieren. AWS IoT Device Defender kann Geräteflotten überprüfen, um sicherzustellen, dass sie sich an bewährte Sicherheitsmethoden halten, und um abnormales Verhalten auf Geräten zu erkennen. Auf diese Weise können Sie einheitliche Sicherheitsrichtlinien für Ihre gesamte AWS IoT Geräteflotte durchsetzen und schnell reagieren, wenn Geräte kompromittiert werden. Weitere Informationen finden Sie unter AWS IoT Device Defender.

AWS IoT Device Advisor veröffentlicht Updates und Patches für Ihre Flotte nach Bedarf. AWS IoT Device Advisor aktualisiert Testfälle automatisch. Bei den von Ihnen ausgewählten Testfällen handelt es sich immer um die aktuelle Version. Weitere Informationen finden Sie unter Device Advisor.

# Bewährte Sicherheitsmethoden in AWS IoT Core

Dieser Abschnitt enthält Informationen zu bewährten Sicherheitsmethoden für AWS IoT Core. Informationen zu den Sicherheitsregeln für IoT-Lösungen finden Sie unter Zehn goldene Regeln in Bezug auf die Sicherheit für IoT-Lösungen.

## Schutz von MQTT-Verbindungen in AWS IoT

AWS IoT Coreist ein verwalteter Cloud-Dienst, der es verbundenen Geräten ermöglicht, einfach und sicher mit Cloud-Anwendungen und anderen Geräten zu interagieren. AWS IoT Core unterstützt HTTP, und MQTT WebSocket, ein einfaches Kommunikationsprotokoll, das speziell für die Tolerierung intermittierender Verbindungen entwickelt wurde. Wenn Sie eine Verbindung AWS IoT über MQTT herstellen, muss jede Ihrer Verbindungen mit einer Kennung verknüpft sein, die als Client-ID bezeichnet wird. Der MQTT-Client identifiziert MQTT-Verbindungen IDs eindeutig. Wenn eine neue Verbindung mit einer Client-ID hergestellt wird, die bereits für eine andere Verbindung beansprucht wurde, löscht der AWS IoT Message Broker die alte Verbindung, um die neue Verbindung zuzulassen. Der Client IDs muss in jedem Fall AWS-Konto einzigartig sein AWS-Region. Das bedeutet, dass Sie nicht die globale Einzigartigkeit des Kunden IDs außerhalb Ihrer Region AWS-Konto oder innerhalb Ihrer AWS-Konto Regionen erzwingen müssen.

Die Auswirkungen und der Schweregrad von getrennten MQTT-Verbindungen auf Ihre Geräteflotte hängt von vielen Faktoren ab. Dazu zählen:

- Ihr Anwendungsfall (z. B. die Daten, an die Ihre Geräte senden AWS IoT, wie viele Daten und die Häufigkeit, mit der die Daten gesendet werden).
- Ihre MQTT-Client-Konfiguration (z. B. Einstellungen zum automatischen Wiederverbinden, zugehörige Backoff-Timings und die Verwendung von persistenten MQTT-Sitzungen).
- Einschränkungen für Geräteressourcen.
- Die Grundursache der Verbindungstrennungen, ihre Aggressivität und ihre Persistenz.

Um Client-ID-Konflikte und ihre möglichen negativen Auswirkungen zu vermeiden, stellen Sie sicher, dass jedes Gerät oder jede mobile Anwendung über eine AWS IoT oder IAM-Richtlinie verfügt, die einschränkt, welcher Client für MQTT-Verbindungen zum Message Broker verwendet werden IDs kann. AWS IoT Sie können beispielsweise eine IAM-Richtlinie verwenden, um zu verhindern, dass ein Gerät unbeabsichtigt die Verbindung eines anderen Geräts schließt, indem es eine bereits verwendete Client-ID nutzt. Weitere Informationen finden Sie unter Autorisierung.

Alle Geräte in Ihrer Flotte müssen über Anmeldeinformationen mit Rechten verfügen, die nur beabsichtigte Aktionen autorisieren. Dazu gehören (aber nicht beschränkt auf) AWS IoT MQTT-Aktionen wie das Veröffentlichen von Nachrichten oder das Abonnieren von Themen mit einem bestimmten Umfang und Kontext. Die spezifischen Berechtigungsrichtlinien können für Ihre Anwendungsfälle variieren. Ermitteln Sie die Berechtigungsrichtlinien, die Ihren Geschäfts- und Sicherheitsanforderungen am besten entsprechen.

Verwenden Sie AWS IoT Core Richtlinienvariablen und IAM-Richtlinienvariablen, um die Erstellung und Verwaltung von Berechtigungsrichtlinien zu vereinfachen. Richtlinienvariablen können in einer Richtlinie platziert werden. Sie werden zu dem Zeitpunkt, zu dem die Richtlinie ausgewertet wird, durch Werte aus der Anforderung des Geräts ersetzt. Mithilfe von Richtlinienvariablen können Sie eine einzelne Richtlinie für die Erteilung von Berechtigungen für mehrere Geräte erstellen. Sie können die relevanten Richtlinienvariablen für Ihren Anwendungsfall anhand Ihrer AWS IoT Kontokonfiguration, Ihres Authentifizierungsmechanismus und Ihres Netzwerkprotokolls, das für die Verbindung zum AWS IoT Message Broker verwendet wird, identifizieren. Um jedoch die besten Berechtigungsrichtlinien zu schreiben, müssen Sie die Besonderheiten Ihres Anwendungsfalls und Ihr Bedrohungsmodell berücksichtigen.

Wenn Sie Ihre Geräte beispielsweise in der AWS IoT Registrierung registriert haben, können Sie Ding-Richtlinienvariablen in AWS IoT Richtlinien verwenden, um Berechtigungen auf der Grundlage von Dingeigenschaften wie Dingnamen, Dingtypen und Dingattributwerten zu gewähren oder zu verweigern. Der Name des Dings wird aus der Client-ID in der MQTT-Verbindungsnachricht abgerufen, die gesendet wird, wenn ein Ding eine Verbindung AWS IoT herstellt. Die Ding-

Richtlinienvariablen werden ersetzt, wenn ein Ding AWS IoT über MQTT mithilfe der gegenseitigen TLS-Authentifizierung oder MQTT über WebSocket das Protokoll mithilfe authentifizierter Amazon Cognito Cognito-Identitäten eine Verbindung herstellt. Sie können die AttachThingPrincipalAPI verwenden, um Zertifikate und authentifizierte Amazon Cognito Cognito-Identitäten an eine Sache anzuhängen. `iot:Connection.Thing.ThingName`ist eine nützliche Richtlinienvariable, um Client-ID-Beschränkungen durchzusetzen. Die folgende AWS IoT Beispielrichtlinie erfordert, dass der Name einer registrierten Sache als Client-ID für MQTT-Verbindungen zum AWS IoT Message Broker verwendet wird:

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

Wenn Sie laufende Client-ID-Konflikte identifizieren möchten, können Sie CloudWatch Logs for AWS IoT aktivieren und verwenden. Für jede MQTT-Verbindung, die der AWS IoT Message Broker aufgrund von Client-ID-Konflikten unterbricht, wird ein Protokolleintrag generiert, der dem folgenden ähnelt:

```
{
    "timestamp": "2019-04-28 22:05:30.105",
    "logLevel": "ERROR",
    "traceId": "02a04a93-0b3a-b608-a27c-1ae8ebdb032a",
    "accountId": "123456789012",
    "status": "Failure",
    "eventType": "Disconnect",
    "protocol": "MQTT",
    "clientId": "clientId01",
    "principalId": "1670fcf6de55adc1930169142405c4a2493d9eb5487127cd0091ca0193a3d3f6",
    "sourceIp": "203.0.113.1",
    "sourcePort": 21335,
    "reason": "DUPLICATE_CLIENT_ID",
    "details": "A new connection was established with the same client ID"
```

```
}
```

Sie können einen CloudWatch Protokollfilter verwenden, `{$.reason= "DUPLICATE_CLIENT_ID" }` um beispielsweise nach Instanzen von Client-ID-Konflikten zu suchen oder um CloudWatch Metrikfilter und entsprechende CloudWatch Alarme für die kontinuierliche Überwachung und Berichterstattung einzurichten.

Sie können AWS IoT Device Defender verwenden, um zu freizügige Richtlinien AWS IoT und IAM-Richtlinien zu identifizieren. AWS IoT Device Defender bietet auch eine Auditprüfung, die Sie benachrichtigt, wenn mehrere Geräte in Ihrer Flotte über dieselbe Client-ID eine Verbindung zum AWS IoT Message Broker herstellen.

Mit AWS IoT Device Advisor können Sie überprüfen, ob Ihre Geräte eine zuverlässige Verbindung zu den bewährten Sicherheitsmethoden herstellen AWS IoT Core und diese befolgen.

### Weitere Informationen finden Sie auch unter

- AWS IoT Core
- AWS IoT-Sicherheitsfunktionen
- AWS IoT Core Richtlinienvariablen
- IAM-Richtlinienvariablen
- Amazon Cognito-Identität
- AWS IoT Device Defender
- CloudWatch Loggt sich für AWS IoT

## Synchronisieren der internen Uhr eines Geräts

Es ist wichtig, dass Sie eine genaue Uhrzeit auf Ihrem Gerät haben. X.509-Zertifikate haben ein Ablaufdatum und eine Ablaufzeit. Die Uhr auf Ihrem Gerät wird verwendet, um sicherzustellen, dass ein Serverzertifikat noch gültig ist. Wenn Sie kommerzielle IoT-Geräte erstellen, denken Sie daran, dass Ihre Produkte vor dem Verkauf über einen längeren Zeitraum gelagert werden können. Echtzeituhren können während dieser Zeit abweichen und die Batterien können entladen werden, sodass die werkseitige Zeiteinstellung nicht ausreicht.

Für die meisten Systeme bedeutet dies, dass die Software des Geräts einen NTP-Client (Network Time Protocol) enthalten muss. Das Gerät sollte warten, bis es mit einem NTP-Server synchronisiert

wird, bevor es versucht, eine Verbindung zu AWS IoT Core herzustellen. Wenn dies nicht möglich ist, sollte das System dem Benutzer die Möglichkeit geben, die Zeit des Gerätes so einzustellen, dass nachfolgende Verbindungen erfolgreich sind.

Nachdem das Gerät mit einem NTP-Server synchronisiert wurde, kann es eine Verbindung mit AWS IoT Core herstellen. Wie viel Taktversatz zulässig ist, hängt davon ab, was Sie mit der Verbindung tun möchten.

## Überprüfen des Serverzertifikats

Das erste, was ein Gerät tut, um mit ihm zu interagieren, AWS IoT ist, eine sichere Verbindung herzustellen. Wenn Sie Ihr Gerät mit verbinden, stellen Sie sicher AWS IoT, dass Sie mit einem anderen Server sprechen AWS IoT und nicht mit einem anderen Server, der sich als solcher ausgibt. AWS IoT Jeder der AWS IoT Server ist mit einem Zertifikat ausgestattet, das für die Domain ausgestellt wurde. `iot.amazonaws.com` Dieses Zertifikat wurde AWS IoT von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt, die unsere Identität und unser Eigentum an der Domain verifizierte.

Wenn ein Gerät eine Verbindung herstellt, wird dem Gerät als Erstes ein Serverzertifikat gesendet. AWS IoT Core Geräte können überprüfen, ob sie eine Verbindung zu `iot.amazonaws.com` erwartet haben und ob der Server am Ende dieser Verbindung ein Zertifikat einer vertrauenswürdigen Autorität für diese Domäne hat.

TLS-Zertifikate liegen im X.509-Format vor und enthalten eine Vielzahl von Informationen wie Name, Standort, Domänenname und Gültigkeitsdauer für die Organisation. Der Gültigkeitszeitraum wird als ein Paar von Zeitwerten angegeben, die `notBefore` und `notAfter` genannt werden. Dienste wie AWS IoT Core verwenden begrenzte Gültigkeitszeiträume (z. B. ein Jahr) für ihre Serverzertifikate und beginnen mit der Bereitstellung neuer Zertifikate, bevor die alten ablaufen.

## Verwenden einer einzigen Identität pro Gerät

Verwenden Sie eine einzige Identität pro Client. Geräte verwenden in der Regel X.509-Client-Zertifikate. Web- und Mobilanwendungen verwenden Amazon Cognito Identity. Auf diese Weise können Sie detaillierte Berechtigungen auf Ihre Geräte anwenden.

Sie könnten beispielsweise eine Anwendung haben, die aus einem Mobiltelefon besteht, das Statusaktualisierungen von zwei verschiedenen Smart-Home-Objekten empfängt einer Glühbirne und einem Thermostat. Die Glühbirne sendet den Status ihres Batteriestands und ein Thermostat sendet Meldungen über die Temperatur.

AWS IoT authentifiziert Geräte einzeln und behandelt jede Verbindung einzeln. Sie können differenzierte Zugriffskontrollen mithilfe von Autorisierungsrichtlinien anwenden. Sie können eine Richtlinie für den Thermostat definieren, die es ihm ermöglicht, in einem Themenbereich zu veröffentlichen. Sie können eine separate Richtlinie für die Glühbirne definieren, die es ihr ermöglicht, in einem anderen Themenbereich zu veröffentlichen. Schließlich können Sie eine Richtlinie für die mobile App definieren, die es ihr nur erlaubt, sich mit den Themen für den Thermostat und die Glühbirne zu verbinden und diese zu abonnieren, um Nachrichten von diesen Geräten zu empfangen.

Wenden Sie das Prinzip der geringsten Privilegien an und beschränken Sie die Berechtigungen pro Gerät so weit wie möglich. Für alle Geräte oder Benutzer sollte eine AWS IoT Richtlinie gelten AWS IoT , die es ihnen nur erlaubt, eine Verbindung mit einer bekannten Client-ID herzustellen und bestimmte Themen zu veröffentlichen und zu abonnieren.

## Verwenden Sie eine Sekunde AWS-Region als Backup

Erwägen Sie, innerhalb einer Sekunde eine Kopie Ihrer Daten AWS-Region als Backup zu speichern. Beachten Sie, dass die AWS Lösung mit dem Namen Disaster Recovery for nicht mehr verfügbar AWS IoT ist. Auf die zugehörige GitHubBibliothek kann zwar weiterhin zugegriffen werden, sie AWS wurde jedoch im Juli 2023 als veraltet eingestuft und bietet keine Wartung oder Unterstützung mehr für sie. Besuchen Sie Kontakt, um Ihre eigenen Lösungen zu implementieren oder zusätzliche Supportoptionen zu erkunden. AWS Wenn Ihrem Konto ein AWS Technical Account Manager zugeordnet ist, wenden Sie sich an diesen, um Hilfe zu erhalten.

## Just-in-Time-Bereitstellung nutzen

Die manuelle Erstellung und Bereitstellung jedes Geräts kann zeitaufwändig sein. AWS IoT bietet die Möglichkeit, eine Vorlage zu definieren, mit der Geräte bereitgestellt werden, wenn sie zum AWS IoT ersten Mal eine Verbindung herstellen. Weitere Informationen finden Sie unter Just-in-time Bereitstellung.

## Berechtigungen zum Ausführen von AWS IoT Device Advisor-Tests

Die folgende Richtlinienvorlage zeigt die Mindestberechtigungen und die IAM-Entität, die für die Ausführung von AWS IoT Device Advisor-Testfällen erforderlich sind. Sie müssen Amazon Resource Name (ARN) durch die Geräterolle ersetzen*your-device-role-arn*, die Sie unter den Voraussetzungen erstellt haben.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "your-device-role-arn",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "iotdeviceadvisor.amazonaws.com"
                }
            }
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "execute-api:Invoke*",
                "iam:ListRoles",   // Required to list device roles in the Device
Advisor console
                "iot:Connect",
                "iot:CreateJob",
                "iot:DeleteJob",
                "iot:DescribeCertificate",
                "iot:DescribeEndpoint",
                "iotjobsdata:DescribeJobExecution",
                "iot:DescribeJob",
                "iot:DescribeThing",
                "iotjobsdata:GetPendingJobExecutions",
                "iot:GetPolicy",
                "iot:ListAttachedPolicies",
                "iot:ListCertificates",
                "iot:ListPrincipalPolicies",
                "iot:ListThingPrincipals",
                "iot:ListThings",
                "iot:Publish",
                "iotjobsdata:StartNextPendingJobExecution",
                "iotjobsdata:UpdateJobExecution",
                "iot:UpdateThingShadow",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents",
```

```
                "logs:PutRetentionPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": "iotdeviceadvisor:*",
            "Resource": "*"
        }
    ]
}
```

## Confused-Deputy-Prävention im dienstübergreifenden Szenario für Device Advisor

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. In AWS kann ein dienstübergreifendes Identitätswechsels zu dem Problem mit dem verwirrten Stellvertreter führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der Anruf-Dienst kann so manipuliert werden, dass er seine Berechtigungen verwendet, um auf die Ressourcen eines anderen Kunden zu reagieren, auf die er sonst nicht zugreifen dürfte. Um dies zu verhindern, AWS bietet Tools, mit denen Sie Ihre Daten für alle Dienste mit Dienstprinzipalen schützen können, denen Zugriff auf Ressourcen in Ihrem Konto gewährt wurde.

Wir empfehlen die Verwendung der globalen Bedingungskontext-Schlüssel `aws:SourceArn` und `aws:SourceAccount` in ressourcenbasierten Richtlinien, um die Berechtigungen, die Device Advisor einem anderen Service erteilt, auf eine bestimmte Ressource zu beschränken. Wenn Sie beide globalen Bedingungskontextschlüssel verwenden, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienanweisung verwendet werden.

Der Wert `aws:SourceArn` muss der ARN Ihrer Suite-Definitionsressource sein. Die Suite-Definitionsressource bezieht sich auf die Testsuite, die Sie mit Device Advisor erstellt haben.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder

wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Bedingungskontext-Schlüssel `aws:SourceArn` mit Platzhaltern (*) für die unbekannten Teile des ARN. Beispiel: `arn:aws:iotdeviceadvisor:*:account-id:suitedefinition/*`

Das folgende Beispiel zeigt, wie Sie die globalen Bedingungskontext-Schlüssel `aws:SourceArn` und `aws:SourceAccount` in Device Advisor verwenden können, um das Confused-Deputy-Problem zu vermeiden.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "iotdeviceadvisor.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:iotdeviceadvisor:us-
east-1:123456789012:suitedefinition/ygp6rxa3tzvn"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

# AWS Schulung und Zertifizierung

Nehmen Sie an dem folgenden Kurs teil, um mehr über wichtige Sicherheitskonzepte zu erfahren: AWS IoT [AWS IoT Security Primer](#).

# Überwachung AWS IoT

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit AWS IoT und Leistung Ihrer AWS Lösungen.

Wir empfehlen Ihnen dringend, Überwachungsdaten aus allen Teilen Ihrer AWS Lösung zu sammeln, um das Debuggen eines etwaigen Fehlers an mehreren Stellen zu erleichtern. Erstellen Sie zunächst einen Überwachungsplan, der die folgenden Fragen beantwortet. Wenn Sie nicht sicher sind, wie Sie diese beantworten sollen, können Sie trotzdem die Protokollierung aktivieren und Ihre Leistungsgrundlagen festlegen.

- Was sind Ihre Überwachungsziele?
- Welche Ressourcen möchten Sie überwachen?
- Wie oft werden diese Ressourcen überwacht?
- Welche Überwachungs-Tools möchten Sie verwenden?
- Wer soll die Überwachungsaufgaben ausführen?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

Ihr nächster Schritt besteht darin, die Protokollierung zu aktivieren und einen Basiswert für die normale AWS IoT Leistung in Ihrer Umgebung festzulegen, indem Sie die Leistung zu verschiedenen Zeiten und unter verschiedenen Lastbedingungen messen. Bewahren Sie bei der Überwachung historische Überwachungsdaten auf, damit Sie sie mit aktuellen Leistungsdaten vergleichen können. AWS IoT Auf diese Weise können Sie normale Leistungsmuster und Leistungsanomalien identifizieren und Methoden zu deren Handhabung entwickeln.

Um Ihre Ausgangsleistung für zu ermitteln AWS IoT, sollten Sie zunächst diese Kennzahlen überwachen. Später können Sie immer noch weitere Metriken überwachen.

- `PublishIn.Success`
- `PublishOut.Success`
- `Subscribe.Success`
- `Ping.Success`
- `Connect.Success`
- `GetThingShadow.Accepted`

- `UpdateThingShadow.Accepted`
- `DeleteThingShadow.Accepted`
- `RulesExecuted`

Die Themen in diesem Abschnitt dienen als Einstieg in die Protokollierung und Überwachung von AWS IoT.

Themen

- Konfigurieren Sie die AWS IoT Protokollierung
- Überwachen Sie AWS IoT Alarme und Messwerte mit Amazon CloudWatch
- Überwachung AWS IoT mithilfe von Protokollen CloudWatch
- Geräteseitige Protokolle auf Amazon hochladen CloudWatch
- Protokollieren von AWS IoT API-Aufrufen mit AWS CloudTrail

# Konfigurieren Sie die AWS IoT Protokollierung

Sie müssen die Protokollierung mithilfe der AWS IoT Konsole, CLI oder API aktivieren, bevor Sie AWS IoT Aktivitäten überwachen und protokollieren können.

Sie können die Protokollierung für alle AWS IoT oder nur für bestimmte Dinggruppen aktivieren. Sie können die AWS IoT Protokollierung mithilfe der AWS IoT Konsole, CLI oder API konfigurieren. Sie müssen jedoch die CLI oder API verwenden, um die Protokollierung für bestimmte Dinggruppen zu konfigurieren.

Wenn Sie überlegen, wie Sie Ihre AWS IoT Protokollierung konfigurieren möchten, bestimmt die Standardkonfiguration für die Protokollierung, wie AWS IoT Aktivitäten protokolliert werden, sofern nicht anders angegeben. Zu Beginn können detaillierte Protokolle mit der Standard-Protokollstufe `INFO` oder `DEBUG` sinnvoll sein. Nachdem Sie die ersten Protokolle geprüft haben, können Sie als Standard-Protokollstufe eine weniger ausführliche Stufe wie `WARN` oder `ERROR` und zugleich eine ausführlichere Protokollstufe für diejenigen Ressourcen aktivieren, die möglicherweise mehr Aufmerksamkeit benötigen. Protokollstufen können jederzeit geändert werden.

In diesem Thema wird die cloudseitige Anmeldung behandelt. AWS IoT Informationen zur geräteseitigen Protokollierung und Überwachung finden Sie unter Geräteseitige Protokolle hochladen auf. CloudWatch

Informationen zur Protokollierung und Überwachung AWS IoT Greengrass finden Sie unter Protokollierung und Überwachung. AWS IoT Greengrass Zum 30. Juni 2023 wurde die AWS IoT Greengrass Core-Software auf AWS IoT Greengrass Version 2 migriert.

## Konfigurieren der Protokollierungsrolle und -richtlinie

Bevor Sie die Anmeldung aktivieren können AWS IoT, müssen Sie eine IAM-Rolle und eine Richtlinie erstellen, die Ihnen die AWS Erlaubnis erteilt, AWS IoT Aktivitäten in Ihrem Namen zu überwachen. Sie können auch eine IAM-Rolle mit den erforderlichen Richtlinien im Abschnitt Protokolle der AWS IoT -Konsole generieren.

> **Note**
>
> Bevor Sie die AWS IoT Protokollierung aktivieren, stellen Sie sicher, dass Sie die Zugriffsberechtigungen für CloudWatch Protokolle verstanden haben. Benutzer mit Zugriff auf CloudWatch Protokolle können Debugging-Informationen von Ihren Geräten einsehen. Weitere Informationen finden Sie unter Authentifizierung und Zugriffskontrolle für Amazon CloudWatch Logs.
>
> Wenn Sie AWS IoT Core aufgrund von Lasttests mit hohen Datenverkehrsmustern rechnen, sollten Sie erwägen, die IoT-Protokollierung zu deaktivieren, um Drosselungen zu vermeiden. Wenn ein hoher Datenverkehr festgestellt wird, deaktiviert unser Service möglicherweise die Protokollierung in Ihrem Konto.

Im Folgenden wird gezeigt, wie Sie eine Protokollierungsrolle und eine Richtlinie für AWS IoT Core Ressourcen erstellen.

### Erstellen einer Protokollierungsrolle

Um eine Protokollierungsrolle zu erstellen, öffnen Sie den Rollen-Hub der IAM-Konsole und wählen Sie Rolle erstellen aus.

1. Wählen Sie unter Vertrauenswürdige Entität auswählen die Option AWS -Service aus. Wählen Sie dann die Option IoT unter Anwendungsfall aus. Wenn IoT nicht angezeigt wird, geben Sie IoT im Drop-down-Menü Anwendungsfälle für andere AWS -Services ein und suchen Sie danach. Klicken Sie auf Weiter.
2. Auf der Seite Berechtigungen hinzufügen sehen Sie die Richtlinien, die automatisch mit der Servicerolle verknüpft werden. Wählen Sie Weiter aus.

3. Geben Sie auf der Seite Name, Überprüfen und Erstellen einen Rollennamen und eine Rollenbeschreibung für die Rolle ein und wählen Sie dann Rolle erstellen.
4. Suchen Sie in der Liste der Rollen nach der Rolle, die Sie erstellt haben, öffnen Sie sie und kopieren Sie die Rollen-ARN (*logging-role-arn*), die Sie verwenden möchten, wenn SieKonfigurieren der Standard-Protokollierung in AWS IoT (Konsole).

## Richtlinie für die Protokollierungsrolle

Die folgenden Richtliniendokumente enthalten die Rollen- und Vertrauensrichtlinien, AWS IoT an die Sie Protokolleinträge in CloudWatch Ihrem Namen senden können. Wenn Sie auch dem LoRa WAN erlaubt AWS IoT Core haben, Protokolleinträge einzureichen, wird ein für Sie erstelltes Richtliniendokument angezeigt, in dem beide Aktivitäten protokolliert werden.

> **Note**
>
> Diese Dokumente wurden für Sie erstellt, als Sie die Protokollierungsrolle erstellt haben. Die Dokumente enthalten Variablen *${partition},${region}*, und*${accountId}*, die Sie durch Ihre Werte ersetzen müssen.

Rollenrichtlinie:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:PutMetricFilter",
    "logs:PutRetentionPolicy",
    "iot:GetLoggingOptions",
    "iot:SetLoggingOptions",
    "iot:SetV2LoggingOptions",
    "iot:GetV2LoggingOptions",
    "iot:SetV2LoggingLevel",
    "iot:ListV2LoggingLevels",
    "iot:DeleteV2LoggingLevel"
```

```
    ],
    "Resource": [
     "arn:${partition}:logs:${region}:${accountId}:log-group:AWSIotLogsV2:*"
    ]
   }
  ]
}
```

Vertraue der Richtlinie, nur AWS IoT Core Aktivitäten zu protokollieren:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "iot.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

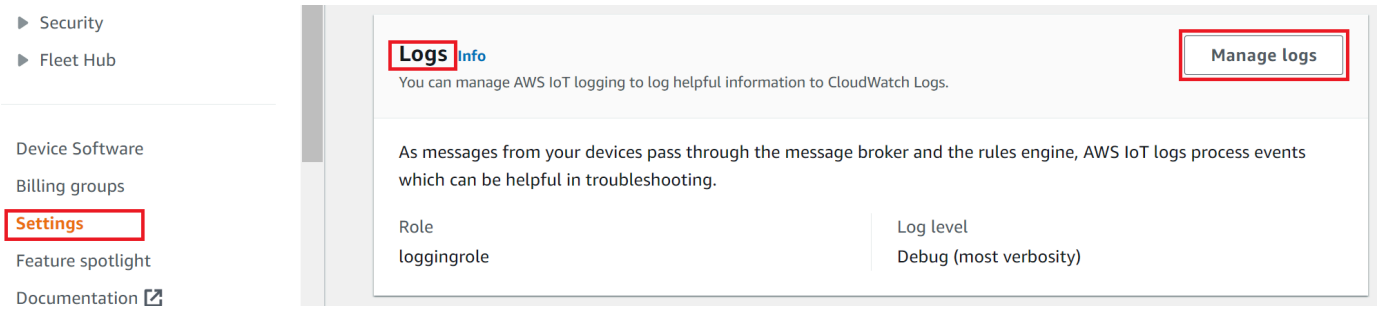
## Konfigurieren der Standard-Protokollierung in AWS IoT (Konsole)

In diesem Abschnitt wird beschrieben, wie Sie mit der AWS IoT Konsole die Protokollierung für alle von konfigurieren AWS IoT. Um die Protokollierung ausschließlich für bestimmte Objektgruppen zu konfigurieren, müssen Sie die CLI oder die API verwenden. Informationen zum Konfigurieren der Protokollierung ausschließlich für bestimmte Objektgruppen finden Sie unter Konfigurieren der ressourcenspezifischen Protokollierung in AWS IoT (CLI).

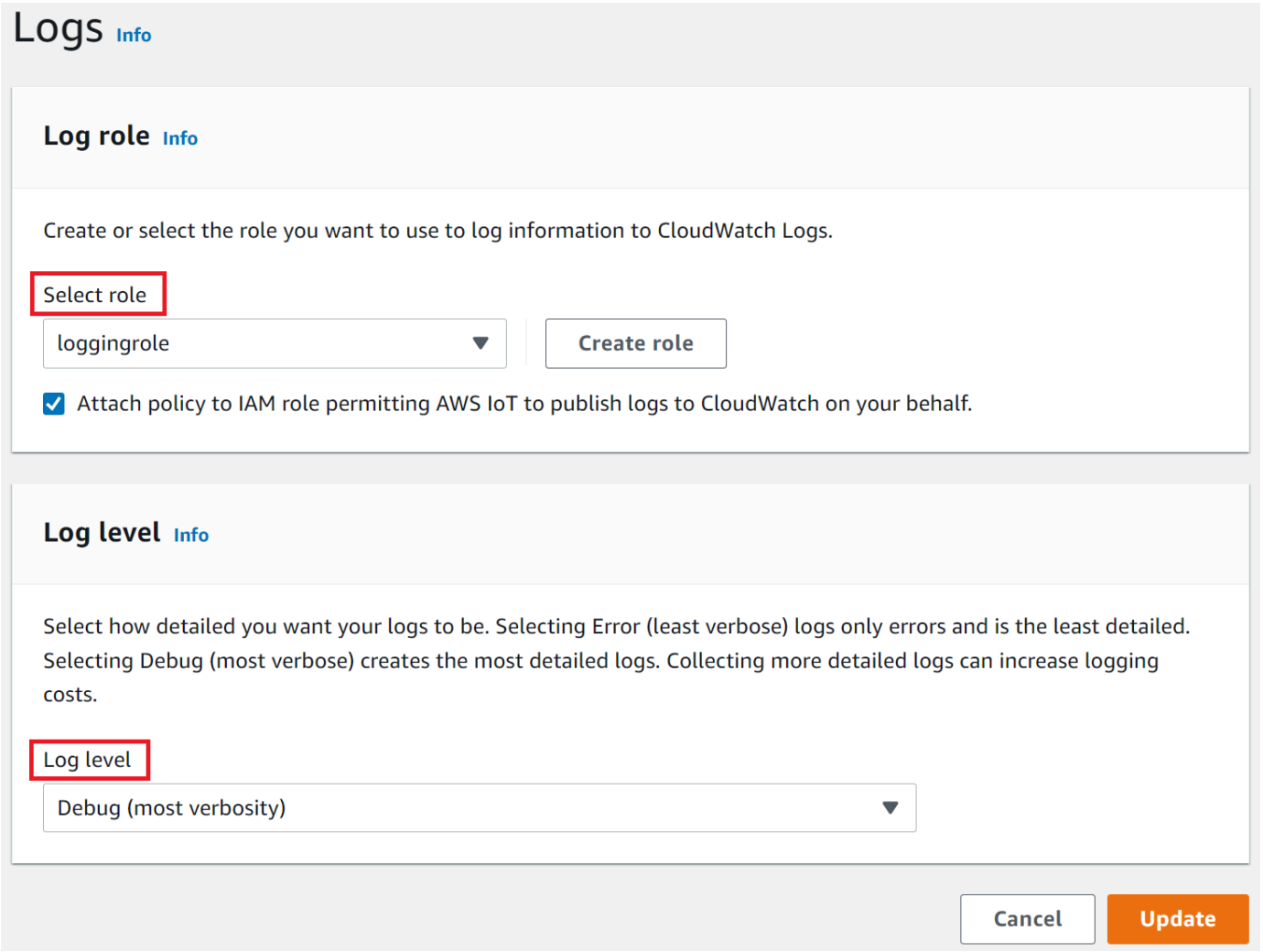
Um die AWS IoT Konsole zur Konfiguration der Standardprotokollierung für alle zu verwenden AWS IoT

1. Melden Sie sich bei der AWS IoT Konsole an. Weitere Informationen finden Sie unter Öffnen Sie die AWS IoT Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus. Wählen Sie im Abschnitt Protokolle der Seite Einstellungen die Option Protokolle verwalten aus.

Auf der Seite Protokolle werden die Protokollierungsrolle und die Ausführlichkeit des Protokolls für alle AWS IoT-Objekte angezeigt.




3. Wählen Sie auf der Seite Protokolle die Option Rolle auswählen aus, um eine Rolle festzulegen, die Sie in Erstellen einer Protokollierungsrolle oder in Rolle erstellen erstellt haben, um eine neue Rolle für die Protokollierung zu erstellen.




4. Wählen Sie die Protokollebene, die den Detaillierungsgrad der Protokolleinträge beschreibt, die in den CloudWatch Protokollen erscheinen sollen.

5. Wählen Sie Aktualisieren aus, um Ihre Änderungen zu speichern.

Nachdem Sie die Protokollierung aktiviert haben, finden Sie unter AWS IoT Protokolle in der CloudWatch Konsole anzeigen Informationen zum Anzeigen der Protokolleinträge.

## Standardanmeldung konfigurieren AWS IoT (CLI)

In diesem Abschnitt wird beschrieben, wie Sie die globale Protokollierung für AWS IoT mithilfe der CLI konfigurieren.

> **Note**
>
> Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle, die Sie verwenden möchten. Wenn Sie eine Rolle für die Protokollierung erstellen müssen, beachten Sie zunächst Erstellen einer Protokollierungsrolle, bevor Sie weitermachen.
> Der zum Aufrufen der API verwendete Prinzipal benötigt Rollenberechtigungen weitergeben für Ihre Protokollierungsrolle.

Sie können dieses Verfahren auch mit der API durchführen, indem Sie die Methoden in der AWS API verwenden, die den hier gezeigten CLI-Befehlen entsprechen.

So verwenden Sie die CLI zur Konfiguration der Standardprotokollierung für AWS IoT

1. Verwenden Sie den Befehl set-v2-logging-options, um die Protokollierungsoptionen für Ihr Konto festzulegen.

   ```
   aws iot set-v2-logging-options \
       --role-arn logging-role-arn \
       --default-log-level log-level
   ```

   Wobei:

   --role-arn

   Der Rollen-ARN, der die AWS IoT Erlaubnis erteilt, in Ihre Logs in CloudWatch Logs zu schreiben.

--default-log-level

Die zu verwendende Protokollstufe. Gültige Werte: `ERROR`, `WARN`, `INFO`, `DEBUG` oder `DISABLED`

--no-disable-all-logs

Ein optionaler Parameter, der die gesamte AWS IoT Protokollierung aktiviert. Verwenden Sie diesen Parameter zum Aktivieren der Protokollierung, wenn sie derzeit deaktiviert ist.

--disable-all-logs

Ein optionaler Parameter, der die gesamte AWS IoT Protokollierung deaktiviert. Verwenden Sie diesen Parameter zum Deaktivieren der Protokollierung, wenn sie derzeit aktiviert ist.

2. Verwenden Sie den Befehl get-v2-logging-options, um Ihre aktuellen Protokollierungsoptionen abzurufen.

```
aws iot get-v2-logging-options
```

Nachdem Sie die Protokollierung aktiviert haben, finden Sie unter AWS IoT Protokolle in der CloudWatch Konsole anzeigen Informationen zum Anzeigen der Protokolleinträge.

> **Note**
>
> AWS IoT unterstützt weiterhin ältere Befehle (set-logging-optionsundget-logging-options) zum Einrichten und Abrufen der globalen Protokollierung für Ihr Konto. Beachten Sie, dass bei Verwendung dieser Befehle die ausgegebenen Protokolle nur Klartext enthalten und keine JSON-Nutzlasten. Zudem ist die Protokollierungslatenz in der Regel höher. Es werden keine weiteren Verbesserungen an der Implementierung dieser älteren Befehle vorgenommen. Wir empfehlen die Verwendung der „v2“-Versionen zur Konfiguration Ihrer Protokollierungsoptionen und, wenn möglich, die Änderung von Legacy-Anwendungen, die ältere Versionen verwenden.

## Konfigurieren der ressourcenspezifischen Protokollierung in AWS IoT (CLI)

In diesem Abschnitt wird beschrieben, wie Sie die ressourcenspezifische Protokollierung AWS IoT mithilfe der CLI konfigurieren. Mit der ressourcenspezifischen Protokollierung können Sie eine Protokollierungsstufe für eine bestimmte Objektgruppe angeben.

Objektgruppen können andere Objektgruppen enthalten, um eine hierarchische Beziehung zu erstellen. In diesem Verfahren wird beschrieben, wie die Protokollierung einer einzelnen Objektgruppe konfiguriert wird. Sie können dieses Verfahren auf die übergeordnete Objektgruppe in einer Hierarchie anwenden, um die Protokollierung für alle Objektgruppen in der Hierarchie zu konfigurieren. Sie können dieses Verfahren auch auf eine untergeordnete Objektgruppe anwenden, um die Protokollierungskonfiguration des übergeordneten Elements zu überschreiben.

Ein Ding kann Mitglied einer Dinggruppe sein. Diese Mitgliedschaft ermöglicht es dem Ding, Konfigurationen, Richtlinien und Einstellungen zu erben, die auf die Dinggruppe angewendet wurden. Dinggruppen werden verwendet, um Einstellungen für mehrere Dinge gemeinsam zu verwalten und anzuwenden, anstatt jedes Ding einzeln zu behandeln. Wenn Ihre Client-ID mit dem Ding-Namen übereinstimmt, AWS IoT Core wird die Client-Sitzung automatisch der entsprechenden Ding-Ressource zugeordnet. Dadurch kann die Clientsitzung die Konfigurationen und Einstellungen übernehmen, die auf die Dinggruppen angewendet wurden, zu denen das Ding gehört, einschließlich der Protokollierungsebenen. Wenn Ihre Client-ID nicht mit dem Namen des Dings übereinstimmt, können Sie den exklusiven Ding-Anhang aktivieren, um die Zuordnung herzustellen. Weitere Informationen finden Sie unter ???.

Neben Objektgruppen können Sie auch Ziele wie die Client-ID, die Quell-IP und die Prinzipal-ID eines Geräts protokollieren.

> **Note**
>
> Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle, die Sie verwenden möchten. Wenn Sie eine Rolle für die Protokollierung erstellen müssen, beachten Sie zunächst Erstellen einer Protokollierungsrolle, bevor Sie weitermachen.
> Der zum Aufrufen der API verwendete Prinzipal benötigt Rollenberechtigungen weitergeben für Ihre Protokollierungsrolle.

Sie können dieses Verfahren auch mit der API durchführen, indem Sie die Methoden in der AWS API verwenden, die den hier gezeigten CLI-Befehlen entsprechen.

So verwenden Sie die CLI zur Konfiguration der ressourcenspezifischen Protokollierung für AWS IoT

1. Verwenden Sie den Befehl set-v2-logging-options, um die Protokollierungsoptionen für Ihr Konto festzulegen.

```
aws iot set-v2-logging-options \
```

```
    --role-arn logging-role-arn \
    --default-log-level log-level
```

Wobei:

--role-arn

Der Rollen-ARN, der die AWS IoT Erlaubnis erteilt, in Ihre Logs in CloudWatch Logs zu schreiben.

--default-log-level

Die zu verwendende Protokollstufe. Gültige Werte: `ERROR`, `WARN`, `INFO`, `DEBUG` oder `DISABLED`

--no-disable-all-logs

Ein optionaler Parameter, der die gesamte AWS IoT Protokollierung aktiviert. Verwenden Sie diesen Parameter zum Aktivieren der Protokollierung, wenn sie derzeit deaktiviert ist.

--disable-all-logs

Ein optionaler Parameter, der die gesamte AWS IoT Protokollierung deaktiviert. Verwenden Sie diesen Parameter zum Deaktivieren der Protokollierung, wenn sie derzeit aktiviert ist.

2. Verwenden Sie den Befehl set-v2-logging-level, um die ressourcenspezifische Protokollierung für eine Objektgruppe zu konfigurieren.

```
aws iot set-v2-logging-level \
             --log-target targetType=THING_GROUP,targetName=thing_group_name \
             --log-level log_level
```

--log-target

Typ und Name der Ressource, für die Sie die Protokollierung konfigurieren. Der Wert `target_type` muss einer der folgenden sein: `THING_GROUP` | `CLIENT_ID` | `SOURCE_IP` | `PRINCIPAL_ID`. Der Wert des Parameters log-target kann Text (wie im Befehlsbeispiel oben) oder eine JSON-Zeichenfolge wie im folgenden Beispiel sein.

```
aws iot set-v2-logging-level \
             --log-target '{"targetType": "THING_GROUP","targetName":
 "thing_group_name"}' \
```

```
                --log-level log_level
```

--log-level

Die Protokollierungsebene, die beim Generieren von Protokollen für die angegebene Ressource verwendet wird. Gültige Werte: DEBUG, INFO, ERROR, WARN und DISABLED.

```
aws iot set-v2-logging-level \
              --log-target targetType=CLIENT_ID,targetName=ClientId1 \
              --log-level DEBUG
```

3. Verwenden Sie den Befehl list-v2-logging-levels, um die aktuell konfigurierten Protokollierungsstufen aufzulisten.

```
aws iot list-v2-logging-levels
```

4. Verwenden Sie den Befehl delete-v2-logging-level, um eine ressourcenspezifische Protokollierungsstufe zu löschen, ähnlich dem folgenden Beispiel.

```
aws iot delete-v2-logging-level \
              --target-type "THING_GROUP" \
              --target-name "thing_group_name"
```

```
aws iot delete-v2-logging-level \
              --target-type=CLIENT_ID
              --target-name=ClientId1
```

--targetType

Der Wert `target_type` muss einer der folgenden sein: `THING_GROUP` | `CLIENT_ID` | `SOURCE_IP` | `PRINCIPAL_ID`.

--targetName

Der Name der Objektgruppe, für welche die Protokollierungsstufe entfernt werden soll.

Nachdem Sie die Protokollierung aktiviert haben, finden Sie unter AWS IoT Protokolle in der CloudWatch Konsole anzeigen Informationen zum Anzeigen der Protokolleinträge.

## Protokollstufen

Diese Protokollstufen bestimmen die Ereignisse, die protokolliert werden und die für Standard- und ressourcenspezifische Protokollstufen berücksichtigt werden.

ERROR

Jeder Fehler, der bewirkt, dass ein Vorgang fehlschlägt.

Protokolle enthalten ausschließlich Fehlerinformationen der Kategorie ERROR.

WARN

Alles, was zu Inkonsistenzen im System führen kann, aber möglicherweise nicht zum Fehlschlagen der Operation führt.

Protokolle enthalten Informationen der Kategorien ERROR und WARN.

INFO

Hochwertige Informationen über den Ablauf der Objekte.

Protokolle enthalten Informationen der Kategorien INFO, ERROR und WARN.

DEBUG

Informationen, die bei der Problembehebung hilfreich sein können.

Protokolle enthalten Informationen der Kategorien DEBUG, INFO, ERROR und WARN.

DISABLED (DEAKTIVIERT)

Die gesamte Protokollierung ist deaktiviert.

# Überwachen Sie AWS IoT Alarme und Messwerte mit Amazon CloudWatch

Sie können die AWS IoT Nutzung überwachen CloudWatch, wobei Rohdaten gesammelt und in lesbare Kennzahlen AWS IoT umgewandelt werden, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden für einen Zeitraum von zwei Wochen aufgezeichnet, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Standardmäßig werden AWS IoT Metrikdaten automatisch CloudWatch in Intervallen von einer Minute gesendet. Weitere Informationen finden Sie

unter Was sind Amazon CloudWatch, Amazon CloudWatch Events und Amazon CloudWatch Logs? im CloudWatch Amazon-Benutzerhandbuch.

## AWS IoT Metriken verwenden

Die von gemeldeten Metriken enthalten AWS IoT Informationen, die Sie auf unterschiedliche Weise analysieren können. Die folgenden Anwendungsfälle basieren auf einem Szenario, bei dem zehn Elemente einmal am Tag eine Verbindung zum Internet herstellen. Jeden Tag:

- Zehn Dinge stellen ungefähr AWS IoT gleichzeitig eine Verbindung her.
- Jedes Objekt meldet sich bei einem Themenfilter an und wartet eine Stunde, bevor des die Verbindung wieder trennt. Während dieser Zeit kommunizieren die Elemente miteinander und erfahren mehr über den Status der Welt.
- Jedes Objekt veröffentlicht eine Sichtweise, die es basierend auf den mit `UpdateThingShadow` neu erhaltenen Daten gebildet hat.
- Jedes Ding trennt sich von AWS IoT.

Um Ihnen den Einstieg zu erleichtern, werden in diesen Themen einige der Fragen behandelt, die Sie möglicherweise haben.

- Wie werde ich benachrichtigt, wenn meine Objekte nicht jeden Tag erfolgreich verbunden werden?
- Wie werde ich benachrichtigt, wenn meine Objekte nicht jeden Tag Daten veröffentlichen?
- Wie werde ich benachrichtigt, wenn die Schattenaktualisierungen meines Objekts jeden Tag abgelehnt werden?
- Wie kann ich einen CloudWatch Alarm für Jobs einrichten?

Weitere Informationen zu CloudWatch Alarmen und Metriken

- CloudWatch Alarme zur Überwachung erstellen AWS IoT
- AWS IoT Metriken und Dimensionen

## CloudWatch Alarme zur Überwachung erstellen AWS IoT

Sie können einen CloudWatch Alarm erstellen, der eine Amazon SNS SNS-Nachricht sendet, wenn sich der Status des Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen festgelegten Zeitraum. Wenn der Wert der Metrik über eine Reihe von Zeiträumen einen

bestimmten Schwellenwert überschreitet, wird mindestens eine Aktion ausgeführt. Die Aktion kann eine Benachrichtigung sein, die an ein Amazon-SNS-Thema oder eine Auto Scaling-Richtlinie gesendet wird. Alarme lösen Aktionen nur bei anhaltenden Statusänderungen aus. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Zustand befinden. Der Zustand muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein.

In den folgenden Themen werden einige Beispiele zur Verwendung von CloudWatch-Alarmen beschrieben.

- Wie werde ich benachrichtigt, wenn meine Objekte nicht jeden Tag erfolgreich verbunden werden?
- Wie werde ich benachrichtigt, wenn meine Objekte nicht jeden Tag Daten veröffentlichen?
- Wie werde ich benachrichtigt, wenn die Schattenaktualisierungen meines Objekts jeden Tag abgelehnt werden?
- Wie kann ich einen CloudWatch Alarm für Jobs erstellen?

Sie können alle Messwerte sehen, die CloudWatch Alarme überwachen könnenAWS IoT Metriken und Dimensionen.

## Wie werde ich benachrichtigt, wenn meine Objekte nicht jeden Tag erfolgreich verbunden werden?

1. Erstellen Sie ein Amazon-SNS-Thema mit dem Namen `things-not-connecting-successfully` und zeichnen Sie dessen Amazon-Ressourcennamen (ARN) auf. In diesem Verfahren wird der ARN des Themas als *`sns-topic-arn`* angegeben.

   Weitere Informationen zum Erstellen einer Amazon-SNS-Benachrichtigung finden Sie unter Erste Schritte mit Amazon SNS.
2. Erstellen Sie den Alarm.

```
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 \
    --evaluation-periods 1 \
    --alarm-actions sns-topic-arn
```

3. Testen Sie den Alarm.

```
aws cloudwatch set-alarm-state --alarm-name ConnectSuccessAlarm --state-reason
 "initializing" --state-value OK
```

```
aws cloudwatch set-alarm-state --alarm-name ConnectSuccessAlarm --state-reason
 "initializing" --state-value ALARM
```

4. Stellen Sie sicher, dass der Alarm in der CloudWatch -Konsole angezeigt wird.

## Wie werde ich benachrichtigt, wenn meine Objekte nicht jeden Tag Daten veröffentlichen?

1. Erstellen Sie ein Amazon-SNS-Thema mit dem Namen `things-not-publishing-data` und zeichnen Sie dessen Amazon-Ressourcennamen (ARN) auf. In diesem Verfahren wird der ARN des Themas als *sns-topic-arn* angegeben.

   Weitere Informationen zum Erstellen einer Amazon-SNS-Benachrichtigung finden Sie unter Erste Schritte mit Amazon SNS.

2. Erstellen Sie den Alarm.

```
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 \
    --evaluation-periods 1 \
    --alarm-actions sns-topic-arn
```

3. Testen Sie den Alarm.

```
aws cloudwatch set-alarm-state --alarm-name PublishInSuccessAlarm --state-reason
 "initializing" --state-value OK
```

```
aws cloudwatch set-alarm-state --alarm-name PublishInSuccessAlarm --state-reason
 "initializing" --state-value ALARM
```

4. Stellen Sie sicher, dass der Alarm in der CloudWatch -Konsole angezeigt wird.

## Wie werde ich benachrichtigt, wenn die Schattenaktualisierungen meines Objekts jeden Tag abgelehnt werden?

1. Erstellen Sie ein Amazon-SNS-Thema mit dem Namen `things-shadow-updates-rejected` und zeichnen Sie dessen Amazon-Ressourcennamen (ARN) auf. In diesem Verfahren wird der ARN des Themas als *`sns-topic-arn`* angegeben.

   Weitere Informationen zum Erstellen einer Amazon-SNS-Benachrichtigung finden Sie unter Erste Schritte mit Amazon SNS.

2. Erstellen Sie den Alarm.

```
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 \
    --threshold 10 \
    --comparison-operator LessThanThreshold \
    --period 86400 \
    --unit Count \
    --evaluation-periods 1 \
    --alarm-actions sns-topic-arn
```

3. Testen Sie den Alarm.

```
aws cloudwatch set-alarm-state --alarm-name UpdateThingShadowSuccessAlarm --state-
reason "initializing" --state-value OK
```

```
aws cloudwatch set-alarm-state --alarm-name UpdateThingShadowSuccessAlarm --state-
reason "initializing" --state-value ALARM
```

4. Stellen Sie sicher, dass der Alarm in der CloudWatch -Konsole angezeigt wird.

## Wie kann ich einen CloudWatch Alarm für Jobs erstellen?

Der Jobs-Service stellt Ihnen CloudWatch Kennzahlen zur Verfügung, mit denen Sie Ihre Jobs überwachen können. Sie können CloudWatch -Alarme erstellen, um alle Jobs-Metriken zu überwachen.

Der folgende Befehl erzeugt einen CloudWatch Alarm, um die Gesamtzahl der fehlgeschlagenen Jobausführungen für Job zu überwachen, *SampleOTAJob* und benachrichtigt Sie, wenn mehr als 20 Jobausführungen fehlgeschlagen sind. Der Alarm überwacht die Jobs-Metrik `FailedJobExecutionTotalCount`, indem der gemeldete Wert alle 300 Sekunden überprüft wird. Er wird aktiviert, wenn ein einzelner gemeldeter Wert größer als 20 ist, was bedeutet, dass seit dem Start des Auftrags mehr als 20 fehlgeschlagene Auftragsausführungen aufgetreten sind. Wenn der Alarm auslöst, wird eine Benachrichtigung an das angegebene Amazon–SNS-Thema gesendet.

```
aws cloudwatch put-metric-alarm \
    --alarm-name TotalFailedJobExecution-SampleOTAJob \
    --alarm-description "Alarm when total number of failed job execution exceeds the
 threshold for SampleOTAJob" \
    --namespace AWS/IoT \
    --metric-name FailedJobExecutionTotalCount \
    --dimensions Name=JobId,Value=SampleOTAJob \
    --statistic Sum \
    --threshold 20 \
    --comparison-operator GreaterThanThreshold \
    --period 300 \
    --unit Count \
    --evaluation-periods 1 \
    --alarm-actions arn:aws:sns:<AWS_REGION>:<AWS_ACCOUNT_ID>:SampleOTAJob-has-too-
many-failed-job-ececutions
```

Der folgende Befehl erzeugt einen CloudWatch Alarm, um die Anzahl der fehlgeschlagenen Jobausführungen für Job *SampleOTAJob* in einem bestimmten Zeitraum zu überwachen. Sie werden dann benachrichtigt, wenn mehr als fünf Auftragsausführungen in diesem Zeitraum fehlgeschlagen sind. Der Alarm überwacht die Jobs-Metrik `FailedJobExecutionCount`, indem der

gemeldete Wert alle 3600 Sekunden überprüft wird. Sie wird aktiviert, wenn ein einzelner gemeldeter Wert größer als 5 ist, was bedeutet, dass in der letzten Stunde mehr als 5 fehlgeschlagene Auftragsausführungen aufgetreten sind. Wenn der Alarm auslöst, wird eine Benachrichtigung an das angegebene Amazon–SNS-Thema gesendet.

```
aws cloudwatch put-metric-alarm \
    --alarm-name FailedJobExecution-SampleOTAJob \
    --alarm-description "Alarm when number of failed job execution per hour exceeds the
 threshold for SampleOTAJob" \
    --namespace AWS/IoT \
    --metric-name FailedJobExecutionCount \
    --dimensions Name=JobId,Value=SampleOTAJob \
    --statistic Sum \
    --threshold 5 \
    --comparison-operator GreaterThanThreshold \
    --period 3600 \
    --unit Count \
    --evaluation-periods 1 \
    --alarm-actions arn:aws:sns:<AWS_REGION>:<AWS_ACCOUNT_ID>:SampleOTAJob-has-too-
many-failed-job-ececutions-per-hour
```

## AWS IoT Metriken und Dimensionen

Wenn Sie mit interagieren AWS IoT, sendet der Service Metriken und Dimensionen an CloudWatch jede Minute. Sie können die CloudWatch Konsole verwenden oder verwenden AWS IoT, AWS CLI um diese Metriken anzusehen.

Um Metriken mit der CloudWatch Konsole anzuzeigen, öffnen Sie die CloudWatch Konsole. Wählen Sie im Navigationsbereich Metriken und dann Alle Metriken aus. Suchen Sie auf der Registerkarte Durchsuchen nach, AWS IoT um die Liste der Metriken anzuzeigen. Metriken werden zunächst nach dem Service-Namespace und anschließend nach den verschiedenen Dimensionskombinationen in den einzelnen Namespaces gruppiert.

Führen Sie den folgenden Befehl aus AWS CLI, um Metriken mit anzuzeigen.

```
aws cloudwatch list-metrics --namespace "AWS/IoT"
```

CloudWatch zeigt die folgenden Gruppen von Metriken für an AWS IoT:

- AWS IoT Metriken
- AWS IoT Core Metriken des Anbieters von Anmeldeinformationen

- Authentifizierungsmetriken
- OCSP Stapling-Metriken für Serverzertifikate
- Regelmetriken
- Regelaktionsmetriken
- Aktionsspezifische HTTP-Metriken
- Message Broker-Metriken
- Geräteschatten-Metriken
- Jobs-Metriken
- Metriken für Device Defender-Prüfung
- Metriken für Device Defender-Erkennung
- Gerätebereitstellungsmetriken
- LoRaWAN-Metriken
- Metriken zur Flottenindizierung
- Dimensionen für Metriken


## AWS IoT Metriken

| Metrik | Beschreibung |
| --- | --- |
| `AddThingToDynamicThingGroupsFailed` | Die Anzahl der Fehlerereignisse, die mit dem Hinzufügen eines Objekts zu einer dynamischen Objektgruppe verbunden sind. Die Dimension `DynamicThingGroupName` enthält den Namen der dynamischen Gruppen, die Objekte nicht hinzufügen konnten. |
| `NumLogBatchesFailedToPublishThrottled` | Der einzelne Stapel der Protokollereignisse, der aufgrund von Drosselungsfehlern nicht veröffentlicht wurde. |
| `NumLogEventsFailedToPublishThrottled` | Die Anzahl der Protokollereignisse innerhalb des Stapels, die aufgrund von Drosselungsfehlern nicht veröffentlicht wurden. |

## AWS IoT Core Metriken des Anbieters von Anmeldeinformationen

| Metrik | Beschreibung |
| --- | --- |
| `CredentialExchangeSuccess` | Die Anzahl der erfolgreichen `AssumeRoleWithCertificate` -Anforderungen an den Anbieter der AWS IoT Core Anmeldeinformationen. |

## Authentifizierungsmetriken

> **Note**
>
> Die Authentifizierungsmetriken werden in der CloudWatch Konsole unter Protokollmetriken angezeigt.

| Metrik | Beschreibung |
| --- | --- |
| `Connection.AuthNError` | Die Anzahl der Verbindungsversuche, die aufgrund von Authentifizierungsfehlern AWS IoT Core abgelehnt wurden. Diese Metrik berücksichtigt nur Verbindungen, die eine SNI-Zeichenfolge (Server Name Indication) senden, die einem Endpunkt von Ihnen entspricht. AWS-Konto Diese Metrik umfasst Verbindungsversuche von externen Quellen wie Internet-Scan-Tools oder Sondierungsaktivitäten. Die `Protocol` Dimension enthält das Protokoll, das zum Senden des Verbindungsversuchs verwendet wurde. |

## OCSP Stapling-Metriken für Serverzertifikate

| Metrik | Beschreibung |
| --- | --- |
| Data.Success abrufen OCSPStaple | Die OCSP-Antwort wurde erfolgreich empfangen und verarbeitet. Diese Antwort wird in den TLS-Hands |

| Metrik | Beschreibung |
| --- | --- |
| | hake für die konfigurierte Domain aufgenommen. Die `DomainConfigurationName` Dimension enthält den Namen der konfigurierten Domain mit aktiviertem Serverzertifikat OCSP Stapling. |

## Regelmetriken

| Metrik | Beschreibung |
| --- | --- |
| `ParseError` | Die Anzahl der JSON-Parsing-Fehler in Nachricht en zu einem Thema, das von einer Regel überwacht wird. Die Dimension `RuleName` enthält den Namen der Regel. |
| `RuleMessageThrottled` | Die Anzahl der Nachrichten, die von der Regeln-En gine aufgrund von schädlichem Verhalten gedrossel t wurden, oder weil die Anzahl der Nachrichten den Drosselungsgrenzwert der Regeln-Engine überschri tten hat. Die Dimension `RuleName` enthält den Namen der auszulösenden Regel. |
| `RuleNotFound` | Die auszulösende Regel konnte nicht gefunden werden. Die Dimension `RuleName` enthält den Namen der Regel. |
| `RulesExecuted` | Die Anzahl der ausgeführten AWS IoT Regeln. |
| `TopicMatch` | Die Anzahl der eingehenden Nachrichten zu einem Thema, das von einer Regel überwacht wird. Die Dimension `RuleName` enthält den Namen der Regel. |

## Regelaktionsmetriken

| Metrik | Beschreibung |
| --- | --- |
| `Failure` | Die Anzahl fehlgeschlagener Aufrufe von Regelaktionen. Die Dimension `RuleName` enthält den Namen der Regel, welche die Aktion vorgibt. Die Dimension `ActionType` enthält den Aktionstyp, der aufgerufen wurde. |
| `Success` | Die Anzahl erfolgreicher Aufrufe von Regelaktionen. Die Dimension `RuleName` enthält den Namen der Regel, welche die Aktion vorgibt. Die Dimension `ActionType` enthält den Aktionstyp, der aufgerufen wurde. |
| `ErrorActionFailure` | Die Anzahl der fehlgeschlagenen Fehleraktionen. Die Dimension `RuleName` enthält den Namen der Regel, welche die Aktion vorgibt. Die Dimension `ActionType` enthält den Aktionstyp, der aufgerufen wurde. |
| `ErrorActionSuccess` | Die Anzahl der erfolgreichen Fehleraktionen. Die Dimension `RuleName` enthält den Namen der Regel, welche die Aktion vorgibt. Die Dimension `ActionType` enthält den Aktionstyp, der aufgerufen wurde. |

## Aktionsspezifische HTTP-Metriken

| Metrik | Beschreibung |
| --- | --- |
| `HttpCode_Other` | Wird generiert, wenn der Statuscode der Antwort aus dem nachgeschalteten Webservice/der nachgeschalteten Anwendung nicht 2xx, 4xx oder 5xx ist. |

| Metrik | Beschreibung |
| --- | --- |
| `HttpCode_4XX` | Wird generiert, wenn der Statuscode der Antwort aus dem nachgeschalteten Webservice/der nachgeschalteten Anwendung zwischen 400 und 499 liegt. |
| `HttpCode_5XX` | Wird generiert, wenn der Statuscode der Antwort aus dem nachgeschalteten Webservice/der nachgeschalteten Anwendung zwischen 500 und 599 liegt. |
| `HttpInvalidUrl` | Wird generiert, wenn eine Endpunkt-URL nach dem Ersetzen von Ersetzungsvorlagen nicht mit `https://` beginnt. |
| `HttpRequestTimeout` | Wird generiert, wenn der nachgeschaltete Webservice/die nachgeschaltete Anwendung nicht innerhalb des Zeitlimits für die Anforderung antwortet. Weitere Informationen finden Sie unter Service Quotas. |
| `HttpUnknownHost` | Wird generiert, wenn zwar die URL gültig ist, der Service jedoch nicht vorhanden oder nicht erreichbar ist. |

## Message Broker-Metriken

> **Note**
>
> Die Message-Broker-Metriken werden in der CloudWatch Konsole unter Protocol Metrics angezeigt.

| Metrik | Beschreibung |
| --- | --- |
| `Connect.AuthError` | Die Anzahl der Verbindungsanforderungen, die vom Message Broker nicht autorisiert werden konnten. Die Dimension `Protocol` enthält das zum Senden der `CONNECT`-Mitteilung verwendete Protokoll. |

| Metrik | Beschreibung |
| --- | --- |
| `Connect.ClientError` | Die Anzahl der Verbindungsanforderungen, die abgewiesen wurden, weil die MQTT-Nachricht nicht den in AWS IoT-Kontingente definierten Anforderungen entsprach. Die Dimension `Protocol` enthält das zum Senden der `CONNECT`-Mitteilung verwendete Protokoll. |
| `Connect.ClientIDThrottle` | Die Anzahl der Verbindungsanforderungen, die gedrosselt wurden, weil der Client die zugelassene Verbindungsanforderungsrate für eine bestimmte Client-ID überschritten hat. Die Dimension `Protocol` enthält das zum Senden der `CONNECT`-Mitteilung verwendete Protokoll. |
| `Connect.ServerError` | Die Anzahl der Verbindungsanforderungen, die aufgrund eines internen Fehlers fehlgeschlagen sind. Die Dimension `Protocol` enthält das zum Senden der `CONNECT`-Mitteilung verwendete Protokoll. |
| `Connect.Success` | Die Anzahl erfolgreicher Verbindungen zum Message Broker. Die Dimension `Protocol` enthält das zum Senden der `CONNECT`-Mitteilung verwendete Protokoll. |
| `Connect.Throttle` | Die Anzahl der Verbindungsanforderungen, die gedrosselt wurden, weil das Konto die zugelassene Verbindungsanforderungsrate überschritten hat. Die Dimension `Protocol` enthält das zum Senden der `CONNECT`-Mitteilung verwendete Protokoll. |
| `Ping.Success` | Die Anzahl der vom Message Broker empfangenen Ping-Meldungen. Die Dimension `Protocol` enthält das zum Senden der Ping-Meldung verwendete Protokoll. |

| Metrik | Beschreibung |
| --- | --- |
| `PublishIn.AuthError` | Die Anzahl der Veröffentlichungsanforderungen, die vom Message Broker nicht autorisiert werden konnten. Die Dimension `Protocol` enthält das zum Veröffentlichen der Mitteilung verwendete Protokoll. HTTP Publish unterstützt diese Metrik nicht. |
| `PublishIn.ClientError` | Die Anzahl der Veröffentlichungsanforderungen, die vom Message Broker abgewiesen wurden, weil die Nachricht nicht den in AWS IoT-Kontingente definierten Anforderungen entsprach. Die Dimension `Protocol` enthält das zum Veröffentlichen der Mitteilung verwendete Protokoll. |
| `PublishIn.ServerError` | Die Anzahl der Veröffentlichungsanforderungen, die vom Message Broker aufgrund eines internen Fehlers nicht verarbeitet werden konnten. Die Dimension `Protocol` enthält das zum Senden der `PUBLISH`-Mitteilung verwendete Protokoll. |
| `PublishIn.Success` | Die Anzahl der Veröffentlichungsanforderungen, die vom Message Broker erfolgreich verarbeitet wurden. Die Dimension `Protocol` enthält das zum Senden der `PUBLISH`-Mitteilung verwendete Protokoll. |
| `PublishIn.Throttle` | Die Anzahl der Veröffentlichungsanforderungen, die gedrosselt wurden, weil der Client die zugelassene Rate für eingehende Mitteilungen überschritten hat. Die Dimension `Protocol` enthält das zum Senden der `PUBLISH`-Mitteilung verwendete Protokoll. HTTP Publish unterstützt diese Metrik nicht. |
| `PublishOut.AuthError` | Die Anzahl der vom Message Broker vorgenomm enen Veröffentlichungsanforderungen, die von AWS IoT nicht autorisiert werden konnten. Die Dimension `Protocol` enthält das zum Senden der `PUBLISH`-Mitteilung verwendete Protokoll. |

| Metrik | Beschreibung |
| --- | --- |
| `PublishOut.ClientError` | Die Anzahl der vom Message Broker ausgegebenen Veröffentlichungsanforderungen, die abgewiesen wurden, weil die Nachricht nicht den in AWS IoT-Kontingente definierten Anforderungen entsprach. Die Dimension `Protocol` enthält das zum Senden der `PUBLISH`-Mitteilung verwendete Protokoll. |
| `PublishOut.Success` | Die Anzahl der vom Message Broker erfolgreich vorgenommenen Veröffentlichungsanforderungen. Die Dimension `Protocol` enthält das zum Senden der `PUBLISH`-Mitteilung verwendete Protokoll. |
| `PublishOut.Throttle` | Die Anzahl der Veröffentlichungsanforderungen, die gedrosselt wurden, weil der Client die zugelassene Rate für ausgehende Mitteilungen überschritten hat. Die Dimension `Protocol` enthält das zum Senden der `PUBLISH`-Mitteilung verwendete Protokoll. |
| `PublishRetained.AuthError` | Die Anzahl der Veröffentlichungsanforderungen mit dem aktivierten `RETAIN`-Flag, die vom Message Broker nicht autorisiert werden konnten. Die Dimension `Protocol` enthält das zum Senden der `PUBLISH`-Mitteilung verwendete Protokoll. |
| `PublishRetained.ServerError` | Die Anzahl der Veröffentlichungsanforderungen, die vom Message Broker aufgrund eines internen Fehlers nicht verarbeitet werden konnten. Die Dimension `Protocol` enthält das zum Senden der `PUBLISH`-Mitteilung verwendete Protokoll. |
| `PublishRetained.Success` | Die Anzahl der Veröffentlichungsanforderungen mit dem aktiven `RETAIN`-Flag, die vom Message Broker erfolgreich verarbeitet wurden. Die Dimension `Protocol` enthält das zum Senden der `PUBLISH`-Mitteilung verwendete Protokoll. |

| Metrik | Beschreibung |
| --- | --- |
| `PublishRetained.Throttle` | Die Anzahl der Veröffentlichungsanforderungen mit dem aktiven `RETAIN`-Flag, die gedrosselt wurden, weil der Client die zugelassene Rate für eingehende Mitteilungen überschritten hat. Die Dimension `Protocol` enthält das zum Senden der `PUBLISH`-Mitteilung verwendete Protokoll. |
| `Queued.Success` | Die Anzahl der gespeicherten Nachrichten, die vom Message Broker erfolgreich verarbeitet wurden, für Clients, die von ihrer persistenten Sitzung getrennt wurden. Nachrichten mit einer QoS von 1 werden gespeichert, während ein Client mit einer persistenten Sitzung getrennt wird. |
| `Queued.Throttle` | Die Anzahl der Nachrichten, die nicht gespeichert werden konnten und gedrosselt wurden, während Clients mit persistenten Sitzungen getrennt wurden. Dies tritt auf, wenn Clients das Limit für Nachrichten in der Warteschlange pro Sekunde pro Konto überschreiten. Nachrichten mit einer QoS von 1 werden gespeichert, während ein Client mit einer persistenten Sitzung getrennt wird. |
| `Queued.ServerError` | Die Anzahl der Nachrichten, die aufgrund eines internen Fehlers für eine persistente Sitzung nicht gespeichert wurden. Wenn Clients mit einer persistenten Sitzung getrennt werden, dann werden Nachrichten mit einer Servicegüte (QoS) von 1 gespeichert. |
| `Subscribe.AuthError` | Die Anzahl der von einem Client vorgenommenen Abonnementanforderungen, die nicht autorisiert werden konnten. Die Dimension `Protocol` enthält das zum Senden der `SUBSCRIBE` -Mitteilung verwendete Protokoll. |

| Metrik | Beschreibung |
| --- | --- |
| `Subscribe.ClientError` | Die Anzahl der Abonnementanforderungen, die abgewiesen wurden, weil die `SUBSCRIBE` -Nachricht nicht den in AWS IoT-Kontingente definierten Anforderungen entsprach. Die Dimension `Protocol` enthält das zum Senden der `SUBSCRIBE` -Mitteilung verwendete Protokoll. |
| `Subscribe.ServerError` | Anzahl der Abonnementanforderungen, die aufgrund eines internen Fehlers abgelehnt wurden. Die Dimension `Protocol` enthält das zum Senden der `SUBSCRIBE` -Mitteilung verwendete Protokoll. |
| `Subscribe.Success` | Anzahl der Abonnementanforderungen, die vom Message Broker erfolgreich verarbeitet wurden. Die Dimension `Protocol` enthält das zum Senden der `SUBSCRIBE` -Mitteilung verwendete Protokoll. |
| `Subscribe.Throttle` | Die Anzahl der Abonnementanfragen, die gedrosselt wurden, weil die zulässigen Ratenlimits für Abonnementanfragen für Sie überschritten wurden. AWS-Konto Zu diesen Grenzwerten gehören Abonnements pro Sekunde pro Konto, Abonnements pro Konto und Abonnements pro Verbindung, die unter Grenzwerte und Kontingente für AWS IoT Core Nachrichtenbroker und Protokolle beschrieben sind. Die Dimension `Protocol` enthält das zum Senden der `SUBSCRIBE` -Mitteilung verwendete Protokoll. |
| `Throttle.Exceeded` | Diese Metrik wird angezeigt, CloudWatch wenn bei einem MQTT-Client die Anzahl der Pakete pro Sekunde pro Verbindungsebene gedrosselt wird. Diese Metrik gilt nicht für HTTP-Verbindungen. |

| Metrik | Beschreibung |
| --- | --- |
| `Unsubscribe.ClientError` | Die Anzahl der Abmeldeanforderungen, die abgelehnt wurden, weil die `UNSUBSCRIBE` -Nachricht nicht den in AWS IoT-Kontingente definierten Anforderungen entsprach. Die Dimension `Protocol` enthält das zum Senden der `UNSUBSCRIBE` -Mitteilung verwendete Protokoll. |
| `Unsubscribe.ServerError` | Anzahl der Abmeldeanforderungen, die aufgrund eines internen Fehlers abgelehnt wurden. Die Dimension `Protocol` enthält das zum Senden der `UNSUBSCRIBE` -Mitteilung verwendete Protokoll. |
| `Unsubscribe.Success` | Anzahl der Abmeldeanforderungen, die vom Message Broker erfolgreich verarbeitet wurden. Die Dimension `Protocol` enthält das zum Senden der `UNSUBSCRIBE` -Mitteilung verwendete Protokoll. |
| `Unsubscribe.Throttle` | Anzahl der Abmeldeanforderungen, die abgelehnt wurden, weil der Client die zugelassene Abmeldeanforderungsrate überschritten hat. Die Dimension `Protocol` enthält das zum Senden der `UNSUBSCRIBE` -Mitteilung verwendete Protokoll. |

## Geräteschatten-Metriken

> **Note**
>
> Die Device Shadow-Metriken werden in der CloudWatch Konsole unter Protocol Metrics angezeigt.

| Metrik | Beschreibung |
| --- | --- |
| `DeleteThingShadow.Accepted` | Die Anzahl der erfolgreich verarbeiteten `DeleteThingShadow` -Anforderungen. Die Dimension |

| Metrik | Beschreibung |
| --- | --- |
| | `Protocol` enthält das zum Senden der Anforderung verwendete Protokoll. |
| `GetThingShadow.Accepted` | Die Anzahl der erfolgreich verarbeiteten `GetThingShadow` -Anforderungen. Die Dimension `Protocol` enthält das zum Senden der Anforderung verwendete Protokoll. |
| `ListThingShadow.Accepted` | Die Anzahl der erfolgreich verarbeiteten `ListThingShadow` -Anforderungen. Die Dimension `Protocol` enthält das zum Senden der Anforderung verwendete Protokoll. |
| `UpdateThingShadow.Accepted` | Die Anzahl der erfolgreich verarbeiteten `UpdateThingShadow` -Anforderungen. Die Dimension `Protocol` enthält das zum Senden der Anforderung verwendete Protokoll. |

## Jobs-Metriken

| Metrik | Beschreibung |
| --- | --- |
| `CanceledJobExecutionCount` | Die Anzahl der Auftragsausführungen, deren Status sich `CANCELED` innerhalb eines Zeitraums geändert hat, der durch CloudWatch bestimmt wird. (Weitere Informationen zu CloudWatch Metriken finden Sie unter Amazon CloudWatch Metrics.) Die Dimension `JobId` enthält die ID des Auftrags. |
| `CanceledJobExecutionTotalCount` | Die Gesamtzahl der Auftragsausführungen mit dem Status `CANCELED` für den jeweiligen Auftrag. Die Dimension `JobId` enthält die ID des Auftrags. |

| Metrik | Beschreibung |
| --- | --- |
| `ClientErrorCount` | Die Anzahl der Clientfehler, die beim Ausführen des Auftrags aufgetreten sind. Die Dimension `JobId` enthält die ID des Auftrags. |
| `FailedJobExecutionCount` | Die Anzahl der Auftragsausführungen, deren Status sich `FAILED` innerhalb eines Zeitraums geändert hat, der durch CloudWatch bestimmt wird. (Weitere Informationen zu CloudWatch Metriken finden Sie unter Amazon CloudWatch Metrics.) Die Dimension `JobId` enthält die ID des Auftrags. |
| `FailedJobExecutionTotalCount` | Die Gesamtzahl der Auftragsausführungen mit dem Status `FAILED` für den jeweiligen Auftrag. Die Dimension `JobId` enthält die ID des Auftrags. |
| `InProgressJobExecutionCount` | Die Anzahl der Auftragsausführungen, deren Status sich `IN_PROGRESS` innerhalb eines Zeitraums geändert hat, der durch CloudWatch bestimmt wird. (Weitere Informationen zu CloudWatch Metriken finden Sie unter Amazon CloudWatch Metrics.) Die Dimension `JobId` enthält die ID des Auftrags. |
| `InProgressJobExecutionTotalCount` | Die Gesamtzahl der Auftragsausführungen mit dem Status `IN_PROGRESS` für den jeweiligen Auftrag. Die Dimension `JobId` enthält die ID des Auftrags. |
| `RejectedJobExecutionTotalCount` | Die Gesamtzahl der Auftragsausführungen mit dem Status `REJECTED` für den jeweiligen Auftrag. Die Dimension `JobId` enthält die ID des Auftrags. |
| `RemovedJobExecutionTotalCount` | Die Gesamtzahl der Auftragsausführungen mit dem Status `REMOVED` für den jeweiligen Auftrag. Die Dimension `JobId` enthält die ID des Auftrags. |

| Metrik | Beschreibung |
| --- | --- |
| `QueuedJobExecutionCount` | Die Anzahl der Auftragsausführungen, deren Status sich `QUEUED` innerhalb eines Zeitraums geändert hat, der durch CloudWatch bestimmt wird. (Weitere Informationen zu CloudWatch Metriken finden Sie unter Amazon CloudWatch Metrics.) Die Dimension `JobId` enthält die ID des Auftrags. |
| `QueuedJobExecutionTotalCount` | Die Gesamtzahl der Auftragsausführungen mit dem Status `QUEUED` für den jeweiligen Auftrag. Die Dimension `JobId` enthält die ID des Auftrags. |
| `RejectedJobExecutionCount` | Die Anzahl der Auftragsausführungen, deren Status sich `REJECTED` innerhalb eines Zeitraums geändert hat, der durch CloudWatch bestimmt wird. (Weitere Informationen zu CloudWatch Metriken finden Sie unter Amazon CloudWatch Metrics.) Die Dimension `JobId` enthält die ID des Auftrags. |
| `RemovedJobExecutionCount` | Die Anzahl der Auftragsausführungen, deren Status sich `REMOVED` innerhalb eines Zeitraums geändert hat, der durch CloudWatch bestimmt wird. (Weitere Informationen zu CloudWatch Metriken finden Sie unter Amazon CloudWatch Metrics.) Die Dimension `JobId` enthält die ID des Auftrags. |
| `ServerErrorCount` | Die Anzahl der Serverfehler, die beim Ausführen das Auftrags aufgetreten sind. Die Dimension `JobId` enthält die ID des Auftrags. |
| `SuccededJobExecutionCount` | Die Anzahl der Auftragsausführungen, deren Status sich `SUCCESS` innerhalb eines Zeitraums geändert hat, der durch CloudWatch bestimmt wird. (Weitere Informationen zu CloudWatch Metriken finden Sie unter Amazon CloudWatch Metrics.) Die Dimension `JobId` enthält die ID des Auftrags. |

| Metrik | Beschreibung |
| --- | --- |
| `SucceededJobExecutionTotalCount` | Die Gesamtzahl der Auftragsausführungen mit dem Status `SUCCESS` für den jeweiligen Auftrag. Die Dimension `JobId` enthält die ID des Auftrags. |

## Metriken für Device Defender-Prüfung

| Metrik | Beschreibung |
| --- | --- |
| `NonCompliantResources` | Die Anzahl der Ressourcen, die bei einer Prüfung als nicht konform befunden wurden. Das System meldet die Anzahl der Ressourcen, die bei der Prüfung eines durchgeführten Audits nicht konform waren. |
| `ResourcesEvaluated` | Die Anzahl der Ressourcen, die auf Konformität geprüft wurden. Das System meldet die Anzahl der Ressourcen, die für die Prüfung der durchgeführten Audits ausgewertet wurden. |
| `MisconfiguredDeviceDefenderNotification` | Benachrichtigt Sie, wenn Ihre SNS-Konfiguration für falsch konfiguriert AWS IoT Device Defender ist.<br><br>Dimensions (Abmessungen) |

## Metriken für Device Defender-Erkennung

| Metrik | Beschreibung |
| --- | --- |
| `NumOfMetricsExported` | Die Anzahl der Metriken, die für eine Cloud-seitige, geräteseitige oder benutzerdefinierte Metrik exportiert wurden. Das System meldet die Anzahl der für das Konto exportierten Metriken für eine bestimmte Metrik. Diese Metrik ist nur für Kunden verfügbar, die den Metrik-Export verwenden. |

| Metrik | Beschreibung |
| --- | --- |
| `NumOfMetricsSkipped` | Die Anzahl der Metriken, die für eine Cloud-sei tige, geräteseitige oder benutzerdefinierte Metrik übersprungen wurden. Das System meldet die Anzahl der Metriken, die für das Konto übersprun gen wurden, für eine bestimmte Metrik, da Device Defender Detect nicht genügend Berechtigungen zur Veröffentlichung im MQTT-Thema erteilt hat. Diese Metrik ist nur für Kunden verfügbar, die den Metrik-Export verwenden. |
| `NumOfMetricsExceedingSizeLi mit` | Die Anzahl der Metriken, die beim Export für eine Cloud-seitige, geräteseitige oder benutzerdefinierte Metrik übersprungen wurden, weil die Größe die Größenbeschränkungen für MQTT-Nachrichten überschreitet. Das System meldet die Anzahl der Metriken, die für den Export für das Konto übersprun gen wurden, und zwar für eine bestimmte Metrik, weil die Größe die Größenbeschränkungen von MQTT-Nachrichten überschreitet. Diese Metrik ist nur für Kunden verfügbar, die den Metrik-Export verwenden. |
| `Violations` | Die Anzahl der neuen Verletzungen des Sicherhei tsprofils, die seit der letzten Auswertung festgestellt wurden. Das System meldet die Anzahl der neuen Verstöße für das Konto, für ein bestimmtes Sicherhei tsprofil und für ein bestimmtes Verhalten eines bestimmten Sicherheitsprofils. |
| `ViolationsCleared` | Die Anzahl der Verstöße des Sicherheitsprofils, die seit der letzten Auswertung gelöst wurden. Das System meldet die Anzahl der gelösten Verstöße für das Konto, für ein bestimmtes Sicherheitsprofil und für ein bestimmtes Verhalten eines bestimmten Sicherheitsprofils. |

| Metrik | Beschreibung |
| --- | --- |
| `ViolationsInvalidated` | Die Anzahl der Verletzungen von Sicherheitsprofile n, für die seit der letzten Auswertung keine Informati onen mehr verfügbar sind (weil das meldende Gerät die Meldung eingestellt hat oder aus irgendeinem Grund nicht mehr überwacht wird). Das System meldet die Anzahl der ungültigen Verstöße für das gesamte Konto, für ein bestimmtes Sicherheitsprofil und für ein bestimmtes Verhalten eines bestimmten Sicherheitsprofils. |
| `MisconfiguredDeviceDefender Notification` | Benachrichtigt Sie, wenn Ihre SNS-Konfiguration für falsch konfiguriert ist. AWS IoT Device Defender<br><br>Dimensions (Abmessungen) |

## Gerätebereitstellungsmetriken

AWS IoT Kennzahlen zur Flottenbereitstellung

| Metrik | Beschreibung |
| --- | --- |
| `ApproximateNumberOfThingsRe gistered` | Die Anzahl der Objekte, die von Flottenbereitstellung registriert wurden.<br><br>Die Anzahl ist zwar im Allgemeinen korrekt, die verteilte Architektur von AWS IoT Core macht es jedoch schwierig, eine genaue Anzahl der registrie rten Objekte aufrechtzuerhalten.<br><br>Die nützlichste Statistik für diese Metrik ist:<br><br>• Max, um die Gesamtzahl der registrierten Objekte zu melden. Die Anzahl der Dinge, die während des CloudWatch Aggregationsfensters registriert wurden, finden Sie in der `RegisterT hingFailed` Metrik. |

| Metrik | Beschreibung |
| --- | --- |
| | Maße: ClaimCertificateId |
| `CreateKeysAndCertificateFailed` | Die Anzahl der Fehler, die beim Aufrufen der `CreateKeysAndCertificate` -MQTT-API aufgetreten sind.<br><br>Die Metrik wird sowohl bei Erfolg (Wert = 0) als auch bei Fehlschlag (Wert = 1) ausgegeben. Diese Metrik kann verwendet werden, um die Anzahl der Zertifikate nachzuverfolgen, die in den von ihnen CloudWatch unterstützten Aggregationsfenstern, z. B. 5 Minuten oder 1 Stunde, erstellt und registriert wurden.<br><br>Für diese Metrik sind folgende Statistiken verfügbar:<br><br>• Summe zur Angabe der Anzahl fehlgeschlagener Aufrufe.<br>• SampleCountum die Gesamtzahl der erfolgreichen und fehlgeschlagenen Aufrufe zu melden. |
| `CreateCertificateFromCsrFailed` | Die Anzahl der Fehler, die beim Aufrufen der `CreateCertificateFromCsr` -MQTT-API aufgetreten sind.<br><br>Die Metrik wird sowohl bei Erfolg (Wert = 0) als auch bei Fehlschlag (Wert = 1) ausgegeben. Diese Metrik kann verwendet werden, um die Anzahl der Dinge zu verfolgen, die während der von CloudWatch ihnen unterstützten Aggregationsfenster registriert wurden, z. B. 5 Minuten oder 1 Stunde.<br><br>Für diese Metrik sind folgende Statistiken verfügbar:<br><br>• Summe zur Angabe der Anzahl fehlgeschlagener Aufrufe.<br>• SampleCountum die Gesamtzahl der erfolgreichen und fehlgeschlagenen Aufrufe zu melden. |

| Metrik | Beschreibung |
| --- | --- |
| `RegisterThingFailed` | Die Anzahl der Fehler, die beim Aufrufen der `RegisterThing` -MQTT-API aufgetreten sind.<br><br>Die Metrik wird sowohl bei Erfolg (Wert = 0) als auch bei Fehlschlag (Wert = 1) ausgegeben. Diese Metrik kann verwendet werden, um die Anzahl der Dinge zu verfolgen, die während der von CloudWatch ihnen unterstützten Aggregationsfenster registriert wurden, z. B. 5 Minuten oder 1 Stunde. Die Gesamtzahl der registrierten Objekte finden Sie in der `Approxima teNumberOfThingsRegistered` -Metrik.<br><br>Für diese Metrik sind folgende Statistiken verfügbar:<br><br>• Summe zur Angabe der Anzahl fehlgeschlagener Aufrufe.<br>• SampleCountum die Gesamtzahl der erfolgreichen und fehlgeschlagenen Aufrufe zu melden.<br><br>Maße: TemplateName |

Just-in-time Metriken für die Bereitstellung

| Metrik | Beschreibung |
| --- | --- |
| `ProvisionThing.ClientError` | Gibt an, wie oft ein Gerät aufgrund eines Client-Fe hlers nicht bereitgestellt werden konnte. Beispiels weise war die in der Vorlage angegebene Richtlinie nicht vorhanden. |
| `ProvisionThing.ServerError` | Gibt an, wie oft ein Gerät aufgrund eines Serverfeh lers nicht bereitgestellt werden konnte. Kunden können erneut versuchen, das Gerät bereitzustellen, nachdem sie gewartet haben und sie können sich |

| Metrik | Beschreibung |
| --- | --- |
| | an AWS IoT wenden, falls das Problem weiterhin besteht. |
| `ProvisionThing.Success` | Die Anzahl der erfolgreich bereitgestellten Geräte. |

## LoRaWAN-Metriken

Die folgende Tabelle zeigt die Metriken AWS IoT Core für LoRa WAN. Weitere Informationen finden Sie unter AWS IoT Core LoRaWAN-Metriken.

AWS IoT Core für LoRa WAN-Metriken

| Metrik | Beschreibung |
| --- | --- |
| Aktive Geräte/Gateways | Die Anzahl der aktiven LoRa WAN-Geräte und Gateways in Ihrem Konto. |
| Anzahl der Uplink-Nachrichten | Die Anzahl der Uplink-Nachrichten, die innerhalb einer bestimmten Zeitdauer für alle aktiven Gateways und Geräte in Ihrem gesendet werden. AWS-Konto Uplink-Nachrichten sind Nachrichten, die von Ihrem Gerät an ein WAN gesendet werden. AWS IoT Core LoRa |
| Anzahl der Downlink-Nachrichten | Die Anzahl der Downlink-Nachrichten, die innerhalb einer bestimmten Zeitdauer für alle aktiven Gateways und Geräte in Ihrem gesendet werden. AWS-Konto Downlink-Nachrichten sind Nachrichten, die über das LoRa WAN an Ihr AWS IoT Core Gerät gesendet werden. |
| Rate des Nachrichtenverlusts | Nachdem Sie Ihr Gerät hinzugefügt und eine LoRa WAN-Verbindung hergestellt haben, kann Ihr Gerät eine Uplink-Nachricht initiieren, um Nachrichten mit der Cloud auszutauschen. AWS IoT Core Mithilfe |

| Metrik | Beschreibung |
| --- | --- |
| | dieser Metrik können Sie dann die Rate der verlorene n Uplink-Nachrichten verfolgen. |
| Metriken verbinden | Nachdem Sie Ihr Gerät und Ihr Gateway hinzugefügt haben, führen Sie ein Verbindungsverfahren durch, damit Ihr Gerät Uplink-Daten senden und mit dem AWS IoT Core WAN kommunizieren kann. LoRa Sie können diese Metrik verwenden, um Informationen zu den Beitrittsmetriken für alle aktiven Geräte in Ihrem zu erhalten. AWS-Konto |
| Anzeige der durchschnittlichen Stärke des empfangenen Signals (RSSI) | Sie können diese Metrik verwenden, um den durchschnittlichen RSSI (Received Signal Strength Indicator) innerhalb der angegebenen Zeitdauer zu überwachen. RSSI ist eine Messung, die angibt, ob das Signal stark genug für eine gute WLAN-Verb indung ist. Dieser Wert ist negativ und muss für eine starke Verbindung näher an Null liegen. |
| Durchschnittliches Signal-Rausch-Verh ältnis (SNR) | Sie können diese Metrik verwenden, um das durchschnittliche SNR (Signal-to-noise Verhältnis) innerhalb der angegebenen Zeitdauer zu überwache n. Das SNR ist eine Messung, die angibt, ob das empfangene Signal im Vergleich zum Geräuschp egel stark genug ist, um eine gute WLAN-Verbindung zu gewährleisten. Der SNR-Wert ist positiv und muss größer als Null sein, um anzuzeigen, dass die Signalleistung stärker ist als die Rauschleistung. |
| Verfügbarkeit des Gateways | Sie können diese Metrik verwenden, um Informati onen über die Verfügbarkeit dieses Gateways innerhalb eines bestimmten Zeitraums abzurufen. Diese Metrik zeigt die Websocket-Verbindungszeit dieses Gateways für einen bestimmten Zeitraum an. |

Just-in-time Metriken für die Bereitstellung

| Metrik | Beschreibung |
| --- | --- |
| `ProvisionThing.ClientError` | Gibt an, wie oft ein Gerät aufgrund eines Client-Fehlers nicht bereitgestellt werden konnte. Beispielsweise war die in der Vorlage angegebene Richtlinie nicht vorhanden. |
| `ProvisionThing.ServerError` | Gibt an, wie oft ein Gerät aufgrund eines Serverfehlers nicht bereitgestellt werden konnte. Kunden können erneut versuchen, das Gerät bereitzustellen, nachdem sie gewartet haben und sie können sich an AWS IoT wenden, falls das Problem weiterhin besteht. |
| `ProvisionThing.Success` | Die Anzahl der erfolgreich bereitgestellten Geräte. |

## Metriken zur Flottenindizierung

AWS IoT Metriken zur Flottenindizierung

| Metrik | Beschreibung |
| --- | --- |
| `NamedShadowCountForDynamicGroupQueryLimitExceeded` | In dynamischen Objektgruppen werden maximal 25 benannte Schatten pro Objekt für Abfragebegriffe verarbeitet, die nicht datenquellenspezifisch sind. Wird dieses Limit für ein Objekt überschritten, wird der Ereignistyp `NamedShadowCountForDynamicGroupQueryLimitExceeded` ausgegeben. |

## Dimensionen für Metriken

Metriken verwenden den Namespace und stellen Metriken für folgende Dimensionen bereit.

| Dimension | Beschreibung |
| --- | --- |
| `ActionType` | Der Aktionstyp, der in der Regel festgelegt ist, welche die Anforderung ausgelöst hat. |
| `BehaviorName` | Der Name des Sicherheitsprofilverhaltens von Device Defender Detect, das überwacht wird. |
| `ClaimCertificateId` | Die `certificateId` des Anspruchs, der für die Bereitstellung der Geräte verwendet wurde. |
| `CheckName` | Der Name der Audit-Prüfung für Device Defender, deren Ergebnisse überwacht werden. |
| `JobId` | Die ID des Auftrags, dessen Fortschritt oder erfolgreiche/fehlgeschlagene Nachrichtenverbindung überwacht wird |
| `Protocol` | Das für die Anforderung verwendete Protokoll. Gültige Werte sind: MQTT oder HTTP |
| `RuleName` | Der Name der von der Anforderung ausgelösten Regel. |
| `ScheduledAuditName` | Der Name der geplanten Audit-Prüfung mit Device Defender, deren Ergebnisse überwacht werden. Dies hat den Wert `0nDemand`, wenn die gemeldeten Ergebnisse für ein Audit gelten, das auf Abruf durchgeführt wurde. |
| `SecurityProfileName` | Der Name des Sicherheitsprofils von Device Defender Detect, dessen Verhalten überwacht wird. |
| `TemplateName` | Der Name der Bereitstellungsvorlage. |

| Dimension | Beschreibung |
| --- | --- |
| `SourceArn` | Bezieht sich auf das Sicherheitsprofil für Detect oder das Konto ARN für Audit. |
| `RoleArn` | Bezieht sich auf die Rolle, die Device Defender übernehmen wollte. |
| `TopicArn` | Bezieht sich auf das SNS-Thema, in dem Device Defender versucht hat, zu veröffentlichen. |
| `Error` | Enthält eine kurze Beschreibung des Fehlers, der beim Versuch, im SNS-Thema zu veröffentlichen, aufgetreten ist. Die möglichen Werte sind:<br>• "KMSKeyNotFound„: gibt an, dass der KMS-Schlü ssel für das Thema nicht existiert.<br>• "InvalidTopicName„: gibt an, dass das SNS-Thema nicht gültig ist.<br>• „KMSAccessVerweigert“: gibt an, dass die Rolle keine Berechtigungen für den KMS-Schlüssel für das Thema hat.<br>• "AuthorizationError„: gibt an, dass die angegeben e Rolle Device Defender nicht autorisiert, Beiträge zum SNS-Thema zu veröffentlichen.<br>• "SNSTopicNotFound„: gibt an, dass das angegebene SNS-Thema nicht existiert.<br>• "FailureToAssumeRole„: gibt an, dass die angegebene Rolle Device Defender nicht autorisie rt, die Rolle zu übernehmen.<br>• "CrossRegionSNSTopic„: gibt an, dass das SNS-Thema in einer anderen Region existiert. |

# Überwachung AWS IoT mithilfe von Protokollen CloudWatch

Wenn die AWS IoT Protokollierung aktiviert ist, werden Fortschrittsereignisse zu jeder Nachricht AWS IoT gesendet, die von Ihren Geräten über den Message Broker und die Rules Engine übertragen wird. In der CloudWatch Konsole werden CloudWatch Protokolle in einer Protokollgruppe mit dem Namen AWSIotLogs angezeigt.

Weitere Informationen zu CloudWatch Protokollen finden Sie unter CloudWatch Protokolle. Informationen zu unterstützten AWS IoT CloudWatch Protokollen finden Sie unterCloudWatch Protokolliert AWS IoT Protokolleinträge.

## AWS IoT Protokolle in der CloudWatch Konsole anzeigen

> **Note**
>
> Die `AWSIotLogsV2` Protokollgruppe ist in der CloudWatch Konsole erst sichtbar, wenn:
>
> - Sie haben die Anmeldung aktiviert AWS IoT. Weitere Informationen zur Aktivierung der Anmeldung finden Sie AWS IoT unter Konfigurieren Sie die AWS IoT Protokollierung
> - Einige Protokolleinträge wurden durch AWS IoT Operationen geschrieben.

Um Ihre AWS IoT Logs in der CloudWatch Konsole einzusehen

1. Navigieren Sie zu https://console.aws.amazon.com/cloudwatch/. Wählen Sie im Navigationsbereich Protokollgruppen aus.
2. Geben Sie in das Textfeld Filter die Zeichenfolge **`AWSIotLogsV2`** ein und drücken Sie die Eingabetaste.
3. Doppelklicken Sie auf die `AWSIotLogsV2`-Protokollgruppe .
4. Wählen Sie Alle durchsuchen aus. Eine vollständige Liste der für Ihr Konto generierten AWS IoT Protokolle wird angezeigt.
5. Wählen Sie das Erweiterungssymbol aus, um einen einzelnen Stream anzusehen.

Sie können auch eine Abfrage in das Textfeld Ereignisse filtern eingeben. Hier einige interessante Abfragen, die Sie ausprobieren können:

- `{ $.logLevel = "INFO" }`

Suchen Sie alle Protokolle mit der Protokollebene `INFO`.

- `{ $.status = "Success" }`

  Suchen Sie alle Protokolle mit dem Status `Success`.

- `{ $.status = "Success" && $.eventType = "GetThingShadow" }`

  Suchen Sie alle Protokolle mit dem Status `Success` und dem Ereignistyp `GetThingShadow`.

Weitere Informationen zum Erstellen von Filterausdrücken finden Sie unter CloudWatch Log-Abfragen.

## CloudWatch Protokolliert AWS IoT Protokolleinträge

Jede Komponente von AWS IoT generiert ihre eigenen Protokolleinträge. Jeder Protokolleintrag besitzt einen `eventType`, der die Operation angibt, die den Protokolleintrag generiert hat. In diesem Abschnitt werden die Protokolleinträge beschrieben, die von den folgenden AWS IoT -Komponenten generiert werden.

Themen

- Message Broker-Protokolleinträge
- OCSP-Protokolleinträge für Serverzertifikate
- Protokolleinträge „Geräteschatten“
- Protokolleinträge zur Regel-Engine
- Auftrag-Protokolleinträge
- Protokolleinträge für Gerätebereitstellung
- Protokolleinträge „Dynamische Objektgruppen“
- Protokolleinträge für die Flottenindizierung
- Allgemeine CloudWatch Log-Attribute

### Message Broker-Protokolleinträge

Der AWS IoT Message Broker generiert Protokolleinträge für die folgenden Ereignisse:

Themen

- Protokolleintrag „Connect“

- Protokolleintrag „Disconnect“
- GetRetainedMessage Protokolleintrag
- ListRetainedMessage Protokolleintrag
- Protokolleintrag „Publish-in“
- Protokolleintrag „Publish-Out“
- Protokolleintrag in der Warteschlange
- Protokolleintrag „Subscribe“
- Logeintrag abbestellen

Protokolleintrag „Connect“

Der AWS IoT Message Broker generiert einen Logeintrag mit einem `eventType` of, `Connect` wenn ein MQTT-Client eine Verbindung herstellt.

Beispiel für den Protokolleintrag „Connect“

```
{
    "timestamp": "2017-08-10 15:37:23.476",
    "logLevel": "INFO",
    "traceId": "20b23f3f-d7f1-feae-169f-82263394fbdb",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "Connect",
    "protocol": "MQTT",
    "clientId": "abf27092886e49a8a5c1922749736453",
    "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
    "sourceIp": "205.251.233.181",
    "sourcePort": 13490
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `Connect`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

Protokoll

Das für die Anforderung verwendete Protokoll. Gültige Werte sind `MQTT` oder `HTTP`.

sourceIp

Die IP-Adresse, von der die Anforderung stammt.

sourcePort

Der Port, von dem die Anforderung stammt.

Protokolleintrag „Disconnect“

Der AWS IoT Message Broker generiert einen Logeintrag mit einem `eventType` of, `Disconnect` wenn ein MQTT-Client die Verbindung trennt.

Beispiel für den Protokolleintrag „Disconnect“

```
{
    "timestamp": "2017-08-10 15:37:23.476",
    "logLevel": "INFO",
    "traceId": "20b23f3f-d7f1-feae-169f-82263394fbdb",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "Disconnect",
    "protocol": "MQTT",
    "clientId": "abf27092886e49a8a5c1922749736453",
    "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
    "sourceIp": "205.251.233.181",
    "sourcePort": 13490,
    "reason": "DUPLICATE_CLIENT_ID",
    "details": "A new connection was established with the same client ID",
    "disconnectReason": "CLIENT_INITIATED_DISCONNECT"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `Disconnect`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

Protokoll

Das für die Anforderung verwendete Protokoll. Gültige Werte sind `MQTT` oder `HTTP`.

sourceIp

Die IP-Adresse, von der die Anforderung stammt.

sourcePort

Der Port, von dem die Anforderung stammt.

Grund

Der Grund, warum der Client die Verbindung trennt.

Details

Eine kurze Erläuterung des Fehlers.

disconnectReason

Der Grund, warum der Client die Verbindung trennt.

### GetRetainedMessage Protokolleintrag

Der AWS IoT Message Broker generiert einen Logeintrag mit der Angabe `eventTypeGetRetainedMessage`, wann er aufgerufen [GetRetainedMessage](#)wird.

GetRetainedMessage Beispiel für einen Protokolleintrag

```
{
    "timestamp": "2017-08-07 18:47:56.664",
    "logLevel": "INFO",
    "traceId": "1a60d02e-15b9-605b-7096-a9f584a6ad3f",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "GetRetainedMessage",
    "protocol": "HTTP",
    "topicName": "a/b/c",
    "qos": "1",
    "lastModifiedDate": "2017-08-07 18:47:56.664"
```

```
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `GetRetainedMessage`-Protokolleinträge die folgenden Attribute:

lastModifiedDate

Datum und Uhrzeit der Epoche (in Millisekunden), zu der die hinterlegte Nachricht gespeichert wurde. AWS IoT

Protokoll

Das für die Anforderung verwendete Protokoll. Zulässiger Wert: `HTTP`.

qos

Das QoS (Quality of Service)-Niveau, das in der Veröffentlichungsanforderung verwendet wird. Gültige Werte sind `0` oder 1.

topicName

Der Name des abonnierten Themas.

ListRetainedMessage Protokolleintrag

Der AWS IoT Message Broker generiert einen Logeintrag mit der Angabe `eventTypeListRetainedMessage`, wann er aufgerufen `ListRetainedMessages`wird.

ListRetainedMessage Beispiel für einen Protokolleintrag

```
{
    "timestamp": "2017-08-07 18:47:56.664",
    "logLevel": "INFO",
    "traceId": "1a60d02e-15b9-605b-7096-a9f584a6ad3f",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "ListRetainedMessage",
    "protocol": "HTTP"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `ListRetainedMessage` Protokolleinträge die folgenden Attribute:

Protokoll

Das für die Anforderung verwendete Protokoll. Zulässiger Wert: `HTTP`.

Protokolleintrag „Publish-in“

Wenn der AWS IoT Message Broker eine MQTT-Nachricht empfängt, generiert er einen Logeintrag mit einem `eventType` of`Publish-In`.

Beispiel für den Protokolleintrag „Publish-in“

```
{
        "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": "abf27092886e49a8a5c1922749736453",
        "principalId":
 "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
        "sourceIp": "205.251.233.181",
        "sourcePort": 13490,
        "retain": "True"
    }
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `Publish-In`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

Protokoll

Das für die Anforderung verwendete Protokoll. Gültige Werte sind `MQTT` oder `HTTP`.

Beibehaltung

Das Attribut, das verwendet wird, wenn für eine Nachricht das RETAIN-Flag auf den Wert `True` festgelegt ist. Wenn für die Nachricht das RETAIN-Flag nicht festgelegt ist, erscheint dieses Attribut nicht im Protokolleintrag. Weitere Informationen finden Sie unter Beibehaltene MQTT-Meldungen.

sourceIp

Die IP-Adresse, von der die Anforderung stammt.

sourcePort

Der Port, von dem die Anforderung stammt.

topicName

Der Name des abonnierten Themas.

Protokolleintrag „Publish-Out“

Wenn der Message Broker eine MQTT-Nachricht veröffentlicht, generiert er einen Protokolleintrag mit dem `eventType` `Publish-Out`

Beispiel für den Protokolleintrag „Publish-Out“

```
{
    "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": "abf27092886e49a8a5c1922749736453",
    "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
    "sourceIp": "205.251.233.181",
    "sourcePort": 13490
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `Publish-Out`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des abonnierten Clients, der Nachrichten zu diesem MQTT-Thema empfängt.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

Protokoll

Das für die Anforderung verwendete Protokoll. Gültige Werte sind `MQTT` oder `HTTP`.

sourceIp

Die IP-Adresse, von der die Anforderung stammt.

sourcePort

Der Port, von dem die Anforderung stammt.

topicName

Der Name des abonnierten Themas.

### Protokolleintrag in der Warteschlange

Wenn ein Gerät mit einer persistenten Sitzung getrennt wird, speichert der MQTT-Nachrichtenbroker die Nachrichten des Geräts und AWS IoT generiert Protokolleinträge mit einem EventType von. `Queued` Weitere Informationen zu persistenten MQTT-Sitzungen finden Sie unter Persistente MQTT-Sitzungen.

Beispiel für einen Eintrag in das Fehlerprotokoll eines Servers in der Warteschlange

```
{
    "timestamp": "2022-08-10 15:39:30.961",
    "logLevel": "ERROR",
    "traceId": "672ec480-31ce-fd8b-b5fb-22e3ac420699",
    "accountId": "123456789012",
    "topicName": "$aws/things/MyThing/get",
    "clientId": "123123123",
    "qos": "1",
    "protocol": "MQTT",
    "eventType": "Queued",
    "status": "Failure",
    "details": "Server Error"
```

```
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `Queued` Server-Fehler-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, für den sich die Nachricht in der Warteschlange befindet.

Details

**`Server Error`**

Aufgrund eines Serverfehlers konnte die Nachricht nicht gespeichert werden.

Protokoll

Das für die Anforderung verwendete Protokoll. Dieser Wert ist immer `MQTT`.

qos

Die QoS (Quality of Service)-Ebene der Anforderung. Der Wert ist immer 1, da die Nachrichten mit QoS von 0 nicht gespeichert werden.

topicName

Der Name des abonnierten Themas.

Beispiel für einen Eintrag in einem Erfolgsprotokoll in der Warteschlange

```
{
    "timestamp": "2022-08-10 15:39:30.961",
    "logLevel": "INFO",
    "traceId": "672ec480-31ce-fd8b-b5fb-22e3ac420699",
    "accountId": "123456789012",
    "topicName": "$aws/things/MyThing/get",
    "clientId": "123123123",
    "qos": "1",
    "protocol": "MQTT",
    "eventType": "Queued",
    "status": "Success"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `Queued` erfolgreiche Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, für den sich die Nachricht in der Warteschlange befindet.

Protokoll

Das für die Anforderung verwendete Protokoll. Dieser Wert ist immer `MQTT`.

qos

Die QoS (Quality of Service)-Ebene der Anforderung. Der Wert ist immer 1, da die Nachrichten mit QoS von 0 nicht gespeichert werden.

topicName

Der Name des abonnierten Themas.

Beispiel für einen gedrosselten Protokolleintrag in der Warteschlange

```
{
    "timestamp": "2022-08-10 15:39:30.961",
    "logLevel": "ERROR",
    "traceId": "672ec480-31ce-fd8b-b5fb-22e3ac420699",
    "accountId": "123456789012",
    "topicName": "$aws/things/MyThing/get",
    "clientId": "123123123",
    "qos": "1",
    "protocol": "MQTT",
    "eventType": "Queued",
    "status": "Failure",
    "details": "Throttled while queueing offline message"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `Queued` gedrosselte Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, für den sich die Nachricht in der Warteschlange befindet.

Details

**`Throttled while queueing offline message`**

Der Client hat das Queued messages per second per account Limit überschritten, sodass die Nachricht nicht gespeichert wurde.

Protokoll

Das für die Anforderung verwendete Protokoll. Dieser Wert ist immer MQTT.

qos

Die QoS (Quality of Service)-Ebene der Anforderung. Der Wert ist immer 1, da die Nachrichten mit QoS von 0 nicht gespeichert werden.

topicName

Der Name des abonnierten Themas.

Protokolleintrag „Subscribe“

Der AWS IoT Message Broker generiert einen Logeintrag mit einem eventType of, Subscribe wenn ein MQTT-Client ein Thema abonniert.

Beispiel für den Protokolleintrag in MQTT-3-Subscribe

```
{
    "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": "abf27092886e49a8a5c1922749736453",
    "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
    "sourceIp": "205.251.233.181",
    "sourcePort": 13490
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten Subscribe-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

Protokoll

Das für die Anforderung verwendete Protokoll. Dieser Wert ist immer `MQTT`.

sourceIp

Die IP-Adresse, von der die Anforderung stammt.

sourcePort

Der Port, von dem die Anforderung stammt.

topicName

Der Name des abonnierten Themas.

Beispiel für den Protokolleintrag in MQTT-5-Subscribe

```
{
 "timestamp": "2022-11-30 16:24:15.628",
 "logLevel": "INFO",
 "traceId": "7aa5c38d-1b49-3753-15dc-513ce4ab9fa6",
 "accountId": "123456789012",
 "status": "Success",
 "eventType": "Subscribe",
 "protocol": "MQTT",
 "topicName": "test/topic1,$invalid/reserved/topic",
 "subscriptions": [
  {
   "topicName": "test/topic1",
   "reasonCode": 1
  },
  {
   "topicName": "$invalid/reserved/topic",
   "reasonCode": 143
  }
 ],
 "clientId": "abf27092886e49a8a5c1922749736453",
 "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
 "sourceIp": "205.251.233.181",
```

```
 "sourcePort": 13490
}
```

Für MQTT 5-Subscribe-Operationen enthalten MQTT 5-Protokolleinträge zusätzlich zu den Protokolleintragsattributen Allgemeine CloudWatch Log-Attribute und den MQTT 3-Subscribe-Protokolleintragsattributen das folgende Attribut: `Subscribe`

Abonnements

Eine Liste von Zuordnungen zwischen den angeforderten Themen in der Abonnement-Anforderung und dem individuellen MQTT 5-Ursachencode. Weitere Informationen finden Sie unter MQTT-Ursachencodes.

Logeintrag abbestellen

Der AWS IoT Message Broker generiert einen Logeintrag mit einem `eventType` of, `Unsubscribe` wenn ein MQTT-Client ein MQTT-Thema abbestellt.

Beispiel für einen MQTT-Abmelde-Logeintrag

```
{
    "timestamp": "2024-08-20 22:53:32.844",
    "logLevel": "INFO",
    "traceId": "db6bd09a-2c3f-1cd2-27cc-fd6b1ce03b58",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "Unsubscribe",
    "protocol": "MQTT",
    "clientId": "abf27092886e49a8a5c1922749736453",
    "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
    "sourceIp": "205.251.233.181",
    "sourcePort": 13490
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `Unsubscribe`-Protokolleinträge die folgenden Attribute:

Protokoll

Das für die Anforderung verwendete Protokoll. Dieser Wert ist immer `MQTT`.

clientId

Die ID des Clients, der die Anforderung stellt.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

sourceIp

Die IP-Adresse, von der die Anforderung stammt.

sourcePort

Der Port, von dem die Anforderung stammt.

## OCSP-Protokolleinträge für Serverzertifikate

AWS IoT Core generiert Protokolleinträge für das folgende Ereignis:

Themen

- OCSPStapleDatenprotokolleintrag abrufen
- Rufen Sie den OCSPStaple Datenprotokolleintrag für private Endpunkte ab

### OCSPStapleDatenprotokolleintrag abrufen

AWS IoT Core generiert einen Protokolleintrag mit dem Wert `eventType` von`RetrieveOCSPStapleData`, wenn der Server die OCSP-Stapeldaten abruft.

Beispiele für OCSPStaple Datenprotokolleinträge abrufen

Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag`Success`.

```
{
 "timestamp": "2024-01-30 15:39:30.961",
 "logLevel": "INFO",
 "traceId": "180532b7-0cc7-057b-687a-5ca1824838f5",
 "accountId": "123456789012",
 "status": "Success",
 "eventType": "RetrieveOCSPStapleData",
 "domainConfigName": "test-domain-config-name",
 "connectionDetails": {
```

```
  "httpStatusCode": "200",
  "ocspResponderUri": "http://ocsp.example.com",
  "sourceIp": "205.251.233.181",
  "targetIp": "250.15.5.3"
 },
 "ocspRequestDetails": {
  "requesterName": "iot.amazonaws.com",
  "requestCertId":
 "30:3A:30:09:06:05:2B:0E:03:02:1A:05:00:04:14:9C:FF:90:A1:97:B0:4D:6C:01:B9:69:96:D8:3E:E7:A2:
 },
 "ocspResponseDetails": {
  "responseCertId":
 "30:3A:30:09:06:05:2B:0E:03:02:1A:05:00:04:14:9C:FF:90:A1:97:B0:4D:6C:01:B9:69:96:D8:3E:E7:A2:
  "ocspResponseStatus": "successful",
  "certStatus": "good",
  "signature":
 "4C:6F:63:61:6C:20:52:65:73:70:6F:6E:64:65:72:20:53:69:67:6E:61:74:75:72:65",
  "thisUpdateTime": "Jan 31 01:21:02 2024 UTC",
  "nextUpdateTime": "Feb 02 00:21:02 2024 UTC",
  "producedAtTime": "Jan 31 01:37:03 2024 UTC",
  "stapledDataPayloadSize": "XXX"
 }
}
```

Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag`Failure`.

```
{
 "timestamp": "2024-01-30 15:39:30.961",
 "logLevel": "ERROR",
 "traceId": "180532b7-0cc7-057b-687a-5ca1824838f5",
 "accountId": "123456789012",
 "status": "Failure",
 "reason": "A non 2xx HTTP response was received from the OCSP responder.",
 "eventType": "RetrieveOCSPStapleData",
 "domainConfigName": "test-domain-config-name",
 "connectionDetails": {
  "httpStatusCode": "444",
  "ocspResponderUri": "http://ocsp.example.com",
  "sourceIp": "205.251.233.181",
  "targetIp": "250.15.5.3"
 },
 "ocspRequestDetails": {
  "requesterName": "iot.amazonaws.com",
```

```
  "requestCertId":
 "30:3A:30:09:06:05:2B:0E:03:02:1A:05:00:04:14:9C:FF:90:A1:97:B0:4D:6C:01:B9:69:96:D8:3E:E7:A2:
 }
}
```

Für den `RetrieveOCSPStaple` Vorgang enthalten die Allgemeine CloudWatch Log-Attribute Protokolleinträge zusätzlich zu den die folgenden Attribute:

Grund

Der Grund, warum der Vorgang fehlschlägt.

domainConfigName

Der Name Ihrer Domain-Konfiguration.

Verbindungsdetails

Eine kurze Erklärung der Verbindungsdetails.

- httpStatusCode

  HTTP-Statuscodes, die vom OCSP-Responder als Antwort auf die Anfrage des Clients an den Server zurückgegeben werden.

- ocspResponderUri

  Die OCSP-Responder-URI, die vom Serverzertifikat AWS IoT Core abgerufen wird.

- sourceIp

  Die Quell-IP-Adresse des Servers. AWS IoT Core

- Ziel-IP

  Die Ziel-IP-Adresse des OCSP-Responders.

ocspRequestDetails

Details der OCSP-Anfrage.

- Name des Anforderers

  Der Bezeichner für den AWS IoT Core Server, der eine Anfrage an den OCSP-Responder sendet.

- requestCertId

Die Zertifikat-ID der Anfrage. Dies ist die ID des Zertifikats, für das die OCSP-Antwort angefordert wird.

ocspResponseDetails

Details der OCSP-Antwort.

- responseCertId

  Die Zertifikat-ID der OCSP-Antwort.

- ocspResponseStatus

  Der Status der OCSP-Antwort.

- CertStatus

  Der Status des Zertifikats.

- signature

  Die Signatur, die von einer vertrauenswürdigen Entität auf die Antwort angewendet wurde.

- thisUpdateTime

  Der Zeitpunkt, zu dem der angezeigte Status bekanntermaßen korrekt ist.

- nextUpdateTime

  Der Zeitpunkt, zu dem oder vor dem neuere Informationen über den Status des Zertifikats verfügbar sein werden.

- producedAtTime

  Der Zeitpunkt, zu dem der OCSP-Responder diese Antwort signiert hat.

- stapledDataPayloadGröße

  Die Nutzdatengröße der gehefteten Daten.

Rufen Sie den OCSPStaple Datenprotokolleintrag für private Endpunkte ab

AWS IoT Core generiert einen Protokolleintrag mit dem Zeichen `eventType` von`RetrieveOCSPStapleData`, wenn der Server die OCSP-Stapeldaten abruft.

Rufen Sie Beispiele OCSPStaple für Datenprotokolleinträge für private Endpunkte ab

Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag von. `Success`


```
{
 "timestamp": "2024-01-30 15:39:30.961",
 "logLevel": "INFO",
 "traceId": "180532b7-0cc7-057b-687a-5ca1824838f5",
 "accountId": "123456789012",
 "status": "Success",
 "eventType": "RetrieveOCSPStapleData",
 "domainConfigName": "test-domain-config-name",
        "lambdaDetails": {
        "lambdaArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
        "sourceArn": "arn:aws:iot:us-west-2:123456789012:domainconfiguration/
testDomainConfigure/6bzfg"
      },
        "authorizedResponderArn": "arn:aws:acm:us-west-2:123456789012:certificate/
certificate_ID",
 "ocspRequestDetails": {
  "requesterName": "iot.amazonaws.com",
  "requestCertId":
 "30:3A:30:09:06:05:2B:0E:03:02:1A:05:00:04:14:9C:FF:90:A1:97:B0:4D:6C:01:B9:69:96:D8:3E:E7:A2:
 },
 "ocspResponseDetails": {
  "responderId": "04:C1:3F:8F:27:D6:49:13:F8:DE:B2:36:9D:85:8E:F8:31:3B:A6:D0"
               "responseCertId":
 "30:3A:30:09:06:05:2B:0E:03:02:1A:05:00:04:14:9C:FF:90:A1:97:B0:4D:6C:01:B9:69:96:D8:3E:E7:A2:
  "ocspResponseStatus": "successful",
  "certStatus": "good",
  "signature":
 "4C:6F:63:61:6C:20:52:65:73:70:6F:6E:64:65:72:20:53:69:67:6E:61:74:75:72:65",
  "thisUpdateTime": "Jan 31 01:21:02 2024 UTC",
  "nextUpdateTime": "Feb 02 00:21:02 2024 UTC",
  "producedAtTime": "Jan 31 01:37:03 2024 UTC",
  "stapledDataPayloadSize": "XXX"
 }
}
```


Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag`Failure`.


```
{
 "timestamp": "2024-01-30 15:39:30.961",
```

```
 "logLevel": "ERROR",
 "traceId": "180532b7-0cc7-057b-687a-5ca1824838f5",
 "accountId": "123456789012",
 "status": "Failure",
 "reason": "The payload returned by the Lambda function exceeds the maximum response
 size of 7 kilobytes.",
 "eventType": "RetrieveOCSPStapleData",
 "domainConfigName": "test-domain-config-name",
        "lambdaDetails": {
        "lambdaArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
        "sourceArn": "arn:aws:iot:us-west-2:123456789012:domainconfiguration/
testDomainConfigure/6bzfg"
      },
        "authorizedResponderArn": "arn:aws:acm:us-west-2:123456789012:certificate/
certificate_ID",
  "ocspRequestDetails": {
  "requesterName": "iot.amazonaws.com",
  "requestCertId":
 "30:3A:30:09:06:05:2B:0E:03:02:1A:05:00:04:14:9C:FF:90:A1:97:B0:4D:6C:01:B9:69:96:D8:3E:E7:A2:
 }
}
```

Für den `RetrieveOCSPStaple` Vorgang enthalten die Protokolleinträge für private Endgeräte zusätzlich zu den Attributen Allgemeine CloudWatch Log-Attribute und den Attributen im Protokolleintrag „OCSPStapleDaten abrufen“ die folgenden Attribute:

Lambda-Details

Einzelheiten der Lambda-Funktion.

- LambdaWarn

  ARN der Lambda-Funktion.

- Quelle: RN

  Der ARN der Domänenkonfiguration.

authorizedResponderArn

Der ARN des Authorizer-Responders, falls in der Domänenkonfiguration einer konfiguriert ist.

## Protokolleinträge „Geräteschatten“

Der AWS IoT Device Shadow-Dienst generiert Protokolleinträge für die folgenden Ereignisse:

Themen

- DeleteThingShadow Protokolleintrag
- GetThingShadow Protokolleintrag
- UpdateThingShadow Protokolleintrag

### DeleteThingShadow Protokolleintrag

Der Geräteschatten-Service generiert einen Protokolleintrag `eventType` für `DeleteThingShadow`, wenn eine Anforderung zum Löschen eines Geräteschattens empfangen wird.

DeleteThingShadow Beispiel für einen Protokolleintrag

```
{
    "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"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `DeleteThingShadow`-Protokolleinträge die folgenden Attribute:

deviceShadowName

Der Name des zu aktualisierenden Schattens.

Protokoll

Das für die Anforderung verwendete Protokoll. Gültige Werte sind `MQTT` oder `HTTP`.

topicName

Der Name des Themas, in dem die Anforderung veröffentlicht wurde.

### GetThingShadow Protokolleintrag

Der Geräteschatten-Service generiert einen Protokolleintrag mit `eventType` für `GetThingShadow`, wenn eine Abrufanforderung für einen Schatten empfangen wird.

#### GetThingShadow Beispiel für einen Protokolleintrag

```
{
    "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"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `GetThingShadow`-Protokolleinträge die folgenden Attribute:

deviceShadowName

Der Name des angefragten Schattens.

Protokoll

Das für die Anforderung verwendete Protokoll. Gültige Werte sind `MQTT` oder `HTTP`.

topicName

Der Name des Themas, in dem die Anforderung veröffentlicht wurde.

### UpdateThingShadow Protokolleintrag

Der Geräteschatten-Service generiert einen Protokolleintrag durch `eventType` `UpdateThingShadow`, wenn eine Anforderung zum Aktualisieren eines Geräteschattens empfangen wird.

#### UpdateThingShadow Beispiel für einen Protokolleintrag

```
{
    "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"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `UpdateThingShadow`-Protokolleinträge die folgenden Attribute:

deviceShadowName

Der Name des zu aktualisierenden Schattens.

Protokoll

Das für die Anforderung verwendete Protokoll. Gültige Werte sind `MQTT` oder `HTTP`.

topicName

Der Name des Themas, in dem die Anforderung veröffentlicht wurde.

## Protokolleinträge zur Regel-Engine

Die AWS IoT Regel-Engine generiert Protokolle für die folgenden Ereignisse:

Themen

- FunctionExecution Protokolleintrag
- RuleExecution Protokolleintrag
- RuleMatch Protokolleintrag
- RuleExecutionThrottled Protokolleintrag
- RuleNotFound Eintrag protokollieren
- StartingRuleExecution Eintrag protokollieren

### FunctionExecution Protokolleintrag

Die Regel-Engine generiert einen Protokolleintrag mit `eventType` von `FunctionExecution`, wenn die SQL-Abfrage einer Regel eine externe Funktion aufruft. Eine externe Funktion wird aufgerufen,

wenn die Aktion einer Regel eine HTTP-Anfrage an AWS IoT oder einen anderen Webdienst sendet (z. B. durch Aufrufen von `get_thing_shadow` oder`machinelearning_predict`).

FunctionExecution Beispiel für einen Protokolleintrag

```
{
    "timestamp": "2017-07-13 18:33:51.903",
    "logLevel": "DEBUG",
    "traceId": "180532b7-0cc7-057b-687a-5ca1824838f5",
    "status": "Success",
    "eventType": "FunctionExecution",
    "clientId": "N/A",
    "topicName":"rules/test",
    "ruleName": "ruleTestPredict",
    "ruleAction": "MachinelearningPredict",
    "resources": {
        "ModelId": "predict-model"
    },
    "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `FunctionExecution`-Protokolleinträge die folgenden Attribute:

clientId

N/A für `FunctionExecution`-Protokolle.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

Ressourcen

Eine Sammlung von Ressourcen, die von den Aktionen der Regel verwendet werden.

ruleName

Der Name der übereinstimmenden Regel.

topicName

Der Name des abonnierten Themas.

RuleExecution Protokolleintrag

Wenn die AWS IoT Regel-Engine die Aktion einer Regel auslöst, generiert sie einen `RuleExecution` Protokolleintrag.

RuleExecution Beispiel für einen Protokolleintrag

```
{
    "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": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `RuleExecution`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

Ressourcen

Eine Sammlung von Ressourcen, die von den Aktionen der Regel verwendet werden.

ruleAction

Der Name der ausgelösten Aktion.

ruleName

Der Name der übereinstimmenden Regel.

topicName

Der Name des abonnierten Themas.

RuleMatch Protokolleintrag

Die AWS IoT Regel-Engine generiert einen Protokolleintrag mit dem Zeichen `eventType` von`RuleMatch`, wenn der Message Broker eine Nachricht empfängt, die einer Regel entspricht.

RuleMatch Beispiel für einen Protokolleintrag

```
{
    "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": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `RuleMatch`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

ruleName

Der Name der übereinstimmenden Regel.

topicName

Der Name des abonnierten Themas.

RuleExecutionThrottled Protokolleintrag

Wenn eine Ausführung gedrosselt wird, generiert die AWS IoT Regel-Engine einen Protokolleintrag mit dem Wert von. `eventType` `RuleExecutionThrottled`

RuleExecutionThrottled Beispiel für einen Protokolleintrag

```
{
    "timestamp": "2017-10-04 19:25:46.070",
    "logLevel": "ERROR",
    "traceId": "30aa7ccc-1d23-0b97-aa7b-76196d83537e",
    "accountId": "123456789012",
    "status": "Failure",
    "eventType": "RuleMessageThrottled",
    "clientId": "abf27092886e49a8a5c1922749736453",
    "topicName": "$aws/rules/example_rule",
    "ruleName": "example_rule",
    "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
    "reason": "RuleExecutionThrottled",
    "details": "Exection of Rule example_rule throttled"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `RuleExecutionThrottled`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

Details

Eine kurze Erläuterung des Fehlers.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

Grund

Die Zeichenfolge "RuleExecutionThrottled“.

ruleName

Der Name der Regel, die ausgelöst werden soll.

topicName

Der Name des Themas, das veröffentlicht wurde.

### RuleNotFound Eintrag protokollieren

Wenn die AWS IoT Regelengine eine Regel mit einem bestimmten Namen nicht finden kann, generiert sie einen Protokolleintrag mit dem Wert `eventType` von`RuleNotFound`.

RuleNotFound Beispiel für einen Protokolleintrag

```
{
    "timestamp": "2017-10-04 19:25:46.070",
    "logLevel": "ERROR",
    "traceId": "30aa7ccc-1d23-0b97-aa7b-76196d83537e",
    "accountId": "123456789012",
    "status": "Failure",
    "eventType": "RuleNotFound",
    "clientId": "abf27092886e49a8a5c1922749736453",
    "topicName": "$aws/rules/example_rule",
    "ruleName": "example_rule",
    "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
    "reason": "RuleNotFound",
    "details": "Rule example_rule not found"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `RuleNotFound`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

Details

Eine kurze Erläuterung des Fehlers.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

Grund

Die Zeichenfolge "RuleNotFound“.

ruleName

Der Name der Regel, die nicht gefunden werden konnte.

topicName

Der Name des Themas, das veröffentlicht wurde.

### StartingRuleExecution Eintrag protokollieren

Wenn die AWS IoT Regel-Engine beginnt, die Aktion einer Regel auszulösen, generiert sie einen Protokolleintrag mit dem Wert `eventType` von`StartingRuleExecution`.

StartingRuleExecution Beispiel für einen Protokolleintrag

```
{
    "timestamp": "2017-08-10 16:32:46.002",
    "logLevel": "DEBUG",
    "traceId": "30aa7ccc-1d23-0b97-aa7b-76196d83537e",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "StartingRuleExecution",
    "clientId": "abf27092886e49a8a5c1922749736453",
    "topicName": "rules/test",
    "ruleName": "JSONLogsRule",
    "ruleAction": "RepublishAction",
    "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `rule`--Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

principalId

Die ID des Prinzipals, der die Anforderung stellt.

ruleAction

Der Name der ausgelösten Aktion.

ruleName

Der Name der übereinstimmenden Regel.

topicName

Der Name des abonnierten Themas.

## Auftrag-Protokolleinträge

Der AWS IoT Job-Service generiert Protokolleinträge für die folgenden Ereignisse. Protokolleinträge werden generiert, wenn eine MQTT- oder HTTP-Anforderung vom Gerät empfangen wird.

Themen

- DescribeJobExecution Protokolleintrag
- GetPendingJobExecution Protokolleintrag
- ReportFinalJobExecutionCount Protokolleintrag
- StartNextPendingJobExecution Protokolleintrag
- UpdateJobExecution Protokolleintrag

### DescribeJobExecution Protokolleintrag

Der AWS IoT Jobs-Service generiert einen Protokolleintrag mit `eventType` der Angabe von`DescribeJobExecution`, wenn der Dienst eine Anfrage zur Beschreibung einer Jobausführung erhält.

DescribeJobExecution Beispiel für einen Protokolleintrag

```
{
    "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."
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `GetJobExecution`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

clientToken

Ein eindeutiger Bezeichner, bei dem die Groß- und Kleinschreibung beachtet werden muss, um die Idempotenz der Anforderung sicherzustellen. Weitere Informationen finden Sie unter So wird Idempotenz sichergestellt.

Details

Weitere Informationen über den Jobs-Service.

jobId

Die Auftrags-ID für die Auftragsausführung.

Protokoll

Das für die Anforderung verwendete Protokoll. Gültige Werte sind `MQTT` oder `HTTP`.

topicName

Das für die Anforderung verwendete Thema.

### GetPendingJobExecution Protokolleintrag

Der AWS IoT Jobs-Dienst generiert einen Protokolleintrag mit der Angabe „`eventTypeVon“GetPendingJobExecution`, wenn der Dienst eine Anfrage zur Auftragsausführung erhält.

### GetPendingJobExecution Beispiel für einen Protokolleintrag

```
{
    "timestamp": "2018-06-13 17:45:17.197",
    "logLevel": "DEBUG",
    "accountId": "123456789012",
```

```
    "status": "Success",
    "eventType": "GetPendingJobExecution",
    "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."
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `GetPendingJobExecution`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

clientToken

Ein eindeutiger Bezeichner, bei dem die Groß- und Kleinschreibung beachtet werden muss, um die Idempotenz der Anforderung sicherzustellen. Weitere Informationen finden Sie unter So wird Idempotenz sichergestellt.

Details

Weitere Informationen über den Jobs-Service.

Protokoll

Das für die Anforderung verwendete Protokoll. Gültige Werte sind `MQTT` oder `HTTP`.

topicName

Der Name des abonnierten Themas.

ReportFinalJobExecutionCount Protokolleintrag

Der AWS IoT Jobs-Dienst generiert einen Protokolleintrag mit der Angabe „`entryTypeVon“ReportFinalJobExecutionCount`, wenn ein Job abgeschlossen ist.

ReportFinalJobExecutionCount Beispiel für einen Protokolleintrag

```
{
    "timestamp": "2017-08-10 19:44:16.776",
```

```
    "logLevel": "INFO",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "ReportFinalJobExecutionCount",
    "jobId": "002",
    "details": "Job 002 completed. QUEUED job execution count: 0 IN_PROGRESS job
 execution count: 0 FAILED job execution count: 0 SUCCEEDED job execution count: 1
 CANCELED job execution count: 0 REJECTED job execution count: 0 REMOVED job execution
 count: 0"
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `ReportFinalJobExecutionCount`-Protokolleinträge die folgenden Attribute:

Details

Weitere Informationen über den Jobs-Service.

jobId

Die Auftrags-ID für die Auftragsausführung.

StartNextPendingJobExecution Protokolleintrag

Wenn der AWS IoT Jobs-Service eine Anforderung zum Starten der nächsten ausstehenden Auftragsausführung erhält, generiert er einen Protokolleintrag mit dem Wert `eventType` von`StartNextPendingJobExecution`.

StartNextPendingJobExecution Beispiel für einen Protokolleintrag

```
{
    "timestamp": "2018-06-13 17:49:51.036",
    "logLevel": "DEBUG",
    "accountId": "123456789012",
    "status": "Success",
    "eventType": "StartNextPendingJobExecution",
    "protocol": "MQTT",
    "clientId": "95c47808-b1ca-4794-bc68-a588d6d9216c",
    "topicName": "$aws/things/95c47808-b1ca-4794-bc68-a588d6d9216c/jobs/start-next",
    "clientToken": "bd7447c4-3a05-49f4-8517-dd89b2c68d94",
    "details": "The request status is SUCCESS."
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `StartNextPendingJobExecution`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

clientToken

Ein eindeutiger Bezeichner, bei dem die Groß- und Kleinschreibung beachtet werden muss, um die Idempotenz der Anforderung sicherzustellen. Weitere Informationen finden Sie unter So wird Idempotenz sichergestellt.

Details

Weitere Informationen über den Jobs-Service.

Protokoll

Das für die Anforderung verwendete Protokoll. Gültige Werte sind `MQTT` oder `HTTP`.

topicName

Das für die Anforderung verwendete Thema.

### UpdateJobExecution Protokolleintrag

Der AWS IoT Jobs-Dienst generiert einen Protokolleintrag mit `eventType` der Angabe von`UpdateJobExecution`, wenn der Dienst eine Anforderung zur Aktualisierung einer Jobausführung erhält.

UpdateJobExecution Beispiel für einen Protokolleintrag

```
{
    "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."
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `UpdateJobExecution`-Protokolleinträge die folgenden Attribute:

clientId

Die ID des Clients, der die Anforderung stellt.

clientToken

Ein eindeutiger Bezeichner, bei dem die Groß- und Kleinschreibung beachtet werden muss, um die Idempotenz der Anforderung sicherzustellen. Weitere Informationen finden Sie unter So wird Idempotenz sichergestellt.

Details

Weitere Informationen über den Jobs-Service.

jobId

Die Auftrags-ID für die Auftragsausführung.

Protokoll

Das für die Anforderung verwendete Protokoll. Gültige Werte sind `MQTT` oder `HTTP`.

topicName

Das für die Anforderung verwendete Thema.

versionNumber

Die Version der Auftragsausführung.

## Protokolleinträge für Gerätebereitstellung

Der AWS IoT Device Provisioning-Dienst generiert Protokolle für die folgenden Ereignisse.

Themen

- GetDeviceCredentials Protokolleintrag
- ProvisionDevice Protokolleintrag

### GetDeviceCredentials Protokolleintrag

Der AWS IoT Device Provisioning-Dienst generiert einen Protokolleintrag mit der Angabe „Von“`GetDeviceCredential`, wenn ein Client anruft`GetDeviceCredential`. `eventType`

### GetDeviceCredentialsBeispiel für einen Protokolleintrag

```
{
  "timestamp" : "2019-02-20 20:31:22.932",
  "logLevel" : "INFO",
  "traceId" : "8d9c016f-6cc7-441e-8909-7ee3d5563405",
  "accountId" : "123456789101",
  "status" : "Success",
  "eventType" : "GetDeviceCredentials",
  "deviceCertificateId" :
 "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
  "details" : "Additional details about this log."
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `GetDeviceCredentials`-Protokolleinträge die folgenden Attribute:

Details

Eine kurze Erläuterung des Fehlers.

deviceCertificateId

Die ID des Gerätezertifikats.

### ProvisionDevice Protokolleintrag

Der AWS IoT Device Provisioning-Dienst generiert einen Protokolleintrag mit der Angabe „Von“`ProvisionDevice`, wenn ein Client anruft`ProvisionDevice`. `eventType`

### ProvisionDevice Beispiel für einen Protokolleintrag

```
{
  "timestamp" : "2019-02-20 20:31:22.932",
  "logLevel" : "INFO",
  "traceId" : "8d9c016f-6cc7-441e-8909-7ee3d5563405",
```

```
  "accountId" : "123456789101",
  "status" : "Success",
  "eventType" : "ProvisionDevice",
  "provisioningTemplateName" : "myTemplate",
  "deviceCertificateId" :
 "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
  "details" : "Additional details about this log."
 }
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `ProvisionDevice`-Protokolleinträge die folgenden Attribute:

Details

Eine kurze Erläuterung des Fehlers.

deviceCertificateId

Die ID des Gerätezertifikats.

provisioningTemplateName

Der Name der Bereitstellungsvorlage.

## Protokolleinträge „Dynamische Objektgruppen“

AWS IoT Dynamische Dinggruppen generieren Protokolle für das folgende Ereignis.

Themen

- AddThingToDynamicThingGroupsFailed Protokolleintrag

### AddThingToDynamicThingGroupsFailed Protokolleintrag

Wenn AWS IoT den angegebenen dynamischen Gruppen nichts hinzugefügt werden konnte, wird ein Protokolleintrag mit dem Wert `eventType` von generiert`AddThingToDynamicThingGroupsFailed`. Dies geschieht, wenn ein Objekt die Kriterien für die Mitgliedschaft in der dynamischen Objektgruppe erfüllt, es aber der dynamischen Gruppe nicht hinzugefügt werden konnte oder es aus der dynamischen Gruppe entfernt wurde. Dies kann aus folgenden Gründen passieren:

- Das Objekt gehört bereits der maximalen Anzahl von Gruppen an.

- Mithilfe der Option --override-dynamic-groups wurde das Objekt zu einer statischen Objektgruppe hinzugefügt. Es wurde aus einer dynamischen Objektgruppe entfernt, um dies möglich zu machen.

Weitere Informationen finden Sie unter Dynamische Objektgruppen – Einschränkungen und Konflikte.

AddThingToDynamicThingGroupsFailed Beispiel für einen Protokolleintrag

In diesem Beispiel ist der Protokolleintrag für einen Fehler `AddThingToDynamicThingGroupsFailed` zu sehen. In diesem Beispiel wurden die Kriterien für die Aufnahme in die unter aufgeführten dynamischen Dinggruppen TestThingerfülltdynamicThingGroupNames, es konnte aber nicht zu diesen dynamischen Gruppen hinzugefügt werden, wie unter beschriebenreason.

```
{
 "timestamp": "2020-03-16 22:24:43.804",
 "logLevel": "ERROR",
 "traceId": "70b1f2f5-d95e-f897-9dcc-31e68c3e1a30",
 "accountId": "57EXAMPLE833",
 "status": "Failure",
 "eventType": "AddThingToDynamicThingGroupsFailed",
 "thingName": "TestThing",
 "dynamicThingGroupNames": [
  "DynamicThingGroup11",
  "DynamicThingGroup12",
  "DynamicThingGroup13",
  "DynamicThingGroup14"
 ],
 "reason": "The thing failed to be added to the given dynamic thing group(s) because
 the thing already belongs to the maximum allowed number of groups."
}
```

Neben Allgemeine CloudWatch Log-Attribute enthalten `AddThingToDynamicThingGroupsFailed`-Protokolleinträge die folgenden Attribute:

dynamicThingGroupNamen

Ein Array der dynamischen Objektgruppen, denen das Objekt nicht hinzugefügt werden konnte.

Grund

Der Grund, warum das Objekt nicht zu den dynamischen Objektgruppen hinzugefügt werden konnte.

thingName

Der Name des Objekts, das keiner dynamischen Objektgruppe hinzugefügt werden konnte.

## Protokolleinträge für die Flottenindizierung

AWS IoT Bei der Flottenindizierung werden Protokolleinträge für die folgenden Ereignisse generiert.

Themen

- NamedShadowCountForDynamicGroupQueryLimitExceeded Protokolleintrag

NamedShadowCountForDynamicGroupQueryLimitExceeded Protokolleintrag

Für Abfragebegriffe, die nicht datenquellenspezifisch sind, werden in dynamischen Gruppen maximal 25 benannte Schatten pro Objekt verarbeitet. Wird dieses Limit für ein Objekt überschritten, wird der Ereignistyp `NamedShadowCountForDynamicGroupQueryLimitExceeded` ausgegeben.

NamedShadowCountForDynamicGroupQueryLimitExceeded Beispiel für einen Protokolleintrag

In diesem Beispiel ist der Protokolleintrag für einen Fehler `NamedShadowCountForDynamicGroupQueryLimitExceeded` zu sehen. In diesem Beispiel können Ergebnisse, die ausschließlich auf Werten `DynamicGroup` basieren, ungenau sein, wie im Feld `reason` beschrieben.

```
{
"timestamp": "2020-03-16 22:24:43.804",
"logLevel": "ERROR",
"traceId": "70b1f2f5-d95e-f897-9dcc-31e68c3e1a30",
"accountId": "571032923833",
"status": "Failure",
"eventType": "NamedShadowCountForDynamicGroupQueryLimitExceeded",
"thingName": "TestThing",
"reason": "A maximum of 25 named shadows per thing are processed for non-data source
 specific query terms in dynamic groups."
}
```

## Allgemeine CloudWatch Log-Attribute

Alle CloudWatch Log-Log-Einträge enthalten die folgenden Attribute:

accountId

Ihre AWS-Konto ID.

eventType

Der Ereignistyp, für den das Protokoll generiert wurde. Der Wert des Ereignistyps hängt vom Ereignis ab, das den Protokolleintrag generiert hat. Jede Beschreibung des Protokolleintrags enthält den Wert von `eventType` für diesen Protokolleintrag.

logLevel

Die verwendete Protokollierungsebene. Weitere Informationen finden Sie unter the section called “Protokollstufen”.

Status

Der Status der Anforderung.

Zeitstempel

Der UNIX-Zeitstempel für den Zeitpunkt, an dem der Client eine Verbindung zum AWS IoT - Message Broker hergestellt hat.

traceId

Eine zufällig erstellte Kennung, die verwendet werden kann, um alle Protokolle für eine bestimmte Anforderung zu korrelieren.

# Geräteseitige Protokolle auf Amazon hochladen CloudWatch

Sie können historische, geräteseitige Protokolle in Amazon hochladen, CloudWatch um die Aktivitäten eines Geräts vor Ort zu überwachen und zu analysieren. Geräteseitige Protokolle können System-, Anwendungs- und Geräteprotokolldateien enthalten. Dieser Prozess verwendet einen Aktionsparameter für CloudWatch Protokollregeln, um geräteseitige Protokolle in einer vom Kunden definierten Protokollgruppe zu veröffentlichen.

## Funktionsweise

Der Prozess beginnt, wenn ein AWS IoT Gerät MQTT-Nachrichten mit formatierten Protokolldateien an ein Thema sendet. AWS IoT Eine AWS IoT Regel überwacht das Nachrichtenthema und sendet die Protokolldateien an eine von Ihnen CloudWatch definierte Protokollgruppe. Sie können die Informationen dann überprüfen und analysieren.

Themen

- MQTT-Themen
- Regelaktion

## MQTT-Themen

Wählen Sie einen Namensraum für MQTT-Themen, den Sie für die Veröffentlichung der Protokolle verwenden werden. Wir empfehlen, das Format `$aws/rules/things/thing_name/logs` für den gemeinsamen Themenbereich und das Format `$aws/rules/things/thing_name/logs/errors` für Fehlerthemen zu verwenden Die Benennungsstruktur für Protokolle und Fehlerthemen wird empfohlen, ist aber nicht erforderlich. Weitere Informationen finden Sie in Der Entwurf von MQTT-Themen für AWS IoT Core.

Wenn Sie den empfohlenen Bereich für allgemeine Themen verwenden, verwenden Sie reservierte AWS IoT Basic-Ingest-Themen. AWS IoT Basic Ingest sendet Gerätedaten auf sichere Weise an die AWS Dienste, die durch AWS IoT Regelaktionen unterstützt werden. Dadurch wird der Broker für Pub/Sub Messaging aus dem Erfassungspfad entfernt, was ihn kostengünstiger macht. Weitere Informationen finden Sie unter Senken der Messaging-Kosten mit Basic Ingest.

Wenn Sie BatchMode zum Hochladen von Protokolldateien verwenden, müssen Ihre Nachrichten einem bestimmten Format folgen, das einen UNIX-Zeitstempel und eine UNIX-Nachricht enthält. Weitere Informationen finden Sie im CloudWatch Thema Anforderungen an das MQTT-Nachrichtenformat für BatchMode unter Regelaktion protokollieren.

## Regelaktion

Beim AWS IoT Empfang der MQTT-Nachrichten von den Client-Geräten überwacht eine AWS IoT Regel das vom Kunden definierte Thema und veröffentlicht den Inhalt in einer von Ihnen definierten CloudWatch Protokollgruppe. Dieser Prozess verwendet eine Regelaktion „ CloudWatch Logs“, um MQTT auf Batches von Protokolldateien zu überwachen. Weitere Informationen finden Sie unter AWS IoT Regelaktion „CloudWatch Logs“.

Batch-Modus

`batchMode`ist ein boolescher Parameter innerhalb der Regelaktion „ AWS IoT CloudWatch Logs“. Dieser Parameter ist optional und standardmäßig deaktiviert (`false`). Um geräteseitige Protokolldateien stapelweise hochzuladen, müssen Sie diesen Parameter bei der Erstellung der Regel aktivieren (`true`). AWS IoT Weitere Informationen finden Sie unter CloudWatch Protokolle im Abschnitt AWS IoT Regelaktionen.

# Geräteseitige Protokolle mithilfe von AWS IoT -Regeln hochladen

Sie können die AWS IoT Regel-Engine verwenden, um Protokolldatensätze aus vorhandenen geräteseitigen Protokolldateien (System-, Anwendungs- und Geräteclient-Logs) zu Amazon hochzuladen. CloudWatch Wenn geräteseitige Protokolle in einem MQTT-Thema veröffentlicht werden, überträgt die Aktion „Regeln CloudWatch protokollieren“ die Nachrichten in Logs. CloudWatch Dieser Prozess beschreibt, wie Geräteprotokolle stapelweise hochgeladen werden, wobei der `batchMode`-Aktionsparameter „Regeln“ aktiviert ist (auf `true` festgelegt).

Um mit dem Hochladen von geräteseitigen Protokollen zu beginnen, müssen CloudWatch Sie die folgenden Voraussetzungen erfüllen.

## Voraussetzungen

Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- Erstellen Sie mindestens ein IoT-Zielgerät, das AWS IoT Core als AWS IoT Ding registriert ist. Weitere Informationen finden Sie unter Ein Objekt erstellen.
- Ermitteln Sie den MQTT-Themenbereich für Erfassung und Fehler. Weitere Informationen zu MQTT-Themen und empfohlenen Namenskonventionen finden Sie im Abschnitt MQTT-Themen MQTT-Themen unter Geräteseitige Logs nach Amazon hochladen. CloudWatch

Weitere Informationen zu diesen Voraussetzungen finden Sie unter Geräteseitige Logs hochladen auf. CloudWatch

## Eine Protokollgruppe erstellen CloudWatch

Gehen Sie wie folgt vor, um eine CloudWatch Protokollgruppe zu erstellen. Wählen Sie die entsprechende Registerkarte aus, je nachdem, ob Sie die Schritte über AWS Management Console oder AWS Command Line Interface (AWS CLI) ausführen möchten.

AWS Management Console

Um eine CloudWatch Protokollgruppe zu erstellen, verwenden Sie AWS Management Console

1. Öffnen Sie das AWS Management Console und navigieren Sie zu CloudWatch.
2. Wählen Sie im Navigationsbereich Protokolle und dann Protokollgruppen aus.
3. Wählen Sie Protokollgruppe erstellen aus.

4. Aktualisieren Sie den Namen der Protokollgruppe und aktualisieren Sie optional die Felder mit den Aufbewahrungseinstellungen.
5. Wählen Sie Erstellen aus.

### AWS CLI

Um eine CloudWatch Protokollgruppe mit dem zu erstellen AWS CLI

1. Führen Sie den folgenden Befehl aus, um die Protokollgruppe zu erstellen. Weitere Informationen finden Sie `create-log-group` in der AWS CLI v2-Befehlsreferenz.

   Ersetzen Sie den Namen der Protokollgruppe im Beispiel (`uploadLogsGroup`) durch Ihren bevorzugten Namen.

   ```
   aws logs create-log-group --log-group-name uploadLogsGroup
   ```

2. Um zu überprüfen, ob die Protokollgruppe korrekt erstellt wurde, führen Sie den folgenden Befehl aus.

   ```
   aws logs describe-log-groups --log-group-name-prefix uploadLogsGroup
   ```

   Beispielausgabe:

   ```
   {
       "logGroups": [
           {
               "logGroupName": "uploadLogsGroup",
               "creationTime": 1674521804657,
               "metricFilterCount": 0,
               "arn": "arn:aws:logs:us-east-1:111122223333:log-
   group:uploadLogsGroup:*",
               "storedBytes": 0
           }
       ]
   }
   ```

## Erstellen einer Themenregel

Gehen Sie wie folgt vor, um eine AWS IoT Regel zu erstellen. Wählen Sie die entsprechende Registerkarte aus, je nachdem, ob Sie die Schritte lieber über AWS Management Console oder über AWS Command Line Interface (AWS CLI) ausführen möchten.

AWS Management Console

Um eine Themenregel zu erstellen, verwenden Sie den AWS Management Console

1. Öffnen Sie den Regel-Hub.
   a. Öffnen Sie die AWS Management Console und navigieren Sie zu AWS IoT.
   b. Wählen Sie in der Navigationsleiste Nachrichtenweiterleitung und dann Regeln aus.
   c. Wählen Sie Regel erstellen aus.
2. Geben Sie die Regeleigenschaften ein.
   a. Geben Sie einen alphanumerischen Regelnamen ein.
   b. (Optional) Geben Sie eine Regelbeschreibung und Tags ein.
   c. Wählen Sie Weiter aus.
3. Geben Sie eine SQL-Anweisung ein.
   a. Geben Sie eine SQL-Anweisung ein, die das MQTT-Thema verwendet, das Sie für die Erfassung definiert haben.

      Beispiel: `SELECT * FROM '$aws/rules/things/thing_name/logs'`
   b. Wählen Sie Weiter aus.
4. Geben Sie Regelaktionen ein.
   a. Wählen Sie im Menü Aktion 1 die Option CloudWatchProtokolle aus.
   b. Wählen Sie den Protokoll-Gruppennamen aus und wählen Sie dann die Protokollgruppe aus, die Sie erstellt haben.
   c. Wählen Sie Batch-Modus verwenden aus.
   d. Geben Sie die IAM-Rolle für die Regel an.

      Führen Sie die folgenden Schritte aus, wenn Sie eine IAM-Rolle für die Regel besitzen.

      1. Wählen Sie im Menü IAM-Rolle Ihre IAM-Rolle aus.

Führen Sie die folgenden Schritte aus, wenn Sie noch keine IAM-Rolle für die Regel besitzen.

1. Klicken Sie auf Neue Rolle erstellen.
2. Geben Sie unter Rollenname einen eindeutigen Namen ein und wählen Sie Erstellen aus.
3. Vergewissern Sie sich, dass der IAM-Rollenname im Feld IAM-Rolle korrekt ist.

e. Wählen Sie Weiter aus.

5. Überprüfen Sie die Vorlagenkonfiguration.

a. Überprüfen Sie die Einstellungen für die Auftragsvorlage, um sicherzustellen, dass sie korrekt sind.

b. Wählen Sie anschließend Erstellen aus.

AWS CLI

Um eine IAM-Rolle und eine Themenregel zu erstellen, verwenden Sie AWS CLI

1. Erstellen Sie eine IAM-Rolle, die Rechte für die AWS IoT Regel gewährt.

a. Erstellen Sie eine IAM-Richtlinie.

Führen Sie den folgenden Befehl aus, um eine IAM-Richtlinie zu erstellen. Stellen Sie sicher, dass Sie den Parameterwert `policy-name` aktualisieren. Weitere Informationen finden Sie `create-policy`in der AWS CLI v2-Befehlsreferenz.

> **Note**
>
> Wenn Sie ein Microsoft Windows-Betriebssystem verwenden, müssen Sie möglicherweise die Zeilenendemarkierung (\) durch ein Häkchen (`) oder ein anderes Zeichen ersetzen.

```
aws iam create-policy \
    --policy-name uploadLogsPolicy \
    --policy-document \
```

```
'{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iot:CreateTopicRule",
            "iot:Publish",
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:PutLogEvents",
            "logs:GetLogEvents"
        ],
        "Resource": "*"
    }
}'
```

b. Kopieren Sie den Richtlinien-ARN aus Ihrer Ausgabe in einen Texteditor.

Beispielausgabe:

```
{
    "Policy": {
        "PolicyName": "uploadLogsPolicy",
        "PermissionsBoundaryUsageCount": 0,
        "CreateDate": "2023-01-23T18:30:10Z",
        "AttachmentCount": 0,
        "IsAttachable": true,
        "PolicyId": "AAABBBCCCDDDEEEFFFGGG",
        "DefaultVersionId": "v1",
        "Path": "/",
        "Arn": "arn:aws:iam::111122223333:policy/uploadLogsPolicy",
        "UpdateDate": "2023-01-23T18:30:10Z"
    }
}
```

c. Erstellen Sie eine IAM-Rolle und eine Vertrauensrichtlinie.

Führen Sie den folgenden Befehl aus, um eine IAM-Richtlinie zu erstellen. Stellen Sie sicher, dass Sie den Parameterwert `role-name` aktualisieren. Weitere Informationen finden Sie `create-role` in der AWS CLI v2-Befehlsreferenz.

```
aws iam create-role \
--role-name uploadLogsRole \
```

```
--assume-role-policy-document \
'{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "iot.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}'
```

d. Hängen Sie die IAM-Richtlinie an die Rolle an.

Führen Sie den folgenden Befehl aus, um eine IAM-Richtlinie zu erstellen. Stellen Sie sicher, dass Sie die `role-name` und die Parameterwerte für `policy-arn` aktualisieren. Weitere Informationen finden Sie attach-role-policyin der AWS CLI v2-Befehlsreferenz.

```
aws iam attach-role-policy \
--role-name uploadLogsRole \
--policy-arn arn:aws:iam::111122223333:policy/uploadLogsPolicy
```

e. Überprüfen Sie die Rolle.

Um zu überprüfen, ob die IAM-Rolle korrekt erstellt wurde, führen Sie den folgenden Befehl aus. Stellen Sie sicher, dass Sie den Parameterwert `role-name` aktualisieren. Weitere Informationen finden Sie get-rolein der AWS CLI v2-Befehlsreferenz.

```
aws iam get-role --role-name uploadLogsRole
```

Beispielausgabe:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "uploadLogsRole",
        "RoleId": "AAABBBCCCDDDEEEFFFGGG",
        "Arn": "arn:aws:iam::111122223333:role/uploadLogsRole",
```

```
        "CreateDate": "2023-01-23T19:17:15+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "iot.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Description": "",
        "MaxSessionDuration": 3600,
        "RoleLastUsed": {}
    }
}
```

2. Erstellen Sie eine AWS IoT Themenregel in der AWS CLI.

   a. Führen Sie den folgenden Befehl aus, um eine AWS IoT Themenregel zu erstellen. Stellen Sie sicher, dass Sie die Werte für den `--rule-name` und die `sql`-Anweisung, `description`, `roleARN` und die Parameterwerte für `logGroupName` aktualisieren. Weitere Informationen finden Sie create-topic-rulein der AWS CLI v2-Befehlsreferenz.

```
aws iot create-topic-rule \
--rule-name uploadLogsRule \
--topic-rule-payload \
 '{
  "sql":"SELECT * FROM 'rules/things/thing_name/logs'",
  "description":"Upload logs test rule",
  "ruleDisabled":false,
  "awsIotSqlVersion":"2016-03-23",
  "actions":[
   {"cloudwatchLogs":
    {"roleArn":"arn:aws:iam::111122223333:role/uploadLogsRole",
    "logGroupName":"uploadLogsGroup",
    "batchMode":true}
    }
   ]
```

```
}'
```

b. Um zu überprüfen, ob die Regel korrekt erstellt wurde, führen Sie den folgenden Befehl aus. Stellen Sie sicher, dass Sie den Parameterwert `role-name` aktualisieren. Weitere Informationen finden Sie get-topic-rulein der AWS CLI v2-Befehlsreferenz.

```
aws iot get-topic-rule --rule-name uploadLogsRule
```

Beispielausgabe:

```
{
    "ruleArn": "arn:aws:iot:us-east-1:111122223333:rule/uploadLogsRule",
    "rule": {
        "ruleName": "uploadLogsRule",
        "sql": "SELECT * FROM rules/things/thing_name/logs",
        "description": "Upload logs test rule",
        "createdAt": "2023-01-24T16:28:15+00:00",
        "actions": [
            {
                "cloudwatchLogs": {
                    "roleArn": "arn:aws:iam::111122223333:role/
uploadLogsRole",
                    "logGroupName": "uploadLogsGroup",
                    "batchMode": true
                }
            }
        ],
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23"
    }
}
```

## Senden der geräteseitigen Protokolle an AWS IoT

Um geräteseitige Protokolle zu senden an AWS IoT

1. Um historische Protokolle an zu senden AWS IoT, kommunizieren Sie mit Ihren Geräten, um Folgendes sicherzustellen.

   - Die Protokollinformationen werden an den richtigen Themen-Namespace gesendet, wie im Abschnitt Voraussetzungen dieses Verfahrens angegeben.

Beispiel: `$aws/rules/things/thing_name/logs`

- Die Payload der MQTT-Nachricht ist korrekt formatiert. Weitere Informationen zum MQTT-Thema und zur empfohlenen Benennungskonvention finden Sie im folgenden MQTT-Themen Abschnitt in Geräteseitige Protokolle auf Amazon hochladen CloudWatch.

2. Vergewissern Sie sich, dass die MQTT-Nachrichten im AWS IoT MQTT-Client empfangen werden.

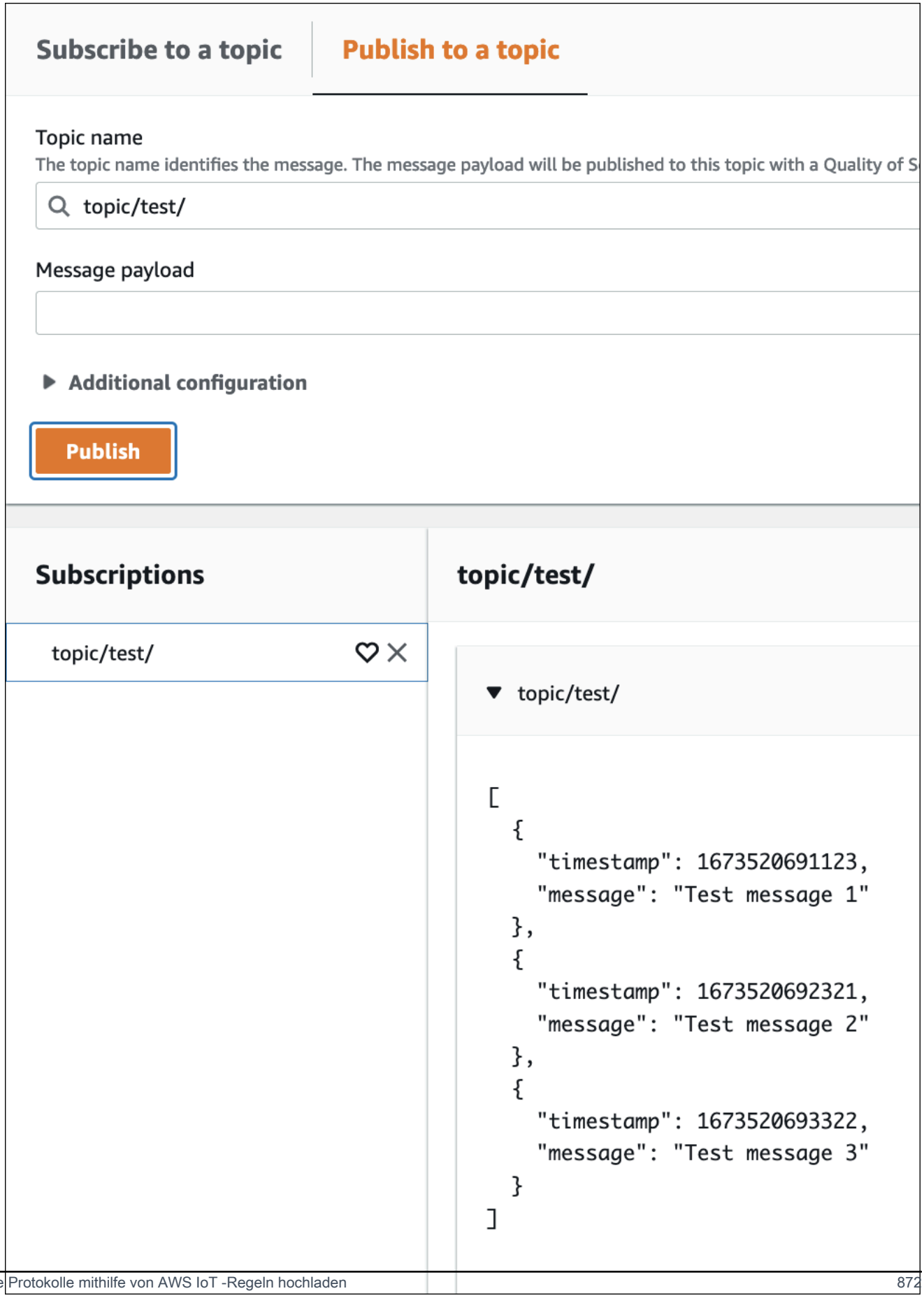
   a. Öffnen Sie das AWS Management Console und navigieren Sie zu. AWS IoT

   b. Um den MQTT-Testclient anzuzeigen, wählen Sie in der Navigationsleiste Test, MQTT-Testclient aus.

   c. Geben Sie unter Thema abonnieren, Themenfilter den Themen-Namespace ein.

   d. Wählen Sie Subscribe (Abonnieren) aus.

      MQTT-Nachrichten werden in der Tabelle Abonnements und Themen angezeigt, wie im Folgenden dargestellt. Der Erscheinen dieser Nachrichten kann bis zu fünf Minuten in Anspruch nehmen.


Subscribe to a topic
Publish to a topic
Topic name
The topic name identifies the message. The message payload will be published to this topic with a Quality of S
topic/test/
Message payload
Additional configuration
Publish
Subscriptions
topic/test/
topic/test/
topic/test/
[
{
"timestamp": 1673520691123,
"message": "Test message 1"
},
{
"timestamp": 1673520692321,
"message": "Test message 2"
},
{
"timestamp": 1673520693322,
"message": "Test message 3"
}
]

### Anzeige der Protokolldaten

Um Ihre Protokolldatensätze in CloudWatch Logs zu überprüfen

1. Öffnen Sie AWS Management Console das und navigieren Sie zu CloudWatch.
2. Wählen Sie in der Navigationsleiste Protokoll, Logs Insights aus.
3. Wählen Sie im Menü Protokollgruppe (n) auswählen die Protokollgruppe aus, die Sie in der AWS IoT Regel angegeben haben.
4. Wählen Sie auf der Seite Logs Insights die Option Abfrage ausführen aus.

## Protokollieren von AWS IoT API-Aufrufen mit AWS CloudTrail

AWS IoT ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurden AWS IoT. CloudTrail erfasst alle API-Aufrufe AWS IoT als Ereignisse, einschließlich Aufrufe von der AWS IoT Konsole und von Codeaufrufen an die AWS IoT APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS IoT. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, an die die Anfrage gestellt wurde AWS IoT, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und andere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

### AWS IoT Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität in stattfindet AWS IoT, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS IoT, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS-Region s. Der Trail protokolliert Ereignisse von allen

AWS-Region s in der AWS Partition und übermittelt die Protokolldateien an den Amazon S3 S3-Bucket, den Sie angeben. Sie können andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

> **Note**
>
> AWS IoT Aktionen auf der Datenebene (geräteseitig) werden nicht protokolliert CloudTrail. Wird verwendet CloudWatch , um diese Aktionen zu überwachen.

Im Allgemeinen werden Aktionen auf der AWS IoT Steuerungsebene, die Änderungen bewirken, von protokolliert CloudTrail. Bei Aufrufen wie CreateThingCreateKeysAndCertificate, und UpdateCertificatehinterlassen CloudTrail Einträge, bei Aufrufen wie ListThingsund ListTopicRulesnicht.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Gibt an, ob die Anforderung mit Root- oder IAM-Benutzer-Anmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

AWS IoT Aktionen sind in der AWS IoT API-Referenz dokumentiert. AWS IoT Wireless-Aktionen sind in der AWS IoT Wireless-API-Referenz dokumentiert.

# Grundlegendes zu AWS IoT Einträgen in Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `AttachPolicy` Aktion demonstriert.


```
{
    "timestamp":"1460159496",
    "AdditionalEventData":"",
    "Annotation":"",
    "ApiVersion":"",
    "ErrorCode":"",
    "ErrorMessage":"",
    "EventID":"8bff4fed-c229-4d2d-8264-4ab28a487505",
    "EventName":"AttachPolicy",
    "EventTime":"2016-04-08T23:51:36Z",
    "EventType":"AwsApiCall",
    "ReadOnly":"",
    "RecipientAccountList":"",
    "RequestID":"d4875df2-fde4-11e5-b829-23bf9b56cbcd",
    "RequestParamters":{
        "principal":"arn:aws:iot:us-
east-1:123456789012:cert/528ce36e8047f6a75ee51ab7beddb4eb268ad41d2ea881a10b67e8e76924d894",
        "policyName":"ExamplePolicyForIoT"
    },
    "Resources":"",
    "ResponseElements":"",
    "SourceIpAddress":"52.90.213.26",
    "UserAgent":"aws-internal/3",
    "UserIdentity":{
        "type":"AssumedRole",
        "principalId":"AKIAI44QH8DHBEXAMPLE",
        "arn":"arn:aws:sts::12345678912:assumed-role/iotmonitor-us-east-1-beta-
InstanceRole-1C5T1YCYMHPYT/i-35d0a4b6",
        "accountId":"222222222222",
```

```
        "accessKeyId":"access-key-id",
        "sessionContext":{
            "attributes":{
                "mfaAuthenticated":"false",
                "creationDate":"Fri Apr 08 23:51:10 UTC 2016"
            },
            "sessionIssuer":{
                "type":"Role",
                "principalId":"AKIAI44QH8DHBEXAMPLE",
                "arn":"arn:aws:iam::123456789012:role/executionServiceEC2Role/
iotmonitor-us-east-1-beta-InstanceRole-1C5T1YCYMHPYT",
                "accountId":"222222222222",
                "userName":"iotmonitor-us-east-1-InstanceRole-1C5T1YCYMHPYT"
            }
        },
        "invokedBy":{
            "serviceAccountId":"111111111111"
        }
    },
    "VpcEndpointId":""
}
```

# Regeln für AWS IoT

Regeln geben Ihren Geräten die Möglichkeit, mit ihnen zu interagieren AWS-Services. Das Analysieren von Regeln sowie das Ausführen von Aktionen erfolgt ausgehend vom MQTT-Topic-Stream. Sie können Regeln verwenden, um die folgenden Aufgaben zu unterstützen:

- Von einem Gerät empfangene Daten ausweiten oder filtern
- Von einem Gerät empfangene Daten in eine Amazon DynamoDB-Datenbank schreiben
- Speichern Sie eine Datei auf Amazon S3.
- Senden Sie eine Push-Benachrichtigung an alle Benutzer, die Amazon SNS verwenden.
- Veröffentlichen Sie Daten in einer Amazon SQS-Warteschlange.
- Rufen Sie eine Lambda-Funktion zum Extrahieren von Daten auf.
- Nachrichten von einer großen Anzahl an Geräten mithilfe von Amazon Kinesis verarbeiten
- Senden Sie Daten an Amazon OpenSearch Service.
- Erfassen Sie eine CloudWatch Metrik.
- Ändern Sie einen CloudWatch Alarm.
- Senden Sie die Daten aus einer MQTT-Nachricht an Amazon SageMaker AI, um Vorhersagen auf der Grundlage eines Modells für maschinelles Lernen (ML) zu treffen.
- Senden Sie eine Nachricht an einen Salesforce IoT-Eingabe-Stream.
- Sendet Nachrichtendaten an einen AWS IoT Analytics Kanal.
- Starten Sie den Prozess eines Step Functions-Zustandsautomaten.
- Sendet Nachrichtendaten an einen AWS IoT Events Eingang.
- Senden Sie Nachrichtendaten an eine Komponenteneigenschaft in AWS IoT SiteWise.
- Senden Sie Nachrichtendaten an eine Webanwendung oder einen Dienst.

Ihre Regeln können MQTT-Nachrichten verwenden, die über das Veröffentlichungs-/Abonnementprotokoll laufen, das von der the section called “Gerätekommunikationsprotokolle” unterstützt wird. Sie können auch die Funktion Basic Ingest verwenden, um Gerätedaten sicher an die zuvor AWS-Services aufgeführten Geräte zu senden, ohne dass Messaging-Kosten anfallen. Die Funktion Basic Ingest optimiert den Datenfluss durch Entfernen der Message Broker für Veröffentlichungen/Abonnements aus dem Aufnahmepfad, damit Daten ökonomischer übertragen werden. Dies macht es kostengünstig und behält gleichzeitig die Sicherheits- und Datenverarbeitungsfunktionen von bei. AWS IoT

Bevor Sie diese Aktionen ausführen AWS IoT können, müssen Sie dem Unternehmen die Erlaubnis erteilen, in Ihrem Namen auf Ihre AWS Ressourcen zuzugreifen. Wenn die Aktionen ausgeführt werden, fallen die Standardgebühren für die Aktionen an AWS-Services , die Sie verwenden.

Inhalt


- Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt
- Rollenberechtigungen weitergeben
- Eine AWS IoT Regel erstellen
- Eine Regel verwalten AWS IoT
- AWS IoT Regelaktionen
- Fehlerbehebung bei einer Regel
- Mithilfe von Regeln auf kontoübergreifende Ressourcen zugreifen AWS IoT
- Fehlerbehandlung (Fehleraktion)
- Senken der Messaging-Kosten mit Basic Ingest
- AWS IoT SQL-Referenz


# Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt

Verwenden Sie IAM-Rollen, um die AWS Ressourcen zu steuern, auf die jede Regel Zugriff hat. Bevor Sie eine Regel erstellen, müssen Sie eine IAM-Rolle mit einer Richtlinie erstellen, die den Zugriff auf die erforderlichen AWS Ressourcen ermöglicht. AWS IoT übernimmt diese Rolle bei der Implementierung einer Regel.

Gehen Sie wie folgt vor, um die IAM-Rolle und die AWS IoT IAM-Richtlinie zu erstellen, die einer AWS IoT Regel den erforderlichen Zugriff gewähren (AWS CLI).

1. Speichern Sie das folgende Dokument mit der Vertrauensrichtlinie, das die AWS IoT Berechtigung zur Übernahme der Rolle erteilt, in einer Datei mit dem Name`iot-role-trust.json`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "iot.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:iot:us-east-1:123456789012:rule/
rulename"
                }
            }
        }
    ]
}
```

Erstellen Sie mit dem Befehl create-role eine IAM-Rolle und geben Sie die Datei `iot-role-trust.json` an:

```
aws iam create-role --role-name my-iot-role --assume-role-policy-document
 file://iot-role-trust.json
```

Die Ausgabe dieses Befehls sieht wie folgt aus:

```
{
 "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. Speichern Sie den folgenden JSON-Code in einer Datei mit dem Namen `my-iot-policy.json`.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
```

```
    "Effect": "Allow",
    "Action": "dynamodb:*",
    "Resource": "*"
   }
  ]
}
```

Dieses JSON ist ein Beispiel für ein Richtliniendokument, das AWS IoT Administratorzugriff auf DynamoDB gewährt.

Verwenden Sie den Befehl create-policy, um AWS IoT Zugriff auf Ihre AWS Ressourcen zu gewähren, sobald Sie die Rolle übernommen haben, indem Sie die Datei übergeben: `my-iot-policy.json`

```
aws iam create-policy --policy-name my-iot-policy --policy-document file://my-iot-policy.json
```

Weitere Informationen darüber, wie Sie Zugriff auf AWS-Services In-Richtlinien für gewähren AWS IoT, finden Sie unter. Eine AWS IoT Regel erstellen

Die Ausgabe des Befehls create-policy enthält den ARN der Richtlinie. Anfügen der Richtlinie an eine Rolle.

```
{
 "Policy": {
  "PolicyName": "my-iot-policy",
  "CreateDate": "2015-09-30T19:31:18.620Z",
  "AttachmentCount": 0,
  "IsAttachable": true,
  "PolicyId": "ZXR6A36LTYANPAI7NJ5UV",
  "DefaultVersionId": "v1",
  "Path": "/",
  "Arn": "arn:aws:iam::123456789012:policy/my-iot-policy",
  "UpdateDate": "2015-09-30T19:31:18.620Z"
 }
}
```

3. Verwenden Sie den attach-role-policyBefehl, um Ihre Richtlinie an Ihre Rolle anzuhängen:

```
aws iam attach-role-policy --role-name my-iot-role --policy-arn
 "arn:aws:iam::123456789012:policy/my-iot-policy"
```

## Widerrufen Sie den Zugriff auf die Regelengine

Gehen Sie wie folgt vor, um den Zugriff auf die Regel-Engine sofort zu widerrufen

1. Entfernen Sie iot.amazonaws.com aus der Vertrauensrichtlinie
2. Folgen Sie den Schritten, um IoT-Rollensitzungen zu widerrufen

# Rollenberechtigungen weitergeben

Zu einer Regeldefinition gehört eine IAM-Rolle, die die Berechtigung zum Zugriff auf Ressourcen gewährt, welche in der Aktion der Regel festgelegt sind. Die Regel-Engine übernimmt diese Rolle, wenn die Aktion der Regel aufgerufen wird. Die Rolle muss genauso definiert sein AWS-Konto wie die Regel.

Bei Erstellen oder Ersetzen einer Rolle übergeben Sie eine Rolle an die Regel-Engine. Die `iam:PassRole` Berechtigung ist erforderlich, um diesen Vorgang durchzuführen. Sie können sicherstellen, dass Sie über diese Berechtigung verfügen, indem Sie eine Richtlinie erstellen, die die `iam:PassRole` Berechtigung gewährt, und diese an Ihren IAM-Benutzer anfügen. Die folgende Richtlinie zeigt, wie Sie die Berechtigung `iam:PassRole` für eine Rolle erlauben.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "Stmt1",
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
   ],
   "Resource": [
    "arn:aws:iam::123456789012:role/myRole"
   ]
  }
 ]
}
```

In diesem Richtlinienbeispiel wird die Berechtigung `iam:PassRole` für die Rolle `myRole` gewährt. Die Rolle wird mit dem ARN der Rolle angegeben. Fügen Sie diese Richtlinie Ihrem IAM-Benutzer

oder der Rolle zu, der Ihr Benutzer angehört. Weitere Informationen finden Sie unter Arbeiten mit verwalteten Richtlinien.

> **Note**
>
> Lambda-Funktionen verwenden eine ressourcenbasierte Richtlinie, wobei die Richtlinie direkt an die Lambda-Funktion selbst angefügt wird. Wenn Sie eine Regel erstellen, die eine Lambda-Funktion aufruft, übergeben Sie keine Rolle, sodass der Benutzer, der die Regel erstellt, die `iam:PassRole` Berechtigung nicht benötigt. Weitere Informationen zur Lambda-Funktionsautorisierung finden Sie unter Gewähren von Berechtigungen mit einer Ressourcenrichtlinie.

# Eine AWS IoT Regel erstellen

Sie können AWS IoT Regeln erstellen, um Daten von Ihren verbundenen Geräten weiterzuleiten, um mit anderen AWS Diensten zu interagieren. Eine AWS IoT Regel besteht aus den folgenden Komponenten:

Bestandteile einer Regel

| Komponente | Beschreibung | Erforderlich oder optional |
|---|---|---|
| Regelname | Der Name der Regel. Beachten Sie, dass wir die Verwendung personenbezogener Daten in Ihren Regelnamen nicht empfehlen. | Erforderlich |
| Regelbeschreibung | Ein Text mit einer Beschreibung der Regel Beachten Sie, dass wir die Verwendung personenbezogener Daten in Ihren Regelbeschreibungen nicht empfehlen. | Optional. |
| SQL-Anweisung | Eine vereinfachte SQL-Syntax zum Filtern von Nachrichten, die zu einem MQTT-Topic empfangen wurden, und zum Übertragen der Daten mithilfe von Push an einen anderen | Erforderlich |

| Komponente | Beschreibung | Erforderlich oder optional |
|---|---|---|
| | Speicherort. Weitere Informationen finden Sie unter AWS IoT SQL-Referenz. | |
| SQL-Version | Die Version der SQL-Regel-Engine, die beim Auswerten der Regel verwendet wird. Diese Eigenschaft ist zwar optional, wir empfehlen Ihnen jedoch dringend, die SQL-Version anzugeben. Die AWS IoT Core Konsole setzt diese Eigenschaft `2016-03-23` standardmäßig auf. Wenn diese Eigenschaft nicht festgelegt ist, z. B. in einem AWS CLI Befehl oder einer AWS CloudFormation Vorlage, `2015-10-08` wird sie verwendet. Weitere Informationen finden Sie unter SQL-Versionen. | Erforderlich |
| Eine oder mehrere Aktionen | Die Aktion wird AWS IoT ausgeführt, wenn die Regel in Kraft gesetzt wird. Sie können beispielsweise Daten in eine DynamoDB-Tabelle einfügen, Daten in einen Amazon S3-Bucket schreiben, in einem Amazon SNS-Thema veröffentlichen oder eine Lambda-Funktion aufrufen. | Erforderlich |
| Eine Fehleraktion | Die Aktion AWS IoT wird ausgeführt, wenn die Aktion einer Regel nicht ausgeführt werden kann. | Optional. |

Bevor Sie eine AWS IoT Regel erstellen, müssen Sie eine IAM-Rolle mit einer Richtlinie erstellen, die den Zugriff auf die erforderlichen AWS Ressourcen ermöglicht. AWS IoT übernimmt diese Rolle bei der Implementierung einer Regel. Weitere Informationen finden Sie unter Einer AWS IoT Regel den erforderlichen Zugriff gewähren und Rollenberechtigungen weitergeben.

Beachten Sie beim Erstellen einer Regel, wie viele Daten Sie in Themen veröffentlichen. Wenn Sie Regeln erstellen, die ein Themenmuster mit Platzhaltern enthalten, stimmen diese möglicherweise mit einem großen Prozentsatz Ihrer Nachrichten überein. In diesem Fall müssen Sie möglicherweise

die Kapazität der AWS Ressourcen erhöhen, die von den Zielaktionen verwendet werden. Wir empfehlen, Themenmuster mit Platzhaltern in Regeln zur erneuten Veröffentlichung zu vermeiden, um doppelte Verarbeitung zu vermeiden und die Kosten zu senken.

> **Note**
>
> Das Erstellen und Aktualisieren von Regeln sind Aktionen auf Administratorebene. Jeder Benutzer mit der Berechtigung zum Erstellen oder Aktualisieren von Regeln kann auf Daten zugreifen, die von den Regeln verarbeitet wurden.

## Erstellen Sie eine Regel (Konsole)

So erstellen Sie eine Regel (AWS Management Console)

Verwenden Sie den AWS Management ConsoleBefehl, um eine Regel zu erstellen:

1. Öffnen Sie die AWS IoT -Konsole.
2. Wählen Sie in der linken Navigationsleiste im Bereich Verwalten die Option Nachrichtenweiterleitung aus. Wählen Sie dann Regeln aus.
3. Wählen Sie auf der Seite Regeln die Option Regel erstellen aus.
4. Geben Sie auf der Seite Regeleigenschaften angeben einen Namen für Ihre Regel ein. Regelbeschreibung und Tags sind optional. Wählen Sie Weiter aus.
5. Wählen Sie auf der Seite „SQL-Anweisung konfigurieren“ eine SQL-Version aus und geben Sie eine SQL-Anweisung ein. Eine Beispiel-SQL-Anweisung kann sein`SELECT temperature FROM 'iot/topic' WHERE temperature > 50`. Weitere Informationen finden Sie unter SQL-Versionen und AWS IoT SQL-Referenz.
6. Fügen Sie auf der Seite „Regelaktionen anhängen“ Regelaktionen hinzu, um Daten an andere AWS Dienste weiterzuleiten.

    1. Wählen Sie unter Regelaktionen eine Regelaktion aus der Dropdownliste aus. Sie können beispielsweise Kinesis Stream wählen. Weitere Informationen zu Regelaktionen finden Sie unter AWS IoT Regelaktionen.
    2. Geben Sie je nach der ausgewählten Regelaktion die entsprechenden Konfigurationsdetails ein. Wenn Sie sich beispielsweise für Kinesis Stream entscheiden, müssen Sie eine Datenstream-Ressource auswählen oder erstellen und optional Konfigurationsdetails wie den Partitionsschlüssel eingeben, mit dem Daten in einem Stream nach Shard gruppiert werden.

3. Wählen oder erstellen Sie in der IAM-Rolle eine Rolle, um AWS IoT Zugriff auf Ihren Endpunkt zu gewähren. Beachten Sie, dass dadurch AWS IoT automatisch eine Richtlinie mit dem Präfix `aws-iot-rule` unter Ihrer ausgewählten IAM-Rolle erstellt wird. Sie können „Ansicht“ wählen, um Ihre IAM-Rolle und die Richtlinie von der IAM-Konsole aus anzuzeigen. Die Aktion „Fehler“ ist optional. Weitere Informationen finden Sie unter Fehlerbehandlung (Fehleraktion). Weitere Informationen zum Erstellen einer IAM-Rolle für Ihre Regel finden Sie unter Gewähren Sie einer Regel den erforderlichen Zugriff. Wählen Sie Weiter aus.

7. Überprüfen Sie auf der Seite Überprüfen und erstellen die gesamte Konfiguration und nehmen Sie bei Bedarf Änderungen vor. Wählen Sie Erstellen aus.

Nachdem Sie eine Regel erfolgreich erstellt haben, wird die Regel auf der Seite Regeln aufgeführt. Sie können eine Regel auswählen, um die Detailseite zu öffnen, auf der Sie eine Regel anzeigen, bearbeiten, eine Regel deaktivieren und eine Regel löschen können.

## Regel erstellen (CLI)

So erstellen Sie eine Regel (AWS CLI)

Verwenden Sie den create-topic-ruleBefehl, um eine Regel zu erstellen:

```
aws iot create-topic-rule --rule-name myrule --topic-rule-payload file://myrule.json
```

Im Folgenden finden Sie ein Beispiel für eine Nutzlastdatei mit einer Regel, die alle an das `iot/test` Thema gesendeten Nachrichten in die angegebene DynamoDB-Tabelle einfügt. Die SQL-Anweisung filtert die Nachrichten und der Rollen-ARN gewährt die AWS IoT Berechtigung, in die DynamoDB-Tabelle zu schreiben.

```
{
 "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()}"
   }
  }
 ]
}
```

Im Folgenden finden Sie ein Beispiel für eine Nutzlastdatei mit einer Regel, die alle an das `iot/test` Thema gesendeten Nachrichten in den angegebenen S3-Bucket einfügt. Die SQL-Anweisung filtert die Nachrichten, und die Rolle ARN gewährt die AWS IoT Erlaubnis, in den Amazon S3 S3-Bucket zu schreiben.

```
{
 "awsIotSqlVersion": "2016-03-23",
 "sql": "SELECT * FROM 'iot/test'",
 "ruleDisabled": false,
 "actions": [
  {
   "s3": {
    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_s3",
    "bucketName": "amzn-s3-demo-bucket",
    "key": "myS3Key"
   }
  }
 ]
}
```

Im Folgenden finden Sie ein Beispiel für eine Payload-Datei mit einer Regel, die Daten an Amazon OpenSearch Service überträgt:

```
{
 "sql": "SELECT *, timestamp() as timestamp FROM 'iot/test'",
 "ruleDisabled": false,
 "awsIotSqlVersion": "2016-03-23",
 "actions": [
  {
   "OpenSearch": {
    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_es",
    "endpoint": "https://my-endpoint",
    "index": "my-index",
    "type": "my-type",
    "id": "${newuuid()}"
   }
```

```
  }
 ]
}
```

Im Folgenden finden Sie ein Beispiel für eine Nutzlastdatei mit einer Regel, die eine Lambda-Funktion aufruft:

```
{
 "sql": "expression",
 "ruleDisabled": false,
 "awsIotSqlVersion": "2016-03-23",
 "actions": [
  {
   "lambda": {
    "functionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-lambda-function"
   }
  }
 ]
}
```

Im Folgenden finden Sie ein Beispiel für eine Nutzlastdatei mit einer Regel, die in einem Amazon SNS-Thema veröffentlicht:

```
{
 "sql": "expression",
 "ruleDisabled": false,
 "awsIotSqlVersion": "2016-03-23",
 "actions": [
  {
   "sns": {
    "targetArn": "arn:aws:sns:us-west-2:123456789012:my-sns-topic",
    "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"
   }
  }
 ]
}
```

Im Folgenden finden Sie ein Beispiel für eine Nutzlastdatei mit einer Regel, die in einem anderen MQTT-Topic erneut veröffentlicht:

```
{
```

```
 "sql": "expression",
 "ruleDisabled": false,
 "awsIotSqlVersion": "2016-03-23",
 "actions": [
  {
   "republish": {
    "topic": "my-mqtt-topic",
    "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"
   }
  }
 ]
}
```

Im Folgenden finden Sie ein Beispiel für eine Payload-Datei mit einer Regel, die Daten in einen Amazon Data Firehose überträgt:

```
{
 "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"
   }
  }
 ]
}
```

Im Folgenden finden Sie ein Beispiel für eine Payload-Datei mit einer Regel, die die Amazon SageMaker `machinelearning_predict` AI-Funktion verwendet, um erneut zu einem Thema zu veröffentlichen, wenn die Daten in der MQTT-Payload als 1 klassifiziert sind.

```
{
 "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"
   }
  }
 ]
}
```

Es folgt ein Beispiel für eine Nutzlastdatei mit einer Regel, nach der Nachrichten in einem Salesforce IoT Cloud-Input-Stream veröffentlicht werden.

```
{
 "sql": "expression",
 "ruleDisabled": false,
 "awsIotSqlVersion": "2016-03-23",
 "actions": [
  {
   "salesforce": {
    "token": "ABCDEFGHI123456789abcdefghi123456789",
    "url": "https://ingestion-cluster-id.my-env.sfdcnow.com/streams/stream-id/
connection-id/my-event"
   }
  }
 ]
}
```

Im Folgenden finden Sie ein Beispiel für eine Nutzlastdatei mit einer Regel, die eine Ausführung eines Step Functions-Zustandsautomaten startet.

```
{
 "sql": "expression",
 "ruleDisabled": false,
 "awsIotSqlVersion": "2016-03-23",
 "actions": [
  {
   "stepFunctions": {
    "stateMachineName": "myCoolStateMachine",
    "executionNamePrefix": "coolRunning",
    "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"
   }
  }
 ]
}
```

# Eine Regel verwalten AWS IoT

Sie können die folgenden Aktionen verwenden, um Ihre AWS IoT Regeln zu verwalten.

In diesem Thema:


- Eine Regel taggen
- Eine Regel anzeigen
- Löschen einer Regel


## Eine Regel taggen

Um Ihren neuen oder bestehenden Regeln eine weitere Ebene der Spezifität hinzuzufügen, können Sie sie mit Tags versehen. Beim Taggen werden Schlüssel-Wert-Paare in Ihren Regeln genutzt, sodass Sie besser kontrollieren können, wie und wo Ihre Regeln auf Ihre Ressourcen und Dienste angewendet werden. AWS IoT Sie können den Geltungsbereich Ihrer Regel beispielsweise so einschränken, dass sie nur in Ihrer Beta-Umgebung für Tests vor der Veröffentlichung gilt (`Key=environment, Value=beta`) oder alle Nachrichten, die nur von einem bestimmten Endpunkt an das `iot/test` Thema gesendet wurden, erfasst und in einem Amazon S3-Bucket speichert.

Beispiel für IAM-Richtlinien

Ein Beispiel, das zeigt, wie Tagging-Berechtigungen für eine Regel erteilt werden, stellen Sie sich einen Benutzer vor, der den folgenden Befehl ausführt, um eine Regel zu erstellen und sie so zu kennzeichnen, dass sie nur für seine Beta-Umgebung gilt.

Ersetzen Sie im Beispiel:

- *`MyTopicRuleName`*mit dem Namen der Regel.
- *`myrule.json`*mit dem Namen des Richtliniendokuments.

```
aws iot create-topic-rule
    --rule-name MyTopicRuleName
    --topic-rule-payload file://myrule.json
    --tags "environment=beta"
```

Für dieses Beispiel müssen Sie die folgende IAM-Richtlinie verwenden:

```
{
    "Version": "2012-10-17",
    "Statement":
    {
        "Action": [ "iot:CreateTopicRule", "iot:TagResource" ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:iot:us-east-1:123456789012:rule/MyTopicRuleName"
        ]
    }
}
```

Das obige Beispiel zeigt eine neu erstellte Regel namens `MyTopicRuleName`, die nur für Ihre Beta-Umgebung gilt. Die `iot:TagResource` in der Grundsatzerklärung mit `MyTopicRuleName` ausdrücklich genannte Option ermöglicht das Taggen bei der Erstellung oder Aktualisierung von `MyTopicRuleName`. Der bei der Erstellung der Regel verwendete Parameter `--tags "environment=beta"` beschränkt den Geltungsbereich von `MyTopicRuleName` nur auf Ihre Beta-Umgebung. Wenn Sie den Parameter `--tags "environment=beta"` entfernen, gilt `MyTopicRuleName` für alle Umgebungen.

Weitere Informationen zum Erstellen von IAM-Rollen und -Richtlinien für eine AWS IoT Regel finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt

Allgemeine Informationen zum Tagging von Ressourcen finden Sie unter Verschlagworten Sie Ihre Ressourcen AWS IoT.

## Eine Regel anzeigen

Verwenden Sie den list-topic-rulesBefehl, um Ihre Regeln aufzulisten:

```
aws iot list-topic-rules
```

Verwenden Sie den get-topic-ruleBefehl, um Informationen zu einer Regel abzurufen:

```
aws iot get-topic-rule --rule-name myrule
```

## Löschen einer Regel

Wenn Sie eine Regel nicht mehr benötigen, können Sie sie löschen.

So löschen Sie eine Regel (AWS CLI)

Verwenden Sie den delete-topic-ruleBefehl, um eine Regel zu löschen:

```
aws iot delete-topic-rule --rule-name myrule
```

# AWS IoT Regelaktionen

AWS IoT Regelaktionen geben an, was zu tun ist, wenn eine Regel aufgerufen wird. Sie können Aktionen definieren, um Daten an eine Amazon DynamoDB DynamoDB-Datenbank zu senden, Daten an Amazon Kinesis Data Streams zu senden, eine AWS Lambda Funktion aufzurufen usw. AWS IoT unterstützt die folgenden Aktionen, AWS-Regionen sofern der Service der Aktion verfügbar ist.

| Regelaktion | Beschreibung | Name in der API |
|---|---|---|
| Apache Kafka | Sendet eine Nachricht an einen Apache-Kafka-Cluster. | `kafka` |
| CloudWatch Alarme | Ändert den Status eines CloudWatch Amazon-Alarms. | `cloudwatchAlarm` |
| CloudWatch Logs | Sendet eine Nachricht an Amazon CloudWatch Logs. | `cloudwatchLogs` |
| CloudWatch Metriken | Sendet eine Nachricht an eine CloudWatch Metrik. | `cloudwatchMetric` |
| DynamoDB | Sendet eine Nachricht an eine DynamoDB-Tabelle. | `dynamoDB` |
| Dynamo DBv2 | Sendet Nachrichtendaten an mehrere Spalten in einer DynamoDB-Tabelle. | `dynamoDBv2` |
| Elasticsearch | Sendet eine Nachricht an einen OpenSearch Endpunkt. | `OpenSearch` |
| HTTP | Sendet eine Nachricht an einen HTTPS-Endpunkt. | `http` |

| Regelaktion | Beschreibung | Name in der API |
| --- | --- | --- |
| IoT Analytics | Sendet eine Nachricht an einen AWS IoT Analytics Kanal. | `iotAnalytics` |
| AWS IoT Events | Sendet eine Nachricht an einen AWS IoT Events Eingang. | `iotEvents` |
| AWS IoT SiteWise | Sendet Nachrichtendaten an AWS IoT SiteWise Objekteig enschaften. | `iotSiteWise` |
| Firehose | Sendet eine Nachricht an einen Firehose-Lieferstream. | `firehose` |
| Kinesis Data Streams | Sendet eine Nachricht an einen Kinesis-Datenstrom. | `kinesis` |
| Lambda | Ruft eine Lambda-Funktion mit Nachrichtendaten als Eingabe auf. | `lambda` |
| Ort | Sendet Standortdaten an Amazon Location Service. | `location` |
| OpenSearch | Sendet eine Nachricht an einen Amazon OpenSearch Service-Endpunkt. | `OpenSearch` |
| Wiederveröffentlichen | Veröffentlicht eine Nachricht erneut in einem anderen MQTT-Thema. | `republish` |
| S3 | Speichert eine Nachricht in einem Amazon Simple Storage Service (Amazon S3)-Bucket. | `s3` |

| Regelaktion | Beschreibung | Name in der API |
| --- | --- | --- |
| Salesforce-IoT | Sendet eine Nachricht an einen Salesforce IoT-Eingabe-Stream. | `salesforce` |
| SNS | Veröffentlichen einer Nachricht als Amazon Simple Notification Service (Amazon SNS) Push-Benachrichtigung. | `sns` |
| SQS | Sendet eine Nachricht an eine Amazon Simple Queue Service (Amazon SQS) Warteschlange. | `sqs` |
| Step Functions | Startet eine AWS Step Functions Zustandsmaschine. | `stepFunctions` |
| the section called “Timestream” | Sendet eine Nachricht an eine Amazon Timestream-Datenbanktabelle. | `timestream` |

Hinweise

- Definieren Sie die Regel genauso AWS-Region wie die Ressource eines anderen Dienstes, sodass die Regelaktion mit dieser Ressource interagieren kann.
- Die AWS IoT Regel-Engine kann mehrere Versuche unternehmen, eine Aktion auszuführen, wenn zeitweise Fehler auftreten. Wenn alle Versuche fehlschlagen, wird die Nachricht verworfen und der Fehler ist in Ihren Protokollen verfügbar. CloudWatch Sie können eine Fehleraktion für jede Regel angeben, die aufgerufen wird, nachdem ein Fehler auftritt. Weitere Informationen finden Sie unter Fehlerbehandlung (Fehleraktion).
- Einige Regelaktionen lösen Aktionen in Services aus, die mit AWS Key Management Service (AWS KMS) integriert werden, um die Verschlüsselung von Daten im Ruhezustand zu unterstützen. Wenn Sie einen vom Kunden verwalteten AWS KMS key (KMS-Schlüssel) verwenden, um Daten im Ruhezustand zu verschlüsseln, muss der Dienst

die Erlaubnis haben, den KMS-Schlüssel im Namen des Anrufers zu verwenden. Wie Sie die Berechtigungen für Ihren vom Kunden verwalteten KMS-Schlüssel verwalten können, erfahren Sie in den Themen zur Datenverschlüsselung im entsprechenden Servicehandbuch. Weitere Informationen über kundenverwaltete KMS-Schlüssel finden Sie unter AWS Key Management Service Konzepte im AWS Key Management Service Entwicklerhandbuch.

## Apache Kafka

Die Apache Kafka (Kafka) -Aktion sendet Nachrichten direkt an Ihr Amazon Managed Streaming for Apache Kafka (Amazon MSK), Apache Kafka-Cluster, die von Drittanbietern wie Confluent Cloud verwaltet werden, oder an selbstverwaltete Apache Kafka-Cluster. Mit Kafka-Regelaktionen können Sie Ihre IoT-Daten an Kafka-Cluster weiterleiten. Auf diese Weise können Sie leistungsstarke Datenpipelines für verschiedene Zwecke einrichten, z. B. für Streaming-Analysen, Datenintegration, Visualisierung und geschäftskritische Geschäftsanwendungen.

> **Note**
>
> Dieses Thema setzt Vertrautheit mit der Apache Kafka-Plattform und verwandten Konzepten voraus. Weitere Informationen zu Apache Kafka finden Sie unter Apache Kafka. MSK Serverless wird nicht unterstützt. Serverlose MSK-Cluster können nur über die IAM-Authentifizierung ausgeführt werden, die die Apache Kafka-Regelaktion derzeit nicht unterstützt. Weitere Informationen zur Konfiguration AWS IoT Core mit Confluent finden Sie unter Leveraging Confluent and Solve IoT Device and Data AWS Management Challenges.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung der,`ec2:CreateNetworkInterface`,,, `ec2:DescribeNetworkInterfaces` `ec2:CreateNetworkInterfacePermissionec2:DeleteNetworkInterface`, `ec2:DescribeSubnets` und -Operationen übernehmen AWS IoT kann. `ec2:DescribeVpcs` `ec2:DescribeVpcAttribute` `ec2:DescribeSecurityGroups` Diese Rolle erstellt und verwaltet ENIs zu Ihrer Amazon Virtual Private Cloud, um Ihren Kafka-Broker zu erreichen. Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT Core zu ermöglichen.

Weitere Informationen zu Netzwerkschnittstellen finden Sie unter Elastic Network Interfaces im EC2 Amazon-Benutzerhandbuch.

Die Richtlinie, die der von Ihnen angegebenen Rolle zugewiesen ist, sollte wie im folgenden Beispiel aussehen.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateNetworkInterface",
            "ec2:DescribeNetworkInterfaces",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:DeleteNetworkInterface",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcs",
            "ec2:DescribeVpcAttribute",
            "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

- Wenn Sie die Anmeldeinformationen speichern AWS Secrets Manager , die für die Verbindung zu Ihrem Kafka-Broker erforderlich sind, müssen Sie eine IAM-Rolle erstellen, die die Ausführung der `secretsmanager:GetSecretValue` AND-Operationen übernehmen AWS IoT Core kann. `secretsmanager:DescribeSecret`

  Die Richtlinie, die der von Ihnen angegebenen Rolle zugewiesen ist, sollte wie im folgenden Beispiel aussehen.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
```

```
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue",
            "secretsmanager:DescribeSecret"
            ],
            "Resource": [

 "arn:aws:secretsmanager:region:123456789012:secret:kafka_client_truststore-*",
                "arn:aws:secretsmanager:region:123456789012:secret:kafka_keytab-*"
            ]
        }
    ]
}
```

- Sie können Ihre Apache Kafka-Cluster in Amazon Virtual Private Cloud (Amazon VPC) ausführen. Sie müssen ein Amazon VPC-Ziel erstellen und ein NAT-Gateway in Ihren Subnetzen verwenden, um Nachrichten von AWS IoT an einen öffentlichen Kafka-Cluster weiterzuleiten. Die AWS IoT Regel-Engine erstellt in jedem der im VPC-Ziel aufgeführten Subnetze eine Netzwerkschnittstelle, um den Verkehr direkt an die VPC weiterzuleiten. Wenn Sie ein VPC-Ziel erstellen, erstellt die AWS IoT Regel-Engine automatisch eine VPC-Regelaktion. Weitere Informationen zu VPC-Regelaktionen finden Sie unter Virtual Private Cloud (VPC) -Ziele.
- Wenn Sie einen vom Kunden verwalteten AWS KMS key (KMS-Schlüssel) verwenden, um Daten im Ruhezustand zu verschlüsseln, muss der Dienst die Erlaubnis haben, den KMS-Schlüssel im Namen des Anrufers zu verwenden. Weitere Informationen finden Sie unter Amazon-MSK-Verschlüsselung im Entwicklerhandbuch für Amazon Managed Streaming for Apache Kafka.

## Parameter

Wenn Sie mit dieser Aktion eine AWS IoT Regel erstellen, müssen Sie die folgenden Informationen angeben:

destinationArn

Der Amazon-Ressourcenname (ARN) des VPC-Ziels. Weitere Informationen zum Erstellen eines VPC-Ziels finden Sie unter Virtual Private Cloud (VPC) -Ziele.

Thema

Das Kafka-Thema für Nachrichten, die an den Kafka-Broker gesendet werden sollen.

Sie können dieses Feld durch eine Ersatzvorlage ersetzen. Weitere Informationen finden Sie unter the section called “Ersetzungsvorlagen”.

Schlüssel (optional)

Der Kafka-Nachrichtenschlüssel.

Sie können dieses Feld durch eine Ersatzvorlage ersetzen. Weitere Informationen finden Sie unter the section called “Ersetzungsvorlagen”.

Überschriften (optional)

Die Liste der Kafka-Header, die Sie festlegen. Jeder Header ist ein Schlüssel-Wert-Paar, das Sie beim Erstellen einer Kafka-Aktion angeben können. Sie können diese Header verwenden, um Daten von IoT-Clients an Downstream-Kafka-Cluster weiterzuleiten, ohne Ihre Nachrichtennutzlast zu ändern.

Sie können dieses Feld durch eine Ersatzvorlage ersetzen. Um zu verstehen, wie die Funktion einer Inline-Regel als Ersatzvorlage in den Header von Kafka Action übergeben wird, siehe Beispiele. Weitere Informationen finden Sie unter the section called “Ersetzungsvorlagen”.

> **Note**
>
> Header im Binärformat werden nicht unterstützt.

Partition (optional)

Die Kafka-Nachrichten-Partition.

Sie können dieses Feld durch eine Ersatzvorlage ersetzen. Weitere Informationen finden Sie unter the section called “Ersetzungsvorlagen”.

clientProperties

Ein Objekt, das die Eigenschaften des Apache Kafka-Producer-Clients definiert.

acks (optional)

Die Anzahl der Bestätigungen, die der Hersteller beim Server erhalten haben muss, bevor eine Anfrage als abgeschlossen betrachtet werden kann.

Wenn Sie 0 als Wert angeben, wartet der Producer nicht auf eine Bestätigung vom Server. Wenn der Server die Nachricht nicht empfängt, versucht der Producer nicht erneut, die Nachricht zu senden.

Zulässige Werte: `-1`, `0`, `1`, `all`. Der Standardwert ist `1`.

bootstrap.servers

Eine Liste von Host- und Port-Paaren (z. B.`host1:port1`, `host2:port2`), die verwendet wurden, um die erste Verbindung zu Ihrem Kafka-Cluster herzustellen.

compression.type (optional)

Der Komprimierungstyp für alle vom Hersteller generierten Daten.

Zulässige Werte: `none`, `gzip`, `snappy`, `lz4`, `zstd`. Der Standardwert ist `none`.

security.protocol

Das Sicherheitsprotokoll, das für die Verbindung mit Ihrem Kafka-Broker verwendet wird.

Zulässige Werte: `SSL`, `SASL_SSL`. Der Standardwert ist `SSL`.

key.serializer

Gibt an, wie die Schlüsselobjekte, die Sie mit `ProducerRecord` bereitstellen, in Bytes umgewandelt werden sollen.

Zulässiger Wert: `StringSerializer`.

value.serializer

Gibt an, wie Wertobjekte, die Sie mit dem `ProducerRecord` bereitstellen, in Bytes umgewandelt werden sollen.

Zulässiger Wert: `ByteBufferSerializer`.

ssl.truststore

Die Truststore-Datei im Base64-Format oder der Speicherort der Truststore-Datei in AWS Secrets Manager. Dieser Wert ist nicht erforderlich, wenn Ihr Truststore von den Amazon-Zertifizierungsstellen (CA) als vertrauenswürdig eingestuft wird.

Dieses Feld unterstützt Substitutionsvorlagen. Wenn Sie Secrets Manager verwenden, um die Anmeldeinformationen zu speichern, die für die Verbindung mit Ihrem Kafka-Broker erforderlich sind, können Sie die `get_secret` SQL-Funktion verwenden, um den Wert für

dieses Feld abzurufen. Weitere Informationen zu Ersatzvorlagen finden Sie unter the section called “Ersetzungsvorlagen”. Weitere Informationen zur `get_secret` SQL Funktion finden Sie unter the section called “get_secret (secretId, geheimer Typ, Schlüssel, roleArn)”. Wenn der Truststore in Form einer Datei vorliegt, verwenden Sie den `SecretBinary` Parameter. Wenn der Truststore die Form einer Zeichenfolge hat, verwenden Sie den `SecretString` Parameter.

Die maximale Größe dieses Wertes beträgt 65 KB.

ssl.truststore.password

Das Passwort für den Truststore Dieser Wert ist nur erforderlich, wenn Sie ein Passwort für den Truststore erstellt haben.

ssl.keystore

Die Keystore-Datei. Dieser Wert ist erforderlich, wenn Sie `SSL` als Wert für `security.protocol` angeben.

Dieses Feld unterstützt Substitutionsvorlagen. Verwenden Sie Secrets Manager, um die Anmeldeinformationen zu speichern, die für die Verbindung mit Ihrem Kafka-Broker erforderlich sind. Verwenden Sie die `get_secret` SQL-Funktion, um den Wert für dieses Feld abzurufen. Weitere Informationen zu Ersatzvorlagen finden Sie unter the section called “Ersetzungsvorlagen”. Weitere Informationen zur `get_secret` SQL Funktion finden Sie unter the section called “get_secret (secretId, geheimer Typ, Schlüssel, roleArn)”. Verwenden Sie den Parameter `SecretBinary`.

ssl.keystore.password

Das Speicherpasswort für die Keystore-Datei. Dieser Wert ist erforderlich, wenn Sie einen Wert für `ssl.keystore` angeben.

Der Wert dieses Feldes kann Klartext sein. Dieses Feld unterstützt auch Ersatzvorlagen. Verwenden Sie Secrets Manager, um die Anmeldeinformationen zu speichern, die für die Verbindung mit Ihrem Kafka-Broker erforderlich sind. Verwenden Sie die `get_secret` SQL-Funktion, um den Wert für dieses Feld abzurufen. Weitere Informationen zu Ersatzvorlagen finden Sie unter the section called “Ersetzungsvorlagen”. Weitere Informationen zur `get_secret` SQL Funktion finden Sie unter the section called “get_secret (secretId, geheimer Typ, Schlüssel, roleArn)”. Verwenden Sie den Parameter `SecretString`.

ssl.key.password

Das Passwort des privaten Schlüssels in Ihrer Keystore-Datei.

Dieses Feld unterstützt Substitutionsvorlagen. Verwenden Sie Secrets Manager, um die Anmeldeinformationen zu speichern, die für die Verbindung mit Ihrem Kafka-Broker erforderlich sind. Verwenden Sie die `get_secret` SQL-Funktion, um den Wert für dieses Feld abzurufen. Weitere Informationen zu Ersatzvorlagen finden Sie unter the section called “Ersetzungsvorlagen”. Weitere Informationen zur `get_secret` SQL Funktion finden Sie unter the section called “get_secret (secretId, geheimer Typ, Schlüssel, roleArn)”. Verwenden Sie den Parameter `SecretString`.

sasl.mechanik

Der Sicherheitsmechanismus, der für die Verbindung zu Ihrem Kafka-Broker verwendet wird. Dieser Wert ist erforderlich, wenn Sie `SASL_SSL` für `security.protocol` angeben.

Zulässige Werte: `PLAIN`, `SCRAM-SHA-512`, `GSSAPI`.

> **Note**
>
> `SCRAM-SHA-512`ist der einzige unterstützte Sicherheitsmechanismus in den Regionen cn-north-1, cn-northwest-1, -1 und -1. us-gov-east us-gov-west

sasl.plain.username

Der Benutzername, der verwendet wird, um die geheime Zeichenfolge vom Secrets Manager abzurufen. Dieser Wert ist erforderlich, wenn Sie `SASL_SSL` für `security.protocol` und `PLAIN` für `sasl.mechanism` angeben.

sasl.plain.password

Das Passwort, das zum Abrufen der geheimen Zeichenfolge von Secrets Manager verwendet wird. Dieser Wert ist erforderlich, wenn Sie `SASL_SSL` für `security.protocol` und `PLAIN` für `sasl.mechanism` angeben.

sasl.scram.username

Der Benutzername, der verwendet wird, um die geheime Zeichenfolge vom Secrets Manager abzurufen. Dieser Wert ist erforderlich, wenn Sie `SASL_SSL` für `security.protocol` und `SCRAM-SHA-512` für `sasl.mechanism` angeben.

sasl.scram.password

Das Passwort, das zum Abrufen der geheimen Zeichenfolge von Secrets Manager verwendet wird. Dieser Wert ist erforderlich, wenn Sie `SASL_SSL` für `security.protocol` und `SCRAM-SHA-512` für `sasl.mechanism` angeben.

sasl.kerberos.keytab

Die Keytab-Datei für die Kerberos-Authentifizierung in Secrets Manager. Dieser Wert ist erforderlich, wenn Sie `SASL_SSL` für `security.protocol` und `GSSAPI` für `sasl.mechanism` angeben.

Dieses Feld unterstützt Substitutionsvorlagen. Verwenden Sie Secrets Manager, um die Anmeldeinformationen zu speichern, die für die Verbindung mit Ihrem Kafka-Broker erforderlich sind. Verwenden Sie die `get_secret` SQL-Funktion, um den Wert für dieses Feld abzurufen. Weitere Informationen zu Ersatzvorlagen finden Sie unter the section called “Ersetzungsvorlagen”. Weitere Informationen zur `get_secret` SQL Funktion finden Sie unter the section called “get_secret (secretId, geheimer Typ, Schlüssel, roleArn)”. Verwenden Sie den Parameter `SecretBinary`.

sasl.kerberos.service.name

Der Kerberos-Prinzipalname, unter dem Apache Kafka ausgeführt wird. Dieser Wert ist erforderlich, wenn Sie `SASL_SSL` für `security.protocol` und `GSSAPI` für `sasl.mechanism` angeben.

sasl.kerberos.krb5.kdc

Der Hostname des Key Distribution Center (KDC), mit dem Ihr Apache Kafka Producer-Client eine Verbindung herstellt. Dieser Wert ist erforderlich, wenn Sie `SASL_SSL` für `security.protocol` und `GSSAPI` für `sasl.mechanism` angeben.

sasl.kerberos.krb5.realm

Der Realm, mit dem Ihr Apache Kafka Producer-Client eine Verbindung herstellt. Dieser Wert ist erforderlich, wenn Sie `SASL_SSL` für `security.protocol` und `GSSAPI` für `sasl.mechanism` angeben.

sasl.kerberos.principal

Die eindeutige Kerberos-Identität, der Kerberos Tickets für den Zugriff auf Kerberos-fähige Dienste zuweisen kann. Dieser Wert ist erforderlich, wenn Sie `SASL_SSL` für `security.protocol` und `GSSAPI` für `sasl.mechanism` angeben.

## Beispiele

Das folgende JSON-Beispiel definiert eine Apache Kafka-Aktion in einer Regel. AWS IoT Im folgenden Beispiel wird die Inline-Funktion sourceIp () als Ersatzvorlage im Kafka Action-Header übergeben.

```
{
 "topicRulePayload": {
  "sql": "SELECT * FROM 'some/topic'",
  "ruleDisabled": false,
  "awsIotSqlVersion": "2016-03-23",
  "actions": [
   {
    "kafka": {
     "destinationArn": "arn:aws:iot:region:123456789012:ruledestination/vpc/
VPCDestinationARN",
     "topic": "TopicName",
     "clientProperties": {
      "bootstrap.servers": "kafka.com:9092",
      "security.protocol": "SASL_SSL",
      "ssl.truststore": "${get_secret('kafka_client_truststore',
 'SecretBinary','arn:aws:iam::123456789012:role/kafka-get-secret-role-name')}",
      "ssl.truststore.password": "kafka password",
      "sasl.mechanism": "GSSAPI",
      "sasl.kerberos.service.name": "kafka",
      "sasl.kerberos.krb5.kdc": "kerberosdns.com",
      "sasl.kerberos.keytab": "${get_secret('kafka_keytab','SecretBinary',
 'arn:aws:iam::123456789012:role/kafka-get-secret-role-name')}",
      "sasl.kerberos.krb5.realm": "KERBEROSREALM",
      "sasl.kerberos.principal": "kafka-keytab/kafka-keytab.com"
     },
     "headers": [
      {
       "key": "static_header_key",
       "value": "static_header_value"
      },
      {
       "key": "substitutable_header_key",
       "value": "${value_from_payload}"
      },
      {
       "key": "source_ip",
       "value": "${sourceIp()}"
```

```
      }
     ]
    }
   }
  ]
 }
}
```

Wichtige Hinweise zu Ihrem Kerberos-Setup

- Ihr Key Distribution Center (KDC) muss über ein privates Domain Name System (DNS) innerhalb Ihrer Ziel-VPC auflösbar sein. Ein möglicher Ansatz besteht darin, den KDC-DNS-Eintrag zu einer privaten gehosteten Zone hinzuzufügen. Weitere Informationen zu diesem Ansatz finden Sie unter Arbeiten mit privat gehosteten Zonen.
- Für jede VPC muss die DNS-Auflösung aktiviert sein. Weitere Informationen finden Sie unter Verwenden von DNS in Ihrer VPC.
- Sicherheitsgruppen für Netzwerkschnittstellen und Sicherheitsgruppen auf Instance-Ebene im VPC-Ziel müssen Datenverkehr aus Ihrer VPC an den folgenden Ports zulassen.
  - TCP-Verkehr auf dem Bootstrap-Broker-Listener-Port (häufig 9092, muss aber im Bereich 9000—9100 liegen)
  - TCP- und UDP-Verkehr auf Port 88 für das KDC
- `SCRAM-SHA-512`ist der einzige unterstützte Sicherheitsmechanismus in den Regionen cn-north-1, cn-northwest-1, -1 und -1. us-gov-east us-gov-west

## Virtual Private Cloud (VPC) -Ziele

Die Apache Kafka-Regelaktion leitet Daten an einen Apache Kafka-Cluster in einer Amazon Virtual Private Cloud (Amazon VPC). Die von der Apache Kafka-Regelaktion verwendete VPC-Konfiguration wird automatisch aktiviert, wenn Sie das VPC-Ziel für Ihre Regelaktion angeben.

Ein VPC-Ziel enthält eine Liste von Subnetzen innerhalb der VPC. Die Regel-Engine erstellt eine ENI in jedem Subnetz, das Sie in dieser Liste angeben. Weitere Informationen zu Netzwerkschnittstellen finden Sie unter Elastic Network Interfaces im EC2 Amazon-Benutzerhandbuch.

Anforderungen und Überlegungen

- Wenn Sie einen selbstverwalteten Apache Kafka-Cluster verwenden, auf den über einen öffentlichen Endpunkt im Internet zugegriffen wird:

- Erstellen Sie ein NAT-Gateway für Instances in Ihren Subnetzen. Das NAT-Gateway verfügt über eine öffentliche IP-Adresse, die eine Verbindung zum Internet herstellen kann. Dadurch kann die Regel-Engine Ihre Nachrichten an den öffentlichen Kafka-Cluster weiterleiten.
- Ordnen Sie den Elastic Network Interfaces (ENIs), die von der VPC-Destination erstellt werden, eine Elastic IP-Adresse zu. Die Sicherheitsgruppen, die Sie verwenden, müssen so konfiguriert sein, dass sie eingehenden Datenverkehr blockieren.

  > **Note**
  >
  > Wenn das VPC-Ziel deaktiviert und dann wieder aktiviert wird, müssen Sie das Elastic erneut IPs mit dem neuen verknüpfen. ENIs

- Wenn ein Ziel für eine VPC-Themenregel 30 Tage hintereinander keinen Traffic empfängt, wird es deaktiviert.
- Wenn sich die vom VPC-Ziel verwendeten Ressourcen ändern, wird das Ziel deaktiviert und kann nicht verwendet werden.
- Zu den Änderungen, die ein VPC-Ziel deaktivieren können, gehören: Löschen der VPC, Subnetze, Sicherheitsgruppen oder der verwendeten Rolle, Ändern der Rolle, sodass sie nicht mehr über die erforderlichen Berechtigungen verfügt, und Deaktivieren des Ziels.

Preisgestaltung

Aus Preisgründen wird eine VPC-Regelaktion zusätzlich zu der Aktion gemessen, die eine Nachricht an eine Ressource sendet, wenn sich die Ressource in Ihrer VPC befindet. Preisinformationen finden Sie unter AWS IoT Core Preise.

Erstellen von Virtual Private Cloud (VPC) -Themenregelzielen

Sie erstellen ein VPC-Ziel (Virtual Private Cloud) mithilfe der CreateTopicRuleDestinationAPI oder der AWS IoT Core Konsole.

Wenn Sie ein VPC-Ziel erstellen, müssen Sie die folgenden Informationen angeben.

vpcId

Die eindeutige ID des VPC-Ziels.

subnetIds

Eine Liste von Subnetzen, in denen die Regel-Engine ENIs erstellt. Die Regel-Engine weist jedem Subnetz in der Liste eine einzelne Netzwerkschnittstelle zu.

securityGroups (optional)

Eine Liste von Sicherheitsgruppen, die auf die Netzwerkschnittstellen anzuwenden sind

roleArn

Der Amazon-Ressourcenname (ARN) einer Rolle, die die Berechtigung zum Erstellen von Netzwerkschnittstellen in Ihrem Namen erteilt.

Diesem ARN sollte eine Richtlinie angehängt sein, die wie im folgenden Beispiel aussieht.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcs",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateNetworkInterfacePermission",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/VPCDestinationENI": "true"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface",
                    "aws:RequestTag/VPCDestinationENI": "true"
                }
            }
        }
    ]
}
```

Erstellen eines VPC-Ziels mithilfe von AWS CLI

Das folgende Beispiel zeigt, wie Sie ein VPC-Ziel mithilfe von AWS CLI erstellen.

```
aws --region regions iot create-topic-rule-destination --destination-configuration
 'vpcConfiguration={subnetIds=["subnet-
123456789101230456"],securityGroups=[],vpcId="vpc-
123456789101230456",roleArn="arn:aws:iam::123456789012:role/role-name"}'
```

Nachdem Sie diesen Befehl ausgeführt haben, lautet der VPC-Zielstatus `IN_PROGRESS`. Nach einigen Minuten ändert sich der Status entweder auf `ERROR` (falls der Befehl nicht erfolgreich ist) oder `ENABLED`. Wenn der Zielstatus `ENABLED` lautet, ist er einsatzbereit.

Sie können den folgenden Befehl verwenden, um den Status Ihres VPC-Ziels abzurufen.

```
aws --region region iot get-topic-rule-destination --arn "VPCDestinationARN"
```

Erstellen eines VPC-Ziels mithilfe der Konsole AWS IoT Core

In den folgenden Schritten wird beschrieben, wie Sie mithilfe der AWS IoT Core Konsole ein VPC-Ziel erstellen.

1. Navigieren Sie zur AWS IoT Core Konsole. Wählen Sie im linken Bereich auf der Registerkarte Aktion die Option Ziele aus.
2. Geben Sie Werte für folgende Felder ein.
   - VPC-ID
   - Subnetz IDs
   - Sicherheitsgruppe
3. Wählen Sie eine Rolle aus, die über die erforderlichen Berechtigungen zum Erstellen von Netzwerkschnittstellen verfügt. Die obige Beispielrichtlinie enthält diese Berechtigungen.

Wenn der VPC-Zielstatus ENABLED (AKTIVIERT) lautet, ist es einsatzbereit.

## CloudWatch Alarme

Die Aktion CloudWatch alarm (`cloudWatchAlarm`) ändert den Status eines CloudWatch Amazon-Alarms. Sie können den Grund für die Zustandsänderung und den Wert in diesem Aufruf angeben.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des `cloudwatch:SetAlarmState` Vorgangs übernehmen AWS IoT kann. Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.

### Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`alarmName`

Der Name des CloudWatch Alarms.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`stateReason`

Der Grund für die Alarmänderung

Unterstützt Ersatzvorlagen: Ja

`stateValue`

Der Wert des Alarmzustands. Zulässige Werte: `OK`, `ALARM`, `INSUFFICIENT_DATA`.

Unterstützt Ersatzvorlagen: Ja

`roleArn`

Die IAM-Rolle, die den Zugriff auf den CloudWatch Alarm ermöglicht. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine CloudWatch Alarmaktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "cloudwatchAlarm": {
                    "alarmName": "IotAlarm",
                    "stateReason": "Temperature stabilized.",
                    "stateValue": "OK",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_cw"
                }
            }
        ]
    }
}
```

## Weitere Informationen finden Sie auch unter

- Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch

- Verwenden von CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch

## CloudWatch Logs

Die Aktion CloudWatch Logs (`cloudwatchLogs`) sendet Daten an Amazon CloudWatch Logs. Sie können `batchMode` verwenden, um mehrere Geräteprotokolldatensätze in einer Nachricht hochzuladen und mit einem Zeitstempel zu versehen. Sie können auch die Protokollgruppe angeben, an die die Aktion Daten sendet.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung der `logs:PutLogEvents` Operationen `logs:CreateLogStreamlogs:DescribeLogStreams`, und übernehmen AWS IoT kann. Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.
- Wenn Sie einen vom Kunden verwalteten AWS KMS key KMS-Schlüssel verwenden, um Protokolldaten in CloudWatch Logs zu verschlüsseln, muss der Dienst die Erlaubnis haben, den KMS-Schlüssel im Namen des Anrufers zu verwenden. Weitere Informationen finden Sie unter Verschlüsseln von Protokolldaten in CloudWatch Logs using AWS KMS im Amazon CloudWatch Logs-Benutzerhandbuch.

### Anforderungen an das MQTT-Nachrichtenformat für **`batchMode`**

Wenn Sie die Regelaktion „ CloudWatch Logs“ bei `batchMode` ausgeschalteter Option verwenden, gibt es keine Anforderungen an die Formatierung von MQTT-Nachrichten. (Hinweis: Der Standardwert des `batchMode` Parameters ist `false`.) Wenn Sie jedoch die Regelaktion CloudWatch Logs mit `batchMode` aktivierter Option verwenden (der Parameterwert ist`true`), müssen MQTT-Nachrichten, die geräteseitige Logs enthalten, so formatiert werden, dass sie einen Zeitstempel und eine Nachrichten-Payload enthalten. Hinweis: `timestamp` stellt den Zeitpunkt dar, zu dem das Ereignis eingetreten ist, und wird als Anzahl der Millisekunden nach dem 1. Januar 1970 00:00:00 UTC ausgedrückt.

Nachfolgend sehen Sie ein Beispiel des Veröffentlichungsformats:

```
[
  {"timestamp": 1673520691093, "message": "Test message 1"},
  {"timestamp": 1673520692879, "message": "Test message 2"},
  {"timestamp": 1673520693442, "message": "Test message 3"}
]
```

Je nachdem, wie die geräteseitigen Protokolle generiert werden, müssen sie möglicherweise gefiltert und neu formatiert werden, bevor sie gesendet werden, um diese Anforderung zu erfüllen. Weitere Informationen finden Sie unter MQTT-Nachrichtennutzlast.

Unabhängig vom `batchMode` Parameter muss der `message` Inhalt den Größenbeschränkungen für Nachrichten entsprechen. AWS IoT Weitere Informationen finden Sie unter AWS IoT Core Endpunkte und -Kontingente.

## Parameter

Wenn Sie mit dieser Aktion eine AWS IoT Regel erstellen, müssen Sie die folgenden Informationen angeben:

`logGroupName`

Die CloudWatch Protokollgruppe, in die die Aktion Daten sendet.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`roleArn`

Die IAM-Rolle, die den Zugriff auf die CloudWatch Protokollgruppe ermöglicht. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

(Optional) `batchMode`

Gibt an, ob Stapel von Protokolldatensätzen extrahiert und in diese hochgeladen werden. CloudWatch Zu den Werten gehört `true` oder `false` (Standard). Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine CloudWatch Logs-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "cloudwatchLogs": {
                    "logGroupName": "IotLogs",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_cw",
                    "batchMode": false
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist Amazon CloudWatch Logs? im Amazon CloudWatch Logs-Benutzerhandbuch

## CloudWatch Metriken

Die Aktion CloudWatch metric (`cloudwatchMetric`) erfasst eine CloudWatch Amazon-Metrik. Sie können den Namespace, den Namen, den Wert, die Einheit und den Zeitstempel der Metrik angeben.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des `cloudwatch:PutMetricData` Vorgangs übernehmen AWS IoT kann. Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.

## Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`metricName`

Der Name der CloudWatch Metrik.

Unterstützt Ersatzvorlagen: Ja

`metricNamespace`

Der Name des CloudWatch Metrik-Namespaces.

Unterstützt Ersatzvorlagen: Ja

`metricUnit`

Die metrische Einheit, die von CloudWatch unterstützt wird.

Unterstützt Ersatzvorlagen: Ja

`metricValue`

Eine Zeichenfolge, die den CloudWatch metrischen Wert enthält.

Unterstützt Ersatzvorlagen: Ja

`metricTimestamp`

(Optional) Eine Zeichenfolge mit dem Zeitstempel, ausgedrückt in Sekunden der Unix-Epochenzeit. Standardmäßig wird die aktuelle Unix-Epochenzeit verwendet.

Unterstützt Ersatzvorlagen: Ja

`roleArn`

Die IAM-Rolle, die den Zugriff auf die CloudWatch Metrik ermöglicht. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine CloudWatch Metrikaktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "cloudwatchMetric": {
                    "metricName": "IotMetric",
                    "metricNamespace": "IotNamespace",
                    "metricUnit": "Count",
                    "metricValue": "1",
                    "metricTimestamp": "1456821314",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_cw"
                }
            }
        ]
    }
}
```

Das folgende JSON-Beispiel definiert eine CloudWatch metrische Aktion mit Ersatzvorlagen in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "cloudwatchMetric": {
                    "metricName": "${topic()}",
                    "metricNamespace": "${namespace}",
                    "metricUnit": "${unit}",
                    "metricValue": "${value}",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_cw"
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch
- Verwendung von CloudWatch Amazon-Metriken im CloudWatch Amazon-Benutzerhandbuch

## DynamoDB

Die Aktion DynamoDB (`dynamoDB`) schreibt eine MQTT-Nachricht ganz oder teilweise in eine Amazon DynamoDB-Tabelle.

Sie können einem Tutorial folgen, das Ihnen veranschaulicht, wie Sie eine Regel mit einer DynamoDB-Aktion erstellen und testen. Weitere Informationen finden Sie unter Tutorial: Gerätedaten in einer DynamoDB-Tabelle speichern.

> **Note**
>
> Diese Regel schreibt Nicht-JSON-Daten als Binärdaten in DynamoDB. Die DynamoDB-Konsole zeigt die Daten als Base64-codierten Text an.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des Vorgangs übernehmen AWS IoT kann. `dynamodb:PutItem` Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.
- Wenn Sie einen vom Kunden verwalteten AWS KMS key (KMS-Schlüssel) verwenden, um ruhende Daten in DynamoDB zu verschlüsseln, muss der Dienst über die Berechtigung verfügen, den KMS-Schlüssel im Namen des Anrufers zu verwenden. Weitere Informationen finden Sie unter Kundenverwalteter KMS-Schlüssel im Amazon DynamoDB Einführungshandbuch..

## Parameter

Wenn Sie mit dieser Aktion eine AWS IoT Regel erstellen, müssen Sie die folgenden Informationen angeben:

`tableName`

Der Name der DynamoDB-Tabelle.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`hashKeyField`

Der Name des Hash-Schlüssels (auch Partitionsschlüssel genannt)

Unterstützt Substitutionsvorlagen: API und nur AWS CLI

`hashKeyType`

(Optional) Der Datentyp des Hash-Schlüssels (auch Partitionsschlüssel genannt). Zulässige Werte: `STRING`, `NUMBER`.

Unterstützt Substitutionsvorlagen: API und nur AWS CLI

`hashKeyValue`

Der Wert des Hash-Schlüssels Erwägen Sie die Verwendung einer Ersatzvorlage wie `${topic()}` oder `${timestamp()}`.

Unterstützt Ersatzvorlagen: Ja

`rangeKeyField`

(Optional) Der Name des Bereichsschlüssels (auch Sortierschlüssel genannt).

Unterstützt Substitutionsvorlagen: API und nur AWS CLI

`rangeKeyType`

(Optional) Der Datentyp des Bereichsschlüssels (auch Sortierschlüssel genannt). Zulässige Werte: `STRING`, `NUMBER`.

Unterstützt Substitutionsvorlagen: API und nur AWS CLI

`rangeKeyValue`

(Optional) Der Wert des Bereichsschlüssels. Erwägen Sie die Verwendung einer Ersatzvorlage wie `${topic()}` oder `${timestamp()}`.

Unterstützt Ersatzvorlagen: Ja

`payloadField`

(Optional) Der Name der Spalte, in die die Nutzlast geschrieben wird. Wenn Sie diesen Wert weglassen, wird die Nutzlast in die Spalte mit dem Namen `payload` geschrieben.

Unterstützt Ersatzvorlagen: Ja

`operation`

(Optional) Der Typ des auszuführenden Vorgangs. Zulässige Werte: `INSERT`, `UPDATE`, `DELETE`.

Unterstützt Ersatzvorlagen: Ja

`roleARN`

Die IAM-Rolle, die den Zugriff auf die DynamoDB-Tabelle erlaubt. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

Die in die DynamoDB-Tabelle geschriebenen Daten sind das Ergebnis der SQL-Anweisung der Regel.

## Beispiele

Das folgende JSON-Beispiel definiert eine DynamoDB-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * AS message FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "dynamoDB": {
                    "tableName": "my_ddb_table",
                    "hashKeyField": "key",
                    "hashKeyValue": "${topic()}",
```

```
                    "rangeKeyField": "timestamp",
                    "rangeKeyValue": "${timestamp()}",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_dynamoDB"
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist Amazon DynamoDB? im Amazon DynamoDB Entwicklerhandbuch
- Erste Schritte mit DynamoDB im Amazon DynamoDB Entwicklerhandbuch
- Tutorial: Gerätedaten in einer DynamoDB-Tabelle speichern

## Dynamo DBv2

Die Dynamo DBv2 (`dynamoDBv2`) -Aktion schreibt eine MQTT-Nachricht ganz oder teilweise in eine Amazon DynamoDB-Tabelle. Jedes Attribut in der Nutzlast wird in eine separate Spalte in der DynamoDB-Datenbank geschrieben.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des Vorgangs übernehmen AWS IoT kann. `dynamodb:PutItem` Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.
- Die MQTT-Nachrichtnutzlast muss einen Schlüssel auf Stammebene enthalten, der mit dem primären Partitionsschlüssel der Tabelle übereinstimmt, sowie über einen Schlüssel auf Stammebene, der mit dem primären Sortierschlüssel der Tabelle (sofern definiert) übereinstimmt.
- Wenn Sie einen vom Kunden verwalteten AWS KMS key (KMS-Schlüssel) verwenden, um ruhende Daten in DynamoDB zu verschlüsseln, muss der Dienst über die Berechtigung verfügen, den KMS-Schlüssel im Namen des Anrufers zu verwenden. Weitere Informationen finden Sie unter Kundenverwalteter KMS-Schlüssel im Amazon DynamoDB Einführungshandbuch..

## Parameter

Wenn Sie mit dieser Aktion eine AWS IoT Regel erstellen, müssen Sie die folgenden Informationen angeben:

`putItem`

Ein Objekt, das die DynamoDB-Tabelle angibt, in die die Nachrichtendaten geschrieben werden sollen. Dieses Objekt muss die folgenden Informationen enthalten:

`tableName`

Der Name der DynamoDB-Tabelle.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`roleARN`

Die IAM-Rolle, die den Zugriff auf die DynamoDB-Tabelle erlaubt. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

Die in die DynamoDB-Tabelle geschriebenen Daten sind das Ergebnis der SQL-Anweisung der Regel.

## Beispiele

Das folgende JSON-Beispiel definiert eine DBv2 Dynamo-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * AS message FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "dynamoDBv2": {
                    "putItem": {
                        "tableName": "my_ddb_table"
                    },
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_dynamoDBv2",
                }
            }
```

```
        ]
    }
}
```

Das folgende JSON-Beispiel definiert eine DynamoDB-Aktion mit Ersatzvorlagen in einer Regel. AWS IoT

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2015-10-08",
        "actions": [
            {
                "dynamoDBv2": {
                    "putItem": {
                        "tableName": "${topic()}"
                    },
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_dynamoDBv2"
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist Amazon DynamoDB? im Amazon DynamoDB Entwicklerhandbuch
- Erste Schritte mit DynamoDB im Amazon DynamoDB Entwicklerhandbuch

## Elasticsearch

Die Elasticsearch (`elasticsearch`) -Aktion schreibt Daten aus MQTT-Nachrichten in eine Amazon OpenSearch Service-Domain. Sie können dann Tools wie OpenSearch Dashboards verwenden, um Daten in Service abzufragen und zu visualisieren. OpenSearch

> **Warning**
>
> Die `Elasticsearch` Aktion kann nur von vorhandenen Regelaktion verwendet werden. Um eine neue Regelaktion zu erstellen oder eine vorhandene Regelaktion zu aktualisieren,

verwenden Sie stattdessen die `OpenSearch` Regelaktion. Weitere Informationen finden Sie unter OpenSearch.

## Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des `es:ESHttpPut` Vorgangs übernehmen AWS IoT kann. Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.
- Wenn Sie einen vom Kunden verwalteten AWS KMS key (KMS-Schlüssel) verwenden, um gespeicherte Daten zu verschlüsseln OpenSearch, muss der Dienst die Erlaubnis haben, den KMS-Schlüssel im Namen des Anrufers zu verwenden. Weitere Informationen finden Sie unter Verschlüsselung ruhender Daten für Amazon OpenSearch Service im Amazon OpenSearch Service Developer Guide.

## Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`endpoint`

Der Endpunkt Ihrer Service-Domain

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`index`

Der Index, in dem Sie die Daten speichern möchten

Unterstützt Ersatzvorlagen: Ja

`type`

Der Typ des Dokuments, das Sie speichern

Unterstützt Ersatzvorlagen: Ja

`id`

Der eindeutige Bezeichner für jedes Dokument

Unterstützt Ersatzvorlagen: Ja

`roleARN`

Die IAM-Rolle, die den Zugriff auf die OpenSearch Service-Domain ermöglicht. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine Elasticsearch-Aktion in einer AWS IoT Regel und zeigt, wie Sie die Felder für die `elasticsearch` Aktion angeben können. Weitere Informationen finden Sie unter ElasticsearchAction.

```
{
    "topicRulePayload": {
        "sql": "SELECT *, timestamp() as timestamp FROM 'iot/test'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "elasticsearch": {
                    "endpoint": "https://my-endpoint",
                    "index": "my-index",
                    "type": "my-type",
                    "id": "${newuuid()}",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_es"
                }
            }
        ]
    }
}
```

Das folgende JSON-Beispiel definiert eine Elasticsearch-Aktion mit Ersatzvorlagen in einer Regel. AWS IoT

```
{
```

```
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "elasticsearch": {
                    "endpoint": "https://my-endpoint",
                    "index": "${topic()}",
                    "type": "${type}",
                    "id": "${newuuid()}",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_es"
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- OpenSearch
- Was ist Amazon OpenSearch Service?

## HTTP

Die Aktion HTTPS (`http`) sendet Daten von einer MQTT-Nachricht an eine Webanwendung oder einen Webdienst.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Sie müssen die HTTPS-Endpunkte bestätigen und aktivieren, bevor sie von der Regel-Engine verwendet werden können. Weitere Informationen finden Sie unter Arbeiten mit HTTP-Themenregelzielen.

### Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`url`

Der HTTPS-Endpunkt, an den die Nachricht mithilfe der HTTP-POST-Methode gesendet wird. Wenn Sie eine IP-Adresse anstelle eines Hostnamens verwenden, muss es sich um eine IPv4 Adresse handeln. IPv6 Adressen werden nicht unterstützt.

Unterstützt Ersatzvorlagen: Ja

`confirmationUrl`

(Optional) Falls angegeben, AWS IoT verwendet die Bestätigungs-URL, um ein passendes Ziel für die Themenregel zu erstellen. Sie müssen das Themenregelziel aktivieren, bevor Sie es in einer HTTP-Aktion verwenden. Weitere Informationen finden Sie unter Arbeiten mit HTTP-Themenregelzielen. Wenn Sie Ersetzungsvorlagen verwenden, müssen Sie Themenregelziele manuell erstellen, bevor die `http` Aktion verwendet werden kann. `confirmationUrl` muss ein Präfix von `url` sein.

Das Verhältnis zwischen `url` und `confirmationUrl` wird wie folgt beschrieben:

- Wenn `url` es fest codiert und nicht angegeben `confirmationUrl` ist, behandeln wir das `url` Feld implizit als. `confirmationUrl` AWS IoT erstellt ein Ziel für eine Themenregel. `url`
- Falls `url` und fest codiert `confirmationUrl` sind, `url` muss mit `confirmationUrl` beginnen. AWS IoT erstellt ein Ziel für `confirmationUrl` eine Themenregel.
- Wenn `url` eine Ersetzungsvorlage enthält, müssen Sie `confirmationUrl` angeben und `url` muss mit `confirmationUrl` beginnen. Wenn `confirmationUrl` Ersetzungsvorlagen enthält, müssen Sie Themenregelziele manuell erstellen, bevor die `http` Aktion verwendet werden kann. Wenn `confirmationUrl` es keine Ersatzvorlagen enthält, AWS IoT erstellt es ein Ziel für Themenregeln für`confirmationUrl`.

Unterstützt Ersatzvorlagen: Ja

`headers`

(Optional) Die Liste der Header, die in HTTP-Anfragen an den Endpunkt aufgenommen werden sollen. Jeder Header muss die folgenden Informationen enthalten:

`key`

Der Schlüssel des Headers.

Unterstützt Ersatzvorlagen: Nein

`value`

Der Wert des Headers

Unterstützt Ersatzvorlagen: Ja

> **Note**
>
> Der Standard-Inhaltstyp ist application/json when the payload is in JSON format. Otherwise, it is application/octet -stream. Sie können ihn überschreiben, indem Sie im Header den genauen Inhaltstyp mit dem Schlüsselinhaltstyp angeben (ohne Berücksichtigung von Groß- und Kleinschreibung).

`auth`

(Optional) Die vom Regelmodul verwendete Authentifizierung, um eine Verbindung mit der im `url` Argument angegebenen Endpunkt-URL herzustellen. Derzeit ist Signature Version 4 der einzige unterstützte Authentifizierungstyp. Weitere Informationen finden Sie unter HTTP-Autorisierung.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine AWS IoT Regel mit einer HTTP-Aktion.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "http": {
                    "url": "https://www.example.com/subpath",
                    "confirmationUrl": "https://www.example.com",
                    "headers": [
                        {
                            "key": "static_header_key",
                            "value": "static_header_value"
```

```
                        },
                        {
                            "key": "substitutable_header_key",
                            "value": "${value_from_payload}"
                        }
                    ]
                }
            }
        ]
    }
}
```

## Logik zur Wiederholung von HTTP-Aktionen

Die AWS IoT Regel-Engine wiederholt die HTTP-Aktion gemäß den folgenden Regeln:

- Die Regel-Engine versucht mindestens einmal, eine Nachricht zu senden.
- Die Regel-Engine wiederholt den Versuch höchstens zweimal. Die maximale Anzahl von Versuchen ist drei.
- Die Regel-Engine unternimmt in folgenden Fällen keinen Wiederholungsversuch:
  - Der vorherige Versuch lieferte eine Antwort mit einer Größe von über 16.384 Bytes.
  - Der nachgeschaltete Webdienst oder die nachgeschaltete Anwendung schließt die TCP-Verbindung nach dem Versuch.
  - Die Gesamtzeit zum Abschließen einer Anforderung mit Wiederholungsversuchen hat das Zeitlimit für die Anforderung überschritten.
  - Die Anforderung gibt einen anderen HTTP-Statuscode als 429, 500–599 zurück.

> **Note**
>
> Für Wiederholungen fallen die Standardkosten für die Datenübertragung an.

## Weitere Informationen finden Sie auch unter

- Arbeiten mit HTTP-Themenregelzielen
- Leiten Sie Daten direkt von AWS IoT Core zu Ihren Webdiensten im Internet der Dinge im Blog weiter AWS

# Arbeiten mit HTTP-Themenregelzielen

Ein Ziel für HTTP-Themenregeln ist ein Webdienst, an den die Regel-Engine Daten aus einer Themenregel weiterleiten kann. Eine AWS IoT Core Ressource beschreibt den Webdienst für AWS IoT. Zielressourcen für Themenregeln können von verschiedenen Regeln gemeinsam genutzt werden.

Bevor Daten an einen anderen Webdienst gesendet werden AWS IoT Core können, muss dieser bestätigen, dass er auf den Endpunkt des Dienstes zugreifen kann.

In diesem Kapitel:


- Übersicht der HTTP-Themenregel
- Ziele für HTTP-Themenregeln verwalten
- Zertifizierungsstellen, die von HTTPS-Endpunkten an Zielorten für Themenregeln unterstützt werden


## Übersicht der HTTP-Themenregel

Ein Ziel für HTTP-Themenregeln bezieht sich auf einen Webdienst, der eine Bestätigungs-URL und eine oder mehrere Datenerfassungen unterstützt URLs. Die Zielressource für HTTP-Themenregeln enthält die Bestätigungs-URL Ihres Webdienstes. Wenn Sie eine Aktion für eine HTTP-Themenregel konfigurieren, geben Sie die tatsächliche URL des Endpunkts, der die Daten erhalten soll, zusammen mit der Bestätigungs-URL des Webdienstes an. Nachdem Ihr Ziel bestätigt wurde, sendet die Themenregel das Ergebnis der SQL-Anweisung an den HTTPS-Endpunkt (und nicht an die Bestätigungs-URL).

Ein HTTP-Themenziel kann die folgenden Zustände aufweisen:

ENABLED (AKTIVIERT)

Das Ziel wurde bestätigt und kann von einer Regelaktion verwendet werden. Ein Ziel muss den Zustand `ENABLED` aufweisen, damit es in einer Regel verwendet werden kann. Sie können nur Ziele im Status „DISABLED“ aktivieren.

DISABLED (DEAKTIVIERT)

Das Ziel wurde bestätigt, kann aber nicht von einer Regelaktion verwendet werden. Dies ist nützlich, wenn Sie Datenverkehr zu Ihrem Endpunkt vorübergehend aussetzen möchten, ohne

den Bestätigungsvorgang erneut durchlaufen zu müssen. Sie können nur Ziele mit dem Status „ENABLED“ deaktivieren.

IN_PROGRESS

Die Bestätigung des Ziels wird ausgeführt.

ERROR

Zeitüberschreitung bei der Zielbestätigung.

Nachdem das Ziel einer HTTP-Themenregel bestätigt und aktiviert wurde, kann es mit jeder Regel in Ihrem Konto verwendet werden.

In den folgenden Abschnitten werden allgemeine Aktionen für HTTP-Themenregelziele beschrieben.

### Ziele für HTTP-Themenregeln verwalten

Sie können die folgenden Operationen verwenden, um die Ziele Ihrer HTTP-Themenregeln zu verwalten.

In diesem Thema:


- Ziele für HTTP-Themenregeln erstellen
- Bestätigen der Ziele von HTTP-Themenregeln
- Senden einer neuen Bestätigungsanforderung
- Deaktivieren und Löschen eines Themenregelziels


### Ziele für HTTP-Themenregeln erstellen

Sie erstellen ein Ziel für HTTP-Themenregeln, indem Sie den `CreateTopicRuleDestination` Vorgang aufrufen oder die AWS IoT Konsole verwenden.

AWS IoT Sendet nach dem Erstellen eines Ziels eine Bestätigungsanfrage an die Bestätigungs-URL. Die Bestätigungsanforderung hat das folgende Format:

```
HTTP POST {confirmationUrl}/?confirmationToken={confirmationToken}
Headers:
x-amz-rules-engine-message-type: DestinationConfirmation
x-amz-rules-engine-destination-arn:"arn:aws:iot:us-east-1:123456789012:ruledestination/
http/7a280e37-b9c6-47a2-a751-0703693f46e4"
```

```
Content-Type: application/json
Body:
{
    "arn":"arn:aws:iot:us-east-1:123456789012:ruledestination/http/7a280e37-b9c6-47a2-
a751-0703693f46e4",
    "confirmationToken": "AYADeMXLrPrNY2wqJAKsFNn-…NBJndA",
    "enableUrl": "https://iot.us-east-1.amazonaws.com/confirmdestination/
AYADeMXLrPrNY2wqJAKsFNn-…NBJndA",
    "messageType": "DestinationConfirmation"
}
```

Der Inhalt der Bestätigungsanforderung umfasst die folgenden Informationen:

arn

Der Amazon Resource Name (ARN) für das Themenregelziel, das bestätigt werden soll.

confirmationToken

Das Bestätigungstoken, gesendet von AWS IoT Core. Das Token im Beispiel ist gekürzt. Ihr tatsächliches Token ist länger. Sie benötigen dieses Token, um Ihr Ziel mit AWS IoT Core zu bestätigen.

enableUrl

Die URL, zu der Sie navigieren, um ein Themenregelziel zu bestätigen.

messageType

Der Nachrichtentyp.

### Bestätigen der Ziele von HTTP-Themenregeln

Wenn Sie den Endpunkt-Bestätigungsprozess verwenden, müssen Sie die folgenden Schritte ausführen AWS CLI, nachdem Ihre Bestätigungs-URL die Bestätigungsanfrage erhalten hat.

1. Vergewissern Sie sich, dass das Ziel bereit ist, Nachrichten zu empfangen

   Um zu bestätigen, dass das Ziel der Themenregel bereit ist, IoT-Nachrichten zu empfangen, rufen Sie entweder die `enableUrl` in der Bestätigungsanfrage auf oder führen Sie den `ConfirmTopicRuleDestination` API-Vorgang `confirmationToken` aus und übergeben Sie die Bestätigungsanfrage.
2. Setzen Sie den Status der Themenregel auf aktiviert

Nachdem Sie bestätigt haben, dass das Ziel Nachrichten empfangen kann, müssen Sie den `UpdateTopicRuleDestination` API-Vorgang ausführen, um den Status der Themenregel auf zu setzen`ENABLED`.

Wenn Sie die AWS IoT Konsole verwenden, kopieren Sie die `confirmationToken` und fügen Sie sie in das Bestätigungsdialogfeld des Ziels in der AWS IoT Konsole ein. Anschließend können Sie die Themenregel aktivieren.

Senden einer neuen Bestätigungsanforderung

Zum Aktivieren einer neuen Bestätigungsnachricht für ein Ziel rufen Sie `UpdateTopicRuleDestination` auf und legen den Zustand des Themenregelziels auf `IN_PROGRESS` fest.

Wiederholen Sie den Bestätigungsvorgang, nachdem Sie eine neue Bestätigungsanforderung gesendet haben.

Deaktivieren und Löschen eines Themenregelziels

Zum Deaktivieren eines Ziels rufen Sie `UpdateTopicRuleDestination` auf und legen den Zustand des Themenregelziels auf `DISABLED` fest. Eine Themenregel mit dem Status DISABLED (DEAKTIVIERT) kann wieder aktiviert werden, ohne dass eine neue Bestätigungsanforderung gesendet werden muss.

Zum Löschen eines Themenregelziels rufen Sie `DeleteTopicRuleDestination` auf.

Zertifizierungsstellen, die von HTTPS-Endpunkten an Zielorten für Themenregeln unterstützt werden

Die folgenden Zertifizierungsstellen werden von HTTPS-Endpunkten in Zielorten für Themenregeln unterstützt. Sie können eine dieser unterstützten Zertifizierungsstellen auswählen. Die Signaturen dienen als Referenz. Beachten Sie, dass Sie keine selbstsignierten Zertifikate verwenden können, da diese nicht funktionieren.

Helfen Sie uns, dieses Thema zu verbessern

Teilen Sie uns mit, was Sie denken.

```
Alias name: swisssignplatinumg2ca
Certificate fingerprints:
```

```
  MD5:  C9:98:27:77:28:1E:3D:0E:15:3C:84:00:B8:85:03:E6
  SHA1: 56:E0:FA:C0:3B:8F:18:23:55:18:E5:D3:11:CA:E8:C2:43:31:AB:66
  SHA256:
 3B:22:2E:56:67:11:E9:92:30:0D:C0:B1:5A:B9:47:3D:AF:DE:F8:C8:4D:0C:EF:7D:33:17:B4:C1:82:1D:14:3

Alias name: hellenicacademicandresearchinstitutionsrootca2011
Certificate fingerprints:
  MD5:  73:9F:4C:4B:73:5B:79:E9:FA:BA:1C:EF:6E:CB:D5:C9
  SHA1: FE:45:65:9B:79:03:5B:98:A1:61:B5:51:2E:AC:DA:58:09:48:22:4D
  SHA256:
 BC:10:4F:15:A4:8B:E7:09:DC:A5:42:A7:E1:D4:B9:DF:6F:05:45:27:E8:02:EA:A9:2D:59:54:44:25:8A:FE:7

Alias name: teliasonerarootcav1
Certificate fingerprints:
  MD5:  37:41:49:1B:18:56:9A:26:F5:AD:C2:66:FB:40:A5:4C
  SHA1: 43:13:BB:96:F1:D5:86:9B:C1:4E:6A:92:F6:CF:F6:34:69:87:82:37
  SHA256:
 DD:69:36:FE:21:F8:F0:77:C1:23:A1:A5:21:C1:22:24:F7:22:55:B7:3E:03:A7:26:06:93:E8:A2:4B:0F:A3:8

Alias name: geotrustprimarycertificationauthority
Certificate fingerprints:
  MD5:  02:26:C3:01:5E:08:30:37:43:A9:D0:7D:CF:37:E6:BF
  SHA1: 32:3C:11:8E:1B:F7:B8:B6:52:54:E2:E2:10:0D:D6:02:90:37:F0:96
  SHA256:
 37:D5:10:06:C5:12:EA:AB:62:64:21:F1:EC:8C:92:01:3F:C5:F8:2A:E9:8E:E5:33:EB:46:19:B8:DE:B4:D0:6

Alias name: trustisfpsrootca
Certificate fingerprints:
  MD5:  30:C9:E7:1E:6B:E6:14:EB:65:B2:16:69:20:31:67:4D
  SHA1: 3B:C0:38:0B:33:C3:F6:A6:0C:86:15:22:93:D9:DF:F5:4B:81:C0:04
  SHA256:
 C1:B4:82:99:AB:A5:20:8F:E9:63:0A:CE:55:CA:68:A0:3E:DA:5A:51:9C:88:02:A0:D3:A6:73:BE:8F:8E:55:7

Alias name: quovadisrootca3g3
Certificate fingerprints:
  MD5:  DF:7D:B9:AD:54:6F:68:A1:DF:89:57:03:97:43:B0:D7
  SHA1: 48:12:BD:92:3C:A8:C4:39:06:E7:30:6D:27:96:E6:A4:CF:22:2E:7D
  SHA256:
 88:EF:81:DE:20:2E:B0:18:45:2E:43:F8:64:72:5C:EA:5F:BD:1F:C2:D9:D2:05:73:07:09:C5:D8:B8:69:0F:4

Alias name: buypassclass2ca
Certificate fingerprints:
  MD5:  46:A7:D2:FE:45:FB:64:5A:A8:59:90:9B:78:44:9B:29
  SHA1: 49:0A:75:74:DE:87:0A:47:FE:58:EE:F6:C7:6B:EB:C6:0B:12:40:99
```

```
  SHA256:
 9A:11:40:25:19:7C:5B:B9:5D:94:E6:3D:55:CD:43:79:08:47:B6:46:B2:3C:DF:11:AD:A4:A0:0E:FF:15:FB:4

Alias name: secureglobalca
Certificate fingerprints:
  MD5:  CF:F4:27:0D:D4:ED:DC:65:16:49:6D:3D:DA:BF:6E:DE
  SHA1: 3A:44:73:5A:E5:81:90:1F:24:86:61:46:1E:3B:9C:C4:5F:F5:3A:1B
  SHA256:
 42:00:F5:04:3A:C8:59:0E:BB:52:7D:20:9E:D1:50:30:29:FB:CB:D4:1C:A1:B5:06:EC:27:F1:5A:DE:7D:AC:6

Alias name: chunghwaepkirootca
Certificate fingerprints:
  MD5:  1B:2E:00:CA:26:06:90:3D:AD:FE:6F:15:68:D3:6B:B3
  SHA1: 67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0
  SHA256:
 C0:A6:F4:DC:63:A2:4B:FD:CF:54:EF:2A:6A:08:2A:0A:72:DE:35:80:3E:2F:F5:FF:52:7A:E5:D8:72:06:DF:D

Alias name: verisignclass2g2ca
Certificate fingerprints:
  MD5:  2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
  SHA1: B3:EA:C4:47:76:C9:C8:1C:EA:F2:9D:95:B6:CC:A0:08:1B:67:EC:9D
  SHA256:
 3A:43:E2:20:FE:7F:3E:A9:65:3D:1E:21:74:2E:AC:2B:75:C2:0F:D8:98:03:05:BC:50:2C:AF:8C:2D:9B:41:A

Alias name: szafirrootca2
Certificate fingerprints:
  MD5:  11:64:C1:89:B0:24:B1:8C:B1:07:7E:89:9E:51:9E:99
  SHA1: E2:52:FA:95:3F:ED:DB:24:60:BD:6E:28:F3:9C:CC:CF:5E:B3:3F:DE
  SHA256:
 A1:33:9D:33:28:1A:0B:56:E5:57:D3:D3:2B:1C:E7:F9:36:7E:B0:94:BD:5F:A7:2A:7E:50:04:C8:DE:D7:CA:F

Alias name: quovadisrootca1g3
Certificate fingerprints:
  MD5:  A4:BC:5B:3F:FE:37:9A:FA:64:F0:E2:FA:05:3D:0B:AB
  SHA1: 1B:8E:EA:57:96:29:1A:C9:39:EA:B8:0A:81:1A:73:73:C0:93:79:67
  SHA256:
 8A:86:6F:D1:B2:76:B5:7E:57:8E:92:1C:65:82:8A:2B:ED:58:E9:F2:F2:88:05:41:34:B7:F1:F4:BF:C9:CC:7

Alias name: utndatacorpsgcca
Certificate fingerprints:
  MD5:  B3:A5:3E:77:21:6D:AC:4A:C0:C9:FB:D5:41:3D:CA:06
  SHA1: 58:11:9F:0E:12:82:87:EA:50:FD:D9:87:45:6F:4F:78:DC:FA:D6:D4
  SHA256:
 85:FB:2F:91:DD:12:27:5A:01:45:B6:36:53:4F:84:02:4A:D6:8B:69:B8:EE:88:68:4F:F7:11:37:58:05:B3:4
```

```
Alias name: autoridaddecertificacionfirmaprofesionalcifa62634068
Certificate fingerprints:
  MD5:  73:3A:74:7A:EC:BB:A3:96:A6:C2:E4:E2:C8:9B:C0:C3
  SHA1: AE:C5:FB:3F:C8:E1:BF:C4:E5:4F:03:07:5A:9A:E8:00:B7:F7:B6:FA
  SHA256:
 04:04:80:28:BF:1F:28:64:D4:8F:9A:D4:D8:32:94:36:6A:82:88:56:55:3F:3B:14:30:3F:90:14:7F:5D:40:E

Alias name: securesignrootca11
Certificate fingerprints:
  MD5:  B7:52:74:E2:92:B4:80:93:F2:75:E4:CC:D7:F2:EA:26
  SHA1: 3B:C4:9F:48:F8:F3:73:A0:9C:1E:BD:F8:5B:B1:C3:65:C7:D8:11:B3
  SHA256:
 BF:0F:EE:FB:9E:3A:58:1A:D5:F9:E9:DB:75:89:98:57:43:D2:61:08:5C:4D:31:4F:6F:5D:72:59:AA:42:16:1

Alias name: amazon-ca-g4-acm2
Certificate fingerprints:
  MD5:  B2:F1:03:2B:93:64:05:80:B8:A8:17:36:B9:1B:52:3C
  SHA1: A7:E6:45:32:1F:7A:B7:AD:C0:70:EA:73:5F:AB:ED:C3:DA:B4:D0:C8
  SHA256:
 D7:A8:7C:69:95:D0:E2:04:2A:32:70:A7:E2:87:FE:A7:E8:F4:C1:70:62:F7:90:C3:EB:BB:53:F2:AC:39:26:B

Alias name: isrgrootx1
Certificate fingerprints:
  MD5:  0C:D2:F9:E0:DA:17:73:E9:ED:86:4D:A5:E3:70:E7:4E
  SHA1: CA:BD:2A:79:A1:07:6A:31:F2:1D:25:36:35:CB:03:9D:43:29:A5:E8
  SHA256:
 96:BC:EC:06:26:49:76:F3:74:60:77:9A:CF:28:C5:A7:CF:E8:A3:C0:AA:E1:1A:8F:FC:EE:05:C0:BD:DF:08:C

Alias name: amazon-ca-g4-acm1
Certificate fingerprints:
  MD5:  E2:F1:18:19:61:5C:43:E0:D4:A8:5D:0B:FA:7C:89:1B
  SHA1: F2:0D:28:B6:29:C2:2C:5E:84:05:E6:02:4D:97:FE:8F:A0:84:93:A0
  SHA256:
 B0:11:A4:F7:29:6C:74:D8:2B:F5:62:DF:87:D7:28:C7:1F:B5:8C:F4:E6:73:F2:78:FC:DA:F3:FF:83:A6:8C:8

Alias name: etugracertificationauthority
Certificate fingerprints:
  MD5:  B8:A1:03:63:B0:BD:21:71:70:8A:6F:13:3A:BB:79:49
  SHA1: 51:C6:E7:08:49:06:6E:F3:92:D4:5C:A0:0D:6D:A3:62:8F:C3:52:39
  SHA256:
 B0:BF:D5:2B:B0:D7:D9:BD:92:BF:5D:4D:C1:3D:A2:55:C0:2C:54:2F:37:83:65:EA:89:39:11:F5:5E:55:F2:3

Alias name: geotrustuniversalca2
```

```
Certificate fingerprints:
  MD5:  34:FC:B8:D0:36:DB:9E:14:B3:C2:F2:DB:8F:E4:94:C7
  SHA1: 37:9A:19:7B:41:85:45:35:0C:A6:03:69:F3:3C:2E:AF:47:4F:20:79
  SHA256:
 A0:23:4F:3B:C8:52:7C:A5:62:8E:EC:81:AD:5D:69:89:5D:A5:68:0D:C9:1D:1C:B8:47:7F:33:F8:78:B9:5B:0

Alias name: digicertglobalrootca
Certificate fingerprints:
  MD5:  79:E4:A9:84:0D:7D:3A:96:D7:C0:4F:E2:43:4C:89:2E
  SHA1: A8:98:5D:3A:65:E5:E5:C4:B2:D7:D6:6D:40:C6:DD:2F:B1:9C:54:36
  SHA256:
 43:48:A0:E9:44:4C:78:CB:26:5E:05:8D:5E:89:44:B4:D8:4F:96:62:BD:26:DB:25:7F:89:34:A4:43:C7:01:6

Alias name: staatdernederlandenevrootca
Certificate fingerprints:
  MD5:  FC:06:AF:7B:E8:1A:F1:9A:B4:E8:D2:70:1F:C0:F5:BA
  SHA1: 76:E2:7E:C1:4F:DB:82:C1:C0:A6:75:B5:05:BE:3D:29:B4:ED:DB:BB
  SHA256:
 4D:24:91:41:4C:FE:95:67:46:EC:4C:EF:A6:CF:6F:72:E2:8A:13:29:43:2F:9D:8A:90:7A:C4:CB:5D:AD:C1:5

Alias name: utnuserfirstclientauthemailca
Certificate fingerprints:
  MD5:  D7:34:3D:EF:1D:27:09:28:E1:31:02:5B:13:2B:DD:F7
  SHA1: B1:72:B1:A5:6D:95:F9:1F:E5:02:87:E1:4D:37:EA:6A:44:63:76:8A
  SHA256:
 43:F2:57:41:2D:44:0D:62:74:76:97:4F:87:7D:A8:F1:FC:24:44:56:5A:36:7A:E6:0E:DD:C2:7A:41:25:31:A

Alias name: actalisauthenticationrootca
Certificate fingerprints:
  MD5:  69:C1:0D:4F:07:A3:1B:C3:FE:56:3D:04:BC:11:F6:A6
  SHA1: F3:73:B3:87:06:5A:28:84:8A:F2:F3:4A:CE:19:2B:DD:C7:8E:9C:AC
  SHA256:
 55:92:60:84:EC:96:3A:64:B9:6E:2A:BE:01:CE:0B:A8:6A:64:FB:FE:BC:C7:AA:B5:AF:C1:55:B3:7F:D7:60:6

Alias name: amazonrootca4
Certificate fingerprints:
  MD5:  89:BC:27:D5:EB:17:8D:06:6A:69:D5:FD:89:47:B4:CD
  SHA1: F6:10:84:07:D6:F8:BB:67:98:0C:C2:E2:44:C2:EB:AE:1C:EF:63:BE
  SHA256:
 E3:5D:28:41:9E:D0:20:25:CF:A6:90:38:CD:62:39:62:45:8D:A5:C6:95:FB:DE:A3:C2:2B:0B:FB:25:89:70:9

Alias name: amazonrootca3
Certificate fingerprints:
  MD5:  A0:D4:EF:0B:F7:B5:D8:49:95:2A:EC:F5:C4:FC:81:87
```

```
  SHA1: 0D:44:DD:8C:3C:8C:1A:1A:58:75:64:81:E9:0F:2E:2A:FF:B3:D2:6E
  SHA256:
 18:CE:6C:FE:7B:F1:4E:60:B2:E3:47:B8:DF:E8:68:CB:31:D0:2E:BB:3A:DA:27:15:69:F5:03:43:B4:6D:B3:A

Alias name: amazonrootca2
Certificate fingerprints:
  MD5:  C8:E5:8D:CE:A8:42:E2:7A:C0:2A:5C:7C:9E:26:BF:66
  SHA1: 5A:8C:EF:45:D7:A6:98:59:76:7A:8C:8B:44:96:B5:78:CF:47:4B:1A
  SHA256:
 1B:A5:B2:AA:8C:65:40:1A:82:96:01:18:F8:0B:EC:4F:62:30:4D:83:CE:C4:71:3A:19:C3:9C:01:1E:A4:6D:B

Alias name: amazonrootca1
Certificate fingerprints:
  MD5:  43:C6:BF:AE:EC:FE:AD:2F:18:C6:88:68:30:FC:C8:E6
  SHA1: 8D:A7:F9:65:EC:5E:FC:37:91:0F:1C:6E:59:FD:C1:CC:6A:6E:DE:16
  SHA256:
 8E:CD:E6:88:4F:3D:87:B1:12:5B:A3:1A:C3:FC:B1:3D:70:16:DE:7F:57:CC:90:4F:E1:CB:97:C6:AE:98:19:6

Alias name: affirmtrustpremium
Certificate fingerprints:
  MD5:  C4:5D:0E:48:B6:AC:28:30:4E:0A:BC:F9:38:16:87:57
  SHA1: D8:A6:33:2C:E0:03:6F:B1:85:F6:63:4F:7D:6A:06:65:26:32:28:27
  SHA256:
 70:A7:3F:7F:37:6B:60:07:42:48:90:45:34:B1:14:82:D5:BF:0E:69:8E:CC:49:8D:F5:25:77:EB:F2:E9:3B:9

Alias name: keynectisrootca
Certificate fingerprints:
  MD5:  CC:4D:AE:FB:30:6B:D8:38:FE:50:EB:86:61:4B:D2:26
  SHA1: 9C:61:5C:4D:4D:85:10:3A:53:26:C2:4D:BA:EA:E4:A2:D2:D5:CC:97
  SHA256:
 42:10:F1:99:49:9A:9A:C3:3C:8D:E0:2B:A6:DB:AA:14:40:8B:DD:8A:6E:32:46:89:C1:92:2D:06:97:15:A3:3

Alias name: equifaxsecureglobalebusinessca1
Certificate fingerprints:
  MD5:  51:F0:2A:33:F1:F5:55:39:07:F2:16:7A:47:C7:5D:63
  SHA1: 3A:74:CB:7A:47:DB:70:DE:89:1F:24:35:98:64:B8:2D:82:BD:1A:36
  SHA256:
 86:AB:5A:65:71:D3:32:9A:BC:D2:E4:E6:37:66:8B:A8:9C:73:1E:C2:93:B6:CB:A6:0F:71:63:40:A0:91:CE:A

Alias name: affirmtrustpremiumca
Certificate fingerprints:
  MD5:  C4:5D:0E:48:B6:AC:28:30:4E:0A:BC:F9:38:16:87:57
  SHA1: D8:A6:33:2C:E0:03:6F:B1:85:F6:63:4F:7D:6A:06:65:26:32:28:27
```

```
  SHA256:
 70:A7:3F:7F:37:6B:60:07:42:48:90:45:34:B1:14:82:D5:BF:0E:69:8E:CC:49:8D:F5:25:77:EB:F2:E9:3B:9

Alias name: baltimorecodesigningca
Certificate fingerprints:
  MD5:  90:F5:28:49:56:D1:5D:2C:B0:53:D4:4B:EF:6F:90:22
  SHA1: 30:46:D8:C8:88:FF:69:30:C3:4A:FC:CD:49:27:08:7C:60:56:7B:0D
  SHA256:
 A9:15:45:DB:D2:E1:9C:4C:CD:F9:09:AA:71:90:0D:18:C7:35:1C:89:B3:15:F0:F1:3D:05:C1:3A:8F:FB:46:8

Alias name: gdcatrustauthr5root
Certificate fingerprints:
  MD5:  63:CC:D9:3D:34:35:5C:6F:53:A3:E2:08:70:48:1F:B4
  SHA1: 0F:36:38:5B:81:1A:25:C3:9B:31:4E:83:CA:E9:34:66:70:CC:74:B4
  SHA256:
 BF:FF:8F:D0:44:33:48:7D:6A:8A:A6:0C:1A:29:76:7A:9F:C2:BB:B0:5E:42:0F:71:3A:13:B9:92:89:1D:38:9

Alias name: certinomisrootca
Certificate fingerprints:
  MD5:  14:0A:FD:8D:A8:28:B5:38:69:DB:56:7E:61:22:03:3F
  SHA1: 9D:70:BB:01:A5:A4:A0:18:11:2E:F7:1C:01:B9:32:C5:34:E7:88:A8
  SHA256:
 2A:99:F5:BC:11:74:B7:3C:BB:1D:62:08:84:E0:1C:34:E5:1C:CB:39:78:DA:12:5F:0E:33:26:88:83:BF:41:5

Alias name: verisignclass3publicprimarycertificationauthorityg5
Certificate fingerprints:
  MD5:  CB:17:E4:31:67:3E:E2:09:FE:45:57:93:F3:0A:FA:1C
  SHA1: 4E:B6:D5:78:49:9B:1C:CF:5F:58:1E:AD:56:BE:3D:9B:67:44:A5:E5
  SHA256:
 9A:CF:AB:7E:43:C8:D8:80:D0:6B:26:2A:94:DE:EE:E4:B4:65:99:89:C3:D0:CA:F1:9B:AF:64:05:E4:1A:B7:D

Alias name: verisignclass3publicprimarycertificationauthorityg4
Certificate fingerprints:
  MD5:  3A:52:E1:E7:FD:6F:3A:E3:6F:F3:6F:99:1B:F9:22:41
  SHA1: 22:D5:D8:DF:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A
  SHA256:
 69:DD:D7:EA:90:BB:57:C9:3E:13:5D:C8:5E:A6:FC:D5:48:0B:60:32:39:BD:C4:54:FC:75:8B:2A:26:CF:7F:7

Alias name: verisignclass3publicprimarycertificationauthorityg3
Certificate fingerprints:
  MD5:  CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:57:44:61:92:09
  SHA1: 13:2D:0D:45:53:4B:69:97:CD:B2:D5:C3:39:E2:55:76:60:9B:5C:C6
  SHA256:
 EB:04:CF:5E:B1:F3:9A:FA:76:2F:2B:B1:20:F2:96:CB:A5:20:C1:B9:7D:B1:58:95:65:B8:1C:B9:A1:7B:72:4
```

```
Alias name: swisssignsilverg2ca
Certificate fingerprints:
  MD5:  E0:06:A1:C9:7D:CF:C9:FC:0D:C0:56:75:96:D8:62:13
  SHA1: 9B:AA:E5:9F:56:EE:21:CB:43:5A:BE:25:93:DF:A7:F0:40:D1:1D:CB
  SHA256:
 BE:6C:4D:A2:BB:B9:BA:59:B6:F3:93:97:68:37:42:46:C3:C0:05:99:3F:A9:8F:02:0D:1D:ED:BE:D4:8A:81:D

Alias name: swisssignsilvercag2
Certificate fingerprints:
  MD5:  E0:06:A1:C9:7D:CF:C9:FC:0D:C0:56:75:96:D8:62:13
  SHA1: 9B:AA:E5:9F:56:EE:21:CB:43:5A:BE:25:93:DF:A7:F0:40:D1:1D:CB
  SHA256:
 BE:6C:4D:A2:BB:B9:BA:59:B6:F3:93:97:68:37:42:46:C3:C0:05:99:3F:A9:8F:02:0D:1D:ED:BE:D4:8A:81:D

Alias name: atostrustedroot2011
Certificate fingerprints:
  MD5:  AE:B9:C4:32:4B:AC:7F:5D:66:CC:77:94:BB:2A:77:56
  SHA1: 2B:B1:F5:3E:55:0C:1D:C5:F1:D4:E6:B7:6A:46:4B:55:06:02:AC:21
  SHA256:
 F3:56:BE:A2:44:B7:A9:1E:B3:5D:53:CA:9A:D7:86:4A:CE:01:8E:2D:35:D5:F8:F9:6D:DF:68:A6:F4:1A:A4:7

Alias name: comodoecccertificationauthority
Certificate fingerprints:
  MD5:  7C:62:FF:74:9D:31:53:5E:68:4A:D5:78:AA:1E:BF:23
  SHA1: 9F:74:4E:9F:2B:4D:BA:EC:0F:31:2C:50:B6:56:3B:8E:2D:93:C3:11
  SHA256:
 17:93:92:7A:06:14:54:97:89:AD:CE:2F:8F:34:F7:F0:B6:6D:0F:3A:E3:A3:B8:4D:21:EC:15:DB:BA:4F:AD:C

Alias name: securetrustca
Certificate fingerprints:
  MD5:  DC:32:C3:A7:6D:25:57:C7:68:09:9D:EA:2D:A9:A2:D1
  SHA1: 87:82:C6:C3:04:35:3B:CF:D2:96:92:D2:59:3E:7D:44:D9:34:FF:11
  SHA256:
 F1:C1:B5:0A:E5:A2:0D:D8:03:0E:C9:F6:BC:24:82:3D:D3:67:B5:25:57:59:B4:E7:1B:61:FC:E9:F7:37:5D:7

Alias name: soneraclass1ca
Certificate fingerprints:
  MD5:  33:B7:84:F5:5F:27:D7:68:27:DE:14:DE:12:2A:ED:6F
  SHA1: 07:47:22:01:99:CE:74:B9:7C:B0:3D:79:B2:64:A2:C8:55:E9:33:FF
  SHA256:
 CD:80:82:84:CF:74:6F:F2:FD:6E:B5:8A:A1:D5:9C:4A:D4:B3:CA:56:FD:C6:27:4A:89:26:A7:83:5F:32:31:3

Alias name: cadisigrootr2
```

```
Certificate fingerprints:
  MD5:  26:01:FB:D8:27:A7:17:9A:45:54:38:1A:43:01:3B:03
  SHA1: B5:61:EB:EA:A4:DE:E4:25:4B:69:1A:98:A5:57:47:C2:34:C7:D9:71
  SHA256:
 E2:3D:4A:03:6D:7B:70:E9:F5:95:B1:42:20:79:D2:B9:1E:DF:BB:1F:B6:51:A0:63:3E:AA:8A:9D:C5:F8:07:0

Alias name: cadisigrootr1
Certificate fingerprints:
  MD5:  BE:EC:11:93:9A:F5:69:21:BC:D7:C1:C0:67:89:CC:2A
  SHA1: 8E:1C:74:F8:A6:20:B9:E5:8A:F4:61:FA:EC:2B:47:56:51:1A:52:C6
  SHA256:
 F9:6F:23:F4:C3:E7:9C:07:7A:46:98:8D:5A:F5:90:06:76:A0:F0:39:CB:64:5D:D1:75:49:B2:16:C8:24:40:C

Alias name: verisignclass3g5ca
Certificate fingerprints:
  MD5:  CB:17:E4:31:67:3E:E2:09:FE:45:57:93:F3:0A:FA:1C
  SHA1: 4E:B6:D5:78:49:9B:1C:CF:5F:58:1E:AD:56:BE:3D:9B:67:44:A5:E5
  SHA256:
 9A:CF:AB:7E:43:C8:D8:80:D0:6B:26:2A:94:DE:EE:E4:B4:65:99:89:C3:D0:CA:F1:9B:AF:64:05:E4:1A:B7:D

Alias name: utnuserfirsthardwareca
Certificate fingerprints:
  MD5:  4C:56:41:E5:0D:BB:2B:E8:CA:A3:ED:18:08:AD:43:39
  SHA1: 04:83:ED:33:99:AC:36:08:05:87:22:ED:BC:5E:46:00:E3:BE:F9:D7
  SHA256:
 6E:A5:47:41:D0:04:66:7E:ED:1B:48:16:63:4A:A3:A7:9E:6E:4B:96:95:0F:82:79:DA:FC:8D:9B:D8:81:21:3

Alias name: addtrustqualifiedca
Certificate fingerprints:
  MD5:  27:EC:39:47:CD:DA:5A:AF:E2:9A:01:65:21:A9:4C:BB
  SHA1: 4D:23:78:EC:91:95:39:B5:00:7F:75:8F:03:3B:21:1E:C5:4D:8B:CF
  SHA256:
 80:95:21:08:05:DB:4B:BC:35:5E:44:28:D8:FD:6E:C2:CD:E3:AB:5F:B9:7A:99:42:98:8E:B8:F4:DC:D0:60:1

Alias name: verisignclass3g3ca
Certificate fingerprints:
  MD5:  CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:57:44:61:92:09
  SHA1: 13:2D:0D:45:53:4B:69:97:CD:B2:D5:C3:39:E2:55:76:60:9B:5C:C6
  SHA256:
 EB:04:CF:5E:B1:F3:9A:FA:76:2F:2B:B1:20:F2:96:CB:A5:20:C1:B9:7D:B1:58:95:65:B8:1C:B9:A1:7B:72:4

Alias name: thawtepersonalfreemailca
Certificate fingerprints:
  MD5:  53:4B:1D:17:58:58:1A:30:A1:90:F8:6E:5C:F2:CF:65
```

```
  SHA1: E6:18:83:AE:84:CA:C1:C1:CD:52:AD:E8:E9:25:2B:45:A6:4F:B7:E2
  SHA256:
 5B:38:BD:12:9E:83:D5:A0:CA:D2:39:21:08:94:90:D5:0D:4A:AE:37:04:28:F8:DD:FF:FF:FA:4C:15:64:E1:8

Alias name: certplusclass3pprimaryca
Certificate fingerprints:
  MD5:  E1:4B:52:73:D7:1B:DB:93:30:E5:BD:E4:09:6E:BE:FB
  SHA1: 21:6B:2A:29:E6:2A:00:CE:82:01:46:D8:24:41:41:B9:25:11:B2:79
  SHA256:
 CC:C8:94:89:37:1B:AD:11:1C:90:61:9B:EA:24:0A:2E:6D:AD:D9:9F:9F:6E:1D:4D:41:E5:8E:D6:DE:3D:02:8

Alias name: swisssigngoldg2ca
Certificate fingerprints:
  MD5:  24:77:D9:A8:91:D1:3B:FA:88:2D:C2:FF:F8:CD:33:93
  SHA1: D8:C5:38:8A:B7:30:1B:1B:6E:D4:7A:E6:45:25:3A:6F:9F:1A:27:61
  SHA256:
 62:DD:0B:E9:B9:F5:0A:16:3E:A0:F8:E7:5C:05:3B:1E:CA:57:EA:55:C8:68:8F:64:7C:68:81:F2:C8:35:7B:9

Alias name: swisssigngoldcag2
Certificate fingerprints:
  MD5:  24:77:D9:A8:91:D1:3B:FA:88:2D:C2:FF:F8:CD:33:93
  SHA1: D8:C5:38:8A:B7:30:1B:1B:6E:D4:7A:E6:45:25:3A:6F:9F:1A:27:61
  SHA256:
 62:DD:0B:E9:B9:F5:0A:16:3E:A0:F8:E7:5C:05:3B:1E:CA:57:EA:55:C8:68:8F:64:7C:68:81:F2:C8:35:7B:9

Alias name: dtrustrootclass3ca22009
Certificate fingerprints:
  MD5:  CD:E0:25:69:8D:47:AC:9C:89:35:90:F7:FD:51:3D:2F
  SHA1: 58:E8:AB:B0:36:15:33:FB:80:F7:9B:1B:6D:29:D3:FF:8D:5F:00:F0
  SHA256:
 49:E7:A4:42:AC:F0:EA:62:87:05:00:54:B5:25:64:B6:50:E4:F4:9E:42:E3:48:D6:AA:38:E0:39:E9:57:B1:C

Alias name: acraizfnmtrcm
Certificate fingerprints:
  MD5:  E2:09:04:B4:D3:BD:D1:A0:14:FD:1A:D2:47:C4:57:1D
  SHA1: EC:50:35:07:B2:15:C4:95:62:19:E2:A8:9A:5B:42:99:2C:4C:2C:20
  SHA256:
 EB:C5:57:0C:29:01:8C:4D:67:B1:AA:12:7B:AF:12:F7:03:B4:61:1E:BC:17:B7:DA:B5:57:38:94:17:9B:93:F

Alias name: securitycommunicationevrootca1
Certificate fingerprints:
  MD5:  22:2D:A6:01:EA:7C:0A:F7:F0:6C:56:43:3F:77:76:D3
  SHA1: FE:B8:C4:32:DC:F9:76:9A:CE:AE:3D:D8:90:8F:FD:28:86:65:64:7D
```

```
  SHA256:
 A2:2D:BA:68:1E:97:37:6E:2D:39:7D:72:8A:AE:3A:9B:62:96:B9:FD:BA:60:BC:2E:11:F6:47:F2:C6:75:FB:3

Alias name: starfieldclass2ca
Certificate fingerprints:
  MD5:  32:4A:4B:BB:C8:63:69:9B:BE:74:9A:C6:DD:1D:46:24
  SHA1: AD:7E:1C:28:B0:64:EF:8F:60:03:40:20:14:C3:D0:E3:37:0E:B5:8A
  SHA256:
 14:65:FA:20:53:97:B8:76:FA:A6:F0:A9:95:8E:55:90:E4:0F:CC:7F:AA:4F:B7:C2:C8:67:75:21:FB:5F:B6:5

Alias name: opentrustrootcag3
Certificate fingerprints:
  MD5:  21:37:B4:17:16:92:7B:67:46:70:A9:96:D7:A8:13:24
  SHA1: 6E:26:64:F3:56:BF:34:55:BF:D1:93:3F:7C:01:DE:D8:13:DA:8A:A6
  SHA256:
 B7:C3:62:31:70:6E:81:07:8C:36:7C:B8:96:19:8F:1E:32:08:DD:92:69:49:DD:8F:57:09:A4:10:F7:5B:62:9

Alias name: opentrustrootcag2
Certificate fingerprints:
  MD5:  57:24:B6:59:24:6B:AE:C8:FE:1C:0C:20:F2:C0:4E:EB
  SHA1: 79:5F:88:60:C5:AB:7C:3D:92:E6:CB:F4:8D:E1:45:CD:11:EF:60:0B
  SHA256:
 27:99:58:29:FE:6A:75:15:C1:BF:E8:48:F9:C4:76:1D:B1:6C:22:59:29:25:7B:F4:0D:08:94:F2:9E:A8:BA:F

Alias name: buypassclass2rootca
Certificate fingerprints:
  MD5:  46:A7:D2:FE:45:FB:64:5A:A8:59:90:9B:78:44:9B:29
  SHA1: 49:0A:75:74:DE:87:0A:47:FE:58:EE:F6:C7:6B:EB:C6:0B:12:40:99
  SHA256:
 9A:11:40:25:19:7C:5B:B9:5D:94:E6:3D:55:CD:43:79:08:47:B6:46:B2:3C:DF:11:AD:A4:A0:0E:FF:15:FB:4

Alias name: opentrustrootcag1
Certificate fingerprints:
  MD5:  76:00:CC:81:29:CD:55:5E:88:6A:7A:2E:F7:4D:39:DA
  SHA1: 79:91:E8:34:F7:E2:EE:DD:08:95:01:52:E9:55:2D:14:E9:58:D5:7E
  SHA256:
 56:C7:71:28:D9:8C:18:D9:1B:4C:FD:FF:BC:25:EE:91:03:D4:75:8E:A2:AB:AD:82:6A:90:F3:45:7D:46:0E:B

Alias name: globalsignr2ca
Certificate fingerprints:
  MD5:  94:14:77:7E:3E:5E:FD:8F:30:BD:41:B0:CF:E7:D0:30
  SHA1: 75:E0:AB:B6:13:85:12:27:1C:04:F8:5F:DD:DE:38:E4:B7:24:2E:FE
  SHA256:
 CA:42:DD:41:74:5F:D0:B8:1E:B9:02:36:2C:F9:D8:BF:71:9D:A1:BD:1B:1E:FC:94:6F:5B:4C:99:F4:2C:1B:9
```

```
Alias name: buypassclass3rootca
Certificate fingerprints:
  MD5:  3D:3B:18:9E:2C:64:5A:E8:D5:88:CE:0E:F9:37:C2:EC
  SHA1: DA:FA:F7:FA:66:84:EC:06:8F:14:50:BD:C7:C2:81:A5:BC:A9:64:57
  SHA256:
 ED:F7:EB:BC:A2:7A:2A:38:4D:38:7B:7D:40:10:C6:66:E2:ED:B4:84:3E:4C:29:B4:AE:1D:5B:93:32:E6:B2:4

Alias name: ecacc
Certificate fingerprints:
  MD5:  EB:F5:9D:29:0D:61:F9:42:1F:7C:C2:BA:6D:E3:15:09
  SHA1: 28:90:3A:63:5B:52:80:FA:E6:77:4C:0B:6D:A7:D6:BA:A6:4A:F2:E8
  SHA256:
 88:49:7F:01:60:2F:31:54:24:6A:E2:8C:4D:5A:EF:10:F1:D8:7E:BB:76:62:6F:4A:E0:B7:F9:5B:A7:96:87:9

Alias name: epkirootcertificationauthority
Certificate fingerprints:
  MD5:  1B:2E:00:CA:26:06:90:3D:AD:FE:6F:15:68:D3:6B:B3
  SHA1: 67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0
  SHA256:
 C0:A6:F4:DC:63:A2:4B:FD:CF:54:EF:2A:6A:08:2A:0A:72:DE:35:80:3E:2F:F5:FF:52:7A:E5:D8:72:06:DF:D

Alias name: verisignclass1g2ca
Certificate fingerprints:
  MD5:  DB:23:3D:F9:69:FA:4B:B9:95:80:44:73:5E:7D:41:83
  SHA1: 27:3E:E1:24:57:FD:C4:F9:0C:55:E8:2B:56:16:7F:62:F5:32:E5:47
  SHA256:
 34:1D:E9:8B:13:92:AB:F7:F4:AB:90:A9:60:CF:25:D4:BD:6E:C6:5B:9A:51:CE:6E:D0:67:D0:0E:C7:CE:9B:7

Alias name: certigna
Certificate fingerprints:
  MD5:  AB:57:A6:5B:7D:42:82:19:B5:D8:58:26:28:5E:FD:FF
  SHA1: B1:2E:13:63:45:86:A4:6F:1A:B2:60:68:37:58:2D:C4:AC:FD:94:97
  SHA256:
 E3:B6:A2:DB:2E:D7:CE:48:84:2F:7A:C5:32:41:C7:B7:1D:54:14:4B:FB:40:C1:1F:3F:1D:0B:42:F5:EE:A1:2

Alias name: camerfirmaglobalchambersignroot
Certificate fingerprints:
  MD5:  C5:E6:7B:BF:06:D0:4F:43:ED:C4:7A:65:8A:FB:6B:19
  SHA1: 33:9B:6B:14:50:24:9B:55:7A:01:87:72:84:D9:E0:2F:C3:D2:D8:E9
  SHA256:
 EF:3C:B4:17:FC:8E:BF:6F:97:87:6C:9E:4E:CE:39:DE:1E:A5:FE:64:91:41:D1:02:8B:7D:11:C0:B2:29:8C:E

Alias name: cfcaevroot
```

```
Certificate fingerprints:
  MD5:  74:E1:B6:ED:26:7A:7A:44:30:33:94:AB:7B:27:81:30
  SHA1: E2:B8:29:4B:55:84:AB:6B:58:C2:90:46:6C:AC:3F:B8:39:8F:84:83
  SHA256:
 5C:C3:D7:8E:4E:1D:5E:45:54:7A:04:E6:87:3E:64:F9:0C:F9:53:6D:1C:CC:2E:F8:00:F3:55:C4:C5:FD:70:F

Alias name: soneraclass2rootca
Certificate fingerprints:
  MD5:  A3:EC:75:0F:2E:88:DF:FA:48:01:4E:0B:5C:48:6F:FB
  SHA1: 37:F7:6D:E6:07:7C:90:C5:B1:3E:93:1A:B7:41:10:B4:F2:E4:9A:27
  SHA256:
 79:08:B4:03:14:C1:38:10:0B:51:8D:07:35:80:7F:FB:FC:F8:51:8A:00:95:33:71:05:BA:38:6B:15:3D:D9:2

Alias name: certumtrustednetworkca
Certificate fingerprints:
  MD5:  D5:E9:81:40:C5:18:69:FC:46:2C:89:75:62:0F:AA:78
  SHA1: 07:E0:32:E0:20:B7:2C:3F:19:2F:06:28:A2:59:3A:19:A7:0F:06:9E
  SHA256:
 5C:58:46:8D:55:F5:8E:49:7E:74:39:82:D2:B5:00:10:B6:D1:65:37:4A:CF:83:A7:D4:A3:2D:B7:68:C4:40:8

Alias name: securitycommunicationrootca2
Certificate fingerprints:
  MD5:  6C:39:7D:A4:0E:55:59:B2:3F:D6:41:B1:12:50:DE:43
  SHA1: 5F:3B:8C:F2:F8:10:B3:7D:78:B4:CE:EC:19:19:C3:73:34:B9:C7:74
  SHA256:
 51:3B:2C:EC:B8:10:D4:CD:E5:DD:85:39:1A:DF:C6:C2:DD:60:D8:7B:B7:36:D2:B5:21:48:4A:A4:7A:0E:BE:F

Alias name: globalsigneccrootcar5
Certificate fingerprints:
  MD5:  9F:AD:3B:1C:02:1E:8A:BA:17:74:38:81:0C:A2:BC:08
  SHA1: 1F:24:C6:30:CD:A4:18:EF:20:69:FF:AD:4F:DD:5F:46:3A:1B:69:AA
  SHA256:
 17:9F:BC:14:8A:3D:D0:0F:D2:4E:A1:34:58:CC:43:BF:A7:F5:9C:81:82:D7:83:A5:13:F6:EB:EC:10:0C:89:2

Alias name: globalsigneccrootcar4
Certificate fingerprints:
  MD5:  20:F0:27:68:D1:7E:A0:9D:0E:E6:2A:CA:DF:5C:89:8E
  SHA1: 69:69:56:2E:40:80:F4:24:A1:E7:19:9F:14:BA:F3:EE:58:AB:6A:BB
  SHA256:
 BE:C9:49:11:C2:95:56:76:DB:6C:0A:55:09:86:D7:6E:3B:A0:05:66:7C:44:2C:97:62:B4:FB:B7:73:DE:22:8

Alias name: chambersofcommerceroot2008
Certificate fingerprints:
  MD5:  5E:80:9E:84:5A:0E:65:0B:17:02:F3:55:18:2A:3E:D7
```

```
  SHA1: 78:6A:74:AC:76:AB:14:7F:9C:6A:30:50:BA:9E:A8:7E:FE:9A:CE:3C
  SHA256:
 06:3E:4A:FA:C4:91:DF:D3:32:F3:08:9B:85:42:E9:46:17:D8:93:D7:FE:94:4E:10:A7:93:7E:E2:9D:96:93:C

Alias name: pscprocert
Certificate fingerprints:
  MD5:  E6:24:E9:12:01:AE:0C:DE:8E:85:C4:CE:A3:12:DD:EC
  SHA1: 70:C1:8D:74:B4:28:81:0A:E4:FD:A5:75:D7:01:9F:99:B0:3D:50:74
  SHA256:
 3C:FC:3C:14:D1:F6:84:FF:17:E3:8C:43:CA:44:0C:00:B9:67:EC:93:3E:8B:FE:06:4C:A1:D7:2C:90:F2:AD:B

Alias name: thawteprimaryrootcag3
Certificate fingerprints:
  MD5:  FB:1B:5D:43:8A:94:CD:44:C6:76:F2:43:4B:47:E7:31
  SHA1: F1:8B:53:8D:1B:E9:03:B6:A6:F0:56:43:5B:17:15:89:CA:F3:6B:F2
  SHA256:
 4B:03:F4:58:07:AD:70:F2:1B:FC:2C:AE:71:C9:FD:E4:60:4C:06:4C:F5:FF:B6:86:BA:E5:DB:AA:D7:FD:D3:4

Alias name: quovadisrootca
Certificate fingerprints:
  MD5:  27:DE:36:FE:72:B7:00:03:00:9D:F4:F0:1E:6C:04:24
  SHA1: DE:3F:40:BD:50:93:D3:9B:6C:60:F6:DA:BC:07:62:01:00:89:76:C9
  SHA256:
 A4:5E:DE:3B:BB:F0:9C:8A:E1:5C:72:EF:C0:72:68:D6:93:A2:1C:99:6F:D5:1E:67:CA:07:94:60:FD:6D:88:7

Alias name: thawteprimaryrootcag2
Certificate fingerprints:
  MD5:  74:9D:EA:60:24:C4:FD:22:53:3E:CC:3A:72:D9:29:4F
  SHA1: AA:DB:BC:22:23:8F:C4:01:A1:27:BB:38:DD:F4:1D:DB:08:9E:F0:12
  SHA256:
 A4:31:0D:50:AF:18:A6:44:71:90:37:2A:86:AF:AF:8B:95:1F:FB:43:1D:83:7F:1E:56:88:B4:59:71:ED:15:5

Alias name: deprecateditsecca
Certificate fingerprints:
  MD5:  A5:96:0C:F6:B5:AB:27:E5:01:C6:00:88:9E:60:33:E5
  SHA1: 12:12:0B:03:0E:15:14:54:F4:DD:B3:F5:DE:13:6E:83:5A:29:72:9D
  SHA256:
 9A:59:DA:86:24:1A:FD:BA:A3:39:FA:9C:FD:21:6A:0B:06:69:4D:E3:7E:37:52:6B:BE:63:C8:BC:83:74:2E:C

Alias name: usertrustrsacertificationauthority
Certificate fingerprints:
  MD5:  1B:FE:69:D1:91:B7:19:33:A3:72:A8:0F:E1:55:E5:B5
  SHA1: 2B:8F:1B:57:33:0D:BB:A2:D0:7A:6C:51:F7:0E:E9:0D:DA:B9:AD:8E
```

```
  SHA256:
 E7:93:C9:B0:2F:D8:AA:13:E2:1C:31:22:8A:CC:B0:81:19:64:3B:74:9C:89:89:64:B1:74:6D:46:C3:D4:CB:D

Alias name: entrustrootcag2
Certificate fingerprints:
  MD5:  4B:E2:C9:91:96:65:0C:F4:0E:5A:93:92:A0:0A:FE:B2
  SHA1: 8C:F4:27:FD:79:0C:3A:D1:66:06:8D:E8:1E:57:EF:BB:93:22:72:D4
  SHA256:
 43:DF:57:74:B0:3E:7F:EF:5F:E4:0D:93:1A:7B:ED:F1:BB:2E:6B:42:73:8C:4E:6D:38:41:10:3D:3A:A7:F3:3

Alias name: networksolutionscertificateauthority
Certificate fingerprints:
  MD5:  D3:F3:A6:16:C0:FA:6B:1D:59:B1:2D:96:4D:0E:11:2E
  SHA1: 74:F8:A3:C3:EF:E7:B3:90:06:4B:83:90:3C:21:64:60:20:E5:DF:CE
  SHA256:
 15:F0:BA:00:A3:AC:7A:F3:AC:88:4C:07:2B:10:11:A0:77:BD:77:C0:97:F4:01:64:B2:F8:59:8A:BD:83:86:0

Alias name: trustcenterclass4caii
Certificate fingerprints:
  MD5:  9D:FB:F9:AC:ED:89:33:22:F4:28:48:83:25:23:5B:E0
  SHA1: A6:9A:91:FD:05:7F:13:6A:42:63:0B:B1:76:0D:2D:51:12:0C:16:50
  SHA256:
 32:66:96:7E:59:CD:68:00:8D:9D:D3:20:81:11:85:C7:04:20:5E:8D:95:FD:D8:4F:1C:7B:31:1E:67:04:FC:3

Alias name: oistewisekeyglobalrootgaca
Certificate fingerprints:
  MD5:  BC:6C:51:33:A7:E9:D3:66:63:54:15:72:1B:21:92:93
  SHA1: 59:22:A1:E1:5A:EA:16:35:21:F8:98:39:6A:46:46:B0:44:1B:0F:A9
  SHA256:
 41:C9:23:86:6A:B4:CA:D6:B7:AD:57:80:81:58:2E:02:07:97:A6:CB:DF:4F:FF:78:CE:83:96:B3:89:37:D7:F

Alias name: verisignuniversalrootcertificationauthority
Certificate fingerprints:
  MD5:  8E:AD:B5:01:AA:4D:81:E4:8C:1D:D1:E1:14:00:95:19
  SHA1: 36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54
  SHA256:
 23:99:56:11:27:A5:71:25:DE:8C:EF:EA:61:0D:DF:2F:A0:78:B5:C8:06:7F:4E:82:82:90:BF:B8:60:E8:4B:3

Alias name: ttelesecglobalrootclass3ca
Certificate fingerprints:
  MD5:  CA:FB:40:A8:4E:39:92:8A:1D:FE:8E:2F:C4:27:EA:EF
  SHA1: 55:A6:72:3E:CB:F2:EC:CD:C3:23:74:70:19:9D:2A:BE:11:E3:81:D1
  SHA256:
 FD:73:DA:D3:1C:64:4F:F1:B4:3B:EF:0C:CD:DA:96:71:0B:9C:D9:87:5E:CA:7E:31:70:7A:F3:E9:6D:52:2B:B
```

```
Alias name: starfieldservicesrootg2ca
Certificate fingerprints:
  MD5:  17:35:74:AF:7B:61:1C:EB:F4:F9:3C:E2:EE:40:F9:A2
  SHA1: 92:5A:8F:8D:2C:6D:04:E0:66:5F:59:6A:FF:22:D8:63:E8:25:6F:3F
  SHA256:
 56:8D:69:05:A2:C8:87:08:A4:B3:02:51:90:ED:CF:ED:B1:97:4A:60:6A:13:C6:E5:29:0F:CB:2A:E6:3E:DA:B

Alias name: addtrustexternalroot
Certificate fingerprints:
  MD5:  1D:35:54:04:85:78:B0:3F:42:42:4D:BF:20:73:0A:3F
  SHA1: 02:FA:F3:E2:91:43:54:68:60:78:57:69:4D:F5:E4:5B:68:85:18:68
  SHA256:
 68:7F:A4:51:38:22:78:FF:F0:C8:B1:1F:8D:43:D5:76:67:1C:6E:B2:BC:EA:B4:13:FB:83:D9:65:D0:6D:2F:F

Alias name: turktrustelektroniksertifikahizmetsaglayicisih5
Certificate fingerprints:
  MD5:  DA:70:8E:F0:22:DF:93:26:F6:5F:9F:D3:15:06:52:4E
  SHA1: C4:18:F6:4D:46:D1:DF:00:3D:27:30:13:72:43:A9:12:11:C6:75:FB
  SHA256:
 49:35:1B:90:34:44:C1:85:CC:DC:5C:69:3D:24:D8:55:5C:B2:08:D6:A8:14:13:07:69:9F:4A:F0:63:19:9D:7

Alias name: camerfirmachambersca
Certificate fingerprints:
  MD5:  5E:80:9E:84:5A:0E:65:0B:17:02:F3:55:18:2A:3E:D7
  SHA1: 78:6A:74:AC:76:AB:14:7F:9C:6A:30:50:BA:9E:A8:7E:FE:9A:CE:3C
  SHA256:
 06:3E:4A:FA:C4:91:DF:D3:32:F3:08:9B:85:42:E9:46:17:D8:93:D7:FE:94:4E:10:A7:93:7E:E2:9D:96:93:C

Alias name: certsignrootca
Certificate fingerprints:
  MD5:  18:98:C0:D6:E9:3A:FC:F9:B0:F5:0C:F7:4B:01:44:17
  SHA1: FA:B7:EE:36:97:26:62:FB:2D:B0:2A:F6:BF:03:FD:E8:7C:4B:2F:9B
  SHA256:
 EA:A9:62:C4:FA:4A:6B:AF:EB:E4:15:19:6D:35:1C:CD:88:8D:4F:53:F3:FA:8A:E6:D7:C4:66:A9:4E:60:42:B

Alias name: verisignuniversalrootca
Certificate fingerprints:
  MD5:  8E:AD:B5:01:AA:4D:81:E4:8C:1D:D1:E1:14:00:95:19
  SHA1: 36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54
  SHA256:
 23:99:56:11:27:A5:71:25:DE:8C:EF:EA:61:0D:DF:2F:A0:78:B5:C8:06:7F:4E:82:82:90:BF:B8:60:E8:4B:3

Alias name: geotrustuniversalca
```

```
Certificate fingerprints:
  MD5:  92:65:58:8B:A2:1A:31:72:73:68:5C:B4:A5:7A:07:48
  SHA1: E6:21:F3:35:43:79:05:9A:4B:68:30:9D:8A:2F:74:22:15:87:EC:79
  SHA256:
 A0:45:9B:9F:63:B2:25:59:F5:FA:5D:4C:6D:B3:F9:F7:2F:F1:93:42:03:35:78:F0:73:BF:1D:1B:46:CB:B9:1



Alias name: luxtrustglobalroot2
Certificate fingerprints:
  MD5:  B2:E1:09:00:61:AF:F7:F1:91:6F:C4:AD:8D:5E:3B:7C
  SHA1: 1E:0E:56:19:0A:D1:8B:25:98:B2:04:44:FF:66:8A:04:17:99:5F:3F
  SHA256:
 54:45:5F:71:29:C2:0B:14:47:C4:18:F9:97:16:8F:24:C5:8F:C5:02:3B:F5:DA:5B:E2:EB:6E:1D:D8:90:2E:D



Alias name: twcaglobalrootca
Certificate fingerprints:
  MD5:  F9:03:7E:CF:E6:9E:3C:73:7A:2A:90:07:69:FF:2B:96
  SHA1: 9C:BB:48:53:F6:A4:F6:D3:52:A4:E8:32:52:55:60:13:F5:AD:AF:65
  SHA256:
 59:76:90:07:F7:68:5D:0F:CD:50:87:2F:9F:95:D5:75:5A:5B:2B:45:7D:81:F3:69:2B:61:0A:98:67:2F:0E:1

Alias name: tubitakkamusmsslkoksertifikasisurum1
Certificate fingerprints:
  MD5:  DC:00:81:DC:69:2F:3E:2F:B0:3B:F6:3D:5A:91:8E:49
  SHA1: 31:43:64:9B:EC:CE:27:EC:ED:3A:3F:0B:8F:0D:E4:E8:91:DD:EE:CA
  SHA256:
 46:ED:C3:68:90:46:D5:3A:45:3F:B3:10:4A:B8:0D:CA:EC:65:8B:26:60:EA:16:29:DD:7E:86:79:90:64:87:1

Alias name: affirmtrustnetworkingca
Certificate fingerprints:
  MD5:  42:65:CA:BE:01:9A:9A:4C:A9:8C:41:49:CD:C0:D5:7F
  SHA1: 29:36:21:02:8B:20:ED:02:F5:66:C5:32:D1:D6:ED:90:9F:45:00:2F
  SHA256:
 0A:81:EC:5A:92:97:77:F1:45:90:4A:F3:8D:5D:50:9F:66:B5:E2:C5:8F:CD:B5:31:05:8B:0E:17:F3:F0:B4:1

Alias name: affirmtrustcommercialca
Certificate fingerprints:
  MD5:  82:92:BA:5B:EF:CD:8A:6F:A6:3D:55:F9:84:F6:D6:B7
  SHA1: F9:B5:B6:32:45:5F:9C:BE:EC:57:5F:80:DC:E9:6E:2C:C7:B2:78:B7
  SHA256:
 03:76:AB:1D:54:C5:F9:80:3C:E4:B2:E2:01:A0:EE:7E:EF:7B:57:B6:36:E8:A9:3C:9B:8D:48:60:C9:6F:5F:A
```

```
Alias name: godaddyrootcertificateauthorityg2
Certificate fingerprints:
  MD5:  80:3A:BC:22:C1:E6:FB:8D:9B:3B:27:4A:32:1B:9A:01
  SHA1: 47:BE:AB:C9:22:EA:E8:0E:78:78:34:62:A7:9F:45:C2:54:FD:E6:8B
  SHA256:
 45:14:0B:32:47:EB:9C:C8:C5:B4:F0:D7:B5:30:91:F7:32:92:08:9E:6E:5A:63:E2:74:9D:D3:AC:A9:19:8E:D

Alias name: starfieldrootg2ca
Certificate fingerprints:
  MD5:  D6:39:81:C6:52:7E:96:69:FC:FC:CA:66:ED:05:F2:96
  SHA1: B5:1C:06:7C:EE:2B:0C:3D:F8:55:AB:2D:92:F4:FE:39:D4:E7:0F:0E
  SHA256:
 2C:E1:CB:0B:F9:D2:F9:E1:02:99:3F:BE:21:51:52:C3:B2:DD:0C:AB:DE:1C:68:E5:31:9B:83:91:54:DB:B7:F

Alias name: dtrustrootclass3ca2ev2009
Certificate fingerprints:
  MD5:  AA:C6:43:2C:5E:2D:CD:C4:34:C0:50:4F:11:02:4F:B6
  SHA1: 96:C9:1B:0B:95:B4:10:98:42:FA:D0:D8:22:79:FE:60:FA:B9:16:83
  SHA256:
 EE:C5:49:6B:98:8C:E9:86:25:B9:34:09:2E:EC:29:08:BE:D0:B0:F3:16:C2:D4:73:0C:84:EA:F1:F3:D3:48:8

Alias name: buypassclass3ca
Certificate fingerprints:
  MD5:  3D:3B:18:9E:2C:64:5A:E8:D5:88:CE:0E:F9:37:C2:EC
  SHA1: DA:FA:F7:FA:66:84:EC:06:8F:14:50:BD:C7:C2:81:A5:BC:A9:64:57
  SHA256:
 ED:F7:EB:BC:A2:7A:2A:38:4D:38:7B:7D:40:10:C6:66:E2:ED:B4:84:3E:4C:29:B4:AE:1D:5B:93:32:E6:B2:4

Alias name: verisignclass2g3ca
Certificate fingerprints:
  MD5:  F8:BE:C4:63:22:C9:A8:46:74:8B:B8:1D:1E:4A:2B:F6
  SHA1: 61:EF:43:D7:7F:CA:D4:61:51:BC:98:E0:C3:59:12:AF:9F:EB:63:11
  SHA256:
 92:A9:D9:83:3F:E1:94:4D:B3:66:E8:BF:AE:7A:95:B6:48:0C:2D:6C:6C:2A:1B:E6:5D:42:36:B6:08:FC:A1:B

Alias name: digicerttrustedrootg4
Certificate fingerprints:
  MD5:  78:F2:FC:AA:60:1F:2F:B4:EB:C9:37:BA:53:2E:75:49
  SHA1: DD:FB:16:CD:49:31:C9:73:A2:03:7D:3F:C8:3A:4D:7D:77:5D:05:E4
  SHA256:
 55:2F:7B:DC:F1:A7:AF:9E:6C:E6:72:01:7F:4F:12:AB:F7:72:40:C7:8E:76:1A:C2:03:D1:D9:D2:0A:C8:99:8

Alias name: quovadisrootca2g3
```

```
Certificate fingerprints:
  MD5:  AF:0C:86:6E:BF:40:2D:7F:0B:3E:12:50:BA:12:3D:06
  SHA1: 09:3C:61:F3:8B:8B:DC:7D:55:DF:75:38:02:05:00:E1:25:F5:C8:36
  SHA256:
 8F:E4:FB:0A:F9:3A:4D:0D:67:DB:0B:EB:B2:3E:37:C7:1B:F3:25:DC:BC:DD:24:0E:A0:4D:AF:58:B4:7E:18:4

Alias name: geotrustprimarycertificationauthorityg3
Certificate fingerprints:
  MD5:  B5:E8:34:36:C9:10:44:58:48:70:6D:2E:83:D4:B8:05
  SHA1: 03:9E:ED:B8:0B:E7:A0:3C:69:53:89:3B:20:D2:D9:32:3A:4C:2A:FD
  SHA256:
 B4:78:B8:12:25:0D:F8:78:63:5C:2A:A7:EC:7D:15:5E:AA:62:5E:E8:29:16:E2:CD:29:43:61:88:6C:D1:FB:D

Alias name: geotrustprimarycertificationauthorityg2
Certificate fingerprints:
  MD5:  01:5E:D8:6B:BD:6F:3D:8E:A1:31:F8:12:E0:98:73:6A
  SHA1: 8D:17:84:D5:37:F3:03:7D:EC:70:FE:57:8B:51:9A:99:E6:10:D7:B0
  SHA256:
 5E:DB:7A:C4:3B:82:A0:6A:87:61:E8:D7:BE:49:79:EB:F2:61:1F:7D:D7:9B:F9:1C:1C:6B:56:6A:21:9E:D7:6

Alias name: godaddyclass2ca
Certificate fingerprints:
  MD5:  91:DE:06:25:AB:DA:FD:32:17:0C:BB:25:17:2A:84:67
  SHA1: 27:96:BA:E6:3F:18:01:E2:77:26:1B:A0:D7:77:70:02:8F:20:EE:E4
  SHA256:
 C3:84:6B:F2:4B:9E:93:CA:64:27:4C:0E:C6:7C:1E:CC:5E:02:4F:FC:AC:D2:D7:40:19:35:0E:81:FE:54:6A:E

Alias name: trustcoreca1
Certificate fingerprints:
  MD5:  27:92:23:1D:0A:F5:40:7C:E9:E6:6B:9D:D8:F5:E7:6C
  SHA1: 58:D1:DF:95:95:67:6B:63:C0:F0:5B:1C:17:4D:8B:84:0B:C8:78:BD
  SHA256:
 5A:88:5D:B1:9C:01:D9:12:C5:75:93:88:93:8C:AF:BB:DF:03:1A:B2:D4:8E:91:EE:15:58:9B:42:97:1D:03:9

Alias name: hellenicacademicandresearchinstitutionseccrootca2015
Certificate fingerprints:
  MD5:  81:E5:B4:17:EB:C2:F5:E1:4B:0D:41:7B:49:92:FE:EF
  SHA1: 9F:F1:71:8D:92:D5:9A:F3:7D:74:97:B4:BC:6F:84:68:0B:BA:B6:66
  SHA256:
 44:B5:45:AA:8A:25:E6:5A:73:CA:15:DC:27:FC:36:D2:4C:1C:B9:95:3A:06:65:39:B1:15:82:DC:48:7B:48:3

Alias name: utnuserfirstobjectca
Certificate fingerprints:
  MD5:  A7:F2:E4:16:06:41:11:50:30:6B:9C:E3:B4:9C:B0:C9
```

```
  SHA1: E1:2D:FB:4B:41:D7:D9:C3:2B:30:51:4B:AC:1D:81:D8:38:5E:2D:46
  SHA256:
 6F:FF:78:E4:00:A7:0C:11:01:1C:D8:59:77:C4:59:FB:5A:F9:6A:3D:F0:54:08:20:D0:F4:B8:60:78:75:E5:8

Alias name: ttelesecglobalrootclass3
Certificate fingerprints:
  MD5:  CA:FB:40:A8:4E:39:92:8A:1D:FE:8E:2F:C4:27:EA:EF
  SHA1: 55:A6:72:3E:CB:F2:EC:CD:C3:23:74:70:19:9D:2A:BE:11:E3:81:D1
  SHA256:
 FD:73:DA:D3:1C:64:4F:F1:B4:3B:EF:0C:CD:DA:96:71:0B:9C:D9:87:5E:CA:7E:31:70:7A:F3:E9:6D:52:2B:B

Alias name: ttelesecglobalrootclass2
Certificate fingerprints:
  MD5:  2B:9B:9E:E4:7B:6C:1F:00:72:1A:CC:C1:77:79:DF:6A
  SHA1: 59:0D:2D:7D:88:4F:40:2E:61:7E:A5:62:32:17:65:CF:17:D8:94:E9
  SHA256:
 91:E2:F5:78:8D:58:10:EB:A7:BA:58:73:7D:E1:54:8A:8E:CA:CD:01:45:98:BC:0B:14:3E:04:1B:17:05:25:5

Alias name: addtrustclass1ca
Certificate fingerprints:
  MD5:  1E:42:95:02:33:92:6B:B9:5F:C0:7F:DA:D6:B2:4B:FC
  SHA1: CC:AB:0E:A0:4C:23:01:D6:69:7B:DD:37:9F:CD:12:EB:24:E3:94:9D
  SHA256:
 8C:72:09:27:9A:C0:4E:27:5E:16:D0:7F:D3:B7:75:E8:01:54:B5:96:80:46:E3:1F:52:DD:25:76:63:24:E9:A

Alias name: amzninternalrootca
Certificate fingerprints:
  MD5:  08:09:73:AC:E0:78:41:7C:0A:26:33:51:E8:CF:E6:60
  SHA1: A7:B7:F6:15:8A:FF:1E:C8:85:13:38:BC:93:EB:A2:AB:A4:09:EF:06
  SHA256:
 0E:DE:63:C1:DC:7A:8E:11:F1:AB:BC:05:4F:59:EE:49:9D:62:9A:2F:DE:9C:A7:16:32:A2:64:29:3E:8B:66:A

Alias name: starfieldrootcertificateauthorityg2
Certificate fingerprints:
  MD5:  D6:39:81:C6:52:7E:96:69:FC:FC:CA:66:ED:05:F2:96
  SHA1: B5:1C:06:7C:EE:2B:0C:3D:F8:55:AB:2D:92:F4:FE:39:D4:E7:0F:0E
  SHA256:
 2C:E1:CB:0B:F9:D2:F9:E1:02:99:3F:BE:21:51:52:C3:B2:DD:0C:AB:DE:1C:68:E5:31:9B:83:91:54:DB:B7:F

Alias name: camerfirmachambersignca
Certificate fingerprints:
  MD5:  9E:80:FF:78:01:0C:2E:C1:36:BD:FE:96:90:6E:08:F3
  SHA1: 4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C
```

```
  SHA256:
 13:63:35:43:93:34:A7:69:80:16:A0:D3:24:DE:72:28:4E:07:9D:7B:52:20:BB:8F:BD:74:78:16:EE:BE:BA:C

Alias name: secomscrootca2
Certificate fingerprints:
  MD5:  6C:39:7D:A4:0E:55:59:B2:3F:D6:41:B1:12:50:DE:43
  SHA1: 5F:3B:8C:F2:F8:10:B3:7D:78:B4:CE:EC:19:19:C3:73:34:B9:C7:74
  SHA256:
 51:3B:2C:EC:B8:10:D4:CD:E5:DD:85:39:1A:DF:C6:C2:DD:60:D8:7B:B7:36:D2:B5:21:48:4A:A4:7A:0E:BE:F

Alias name: entrustevca
Certificate fingerprints:
  MD5:  D6:A5:C3:ED:5D:DD:3E:00:C1:3D:87:92:1F:1D:3F:E4
  SHA1: B3:1E:B1:B7:40:E3:6C:84:02:DA:DC:37:D4:4D:F5:D4:67:49:52:F9
  SHA256:
 73:C1:76:43:4F:1B:C6:D5:AD:F4:5B:0E:76:E7:27:28:7C:8D:E5:76:16:C1:E6:E6:14:1A:2B:2C:BC:7D:8E:4

Alias name: secomscrootca1
Certificate fingerprints:
  MD5:  F1:BC:63:6A:54:E0:B5:27:F5:CD:E7:1A:E3:4D:6E:4A
  SHA1: 36:B1:2B:49:F9:81:9E:D7:4C:9E:BC:38:0F:C6:56:8F:5D:AC:B2:F7
  SHA256:
 E7:5E:72:ED:9F:56:0E:EC:6E:B4:80:00:73:A4:3F:C3:AD:19:19:5A:39:22:82:01:78:95:97:4A:99:02:6B:6

Alias name: affirmtrustcommercial
Certificate fingerprints:
  MD5:  82:92:BA:5B:EF:CD:8A:6F:A6:3D:55:F9:84:F6:D6:B7
  SHA1: F9:B5:B6:32:45:5F:9C:BE:EC:57:5F:80:DC:E9:6E:2C:C7:B2:78:B7
  SHA256:
 03:76:AB:1D:54:C5:F9:80:3C:E4:B2:E2:01:A0:EE:7E:EF:7B:57:B6:36:E8:A9:3C:9B:8D:48:60:C9:6F:5F:A

Alias name: digicertassuredidrootg3
Certificate fingerprints:
  MD5:  7C:7F:65:31:0C:81:DF:8D:BA:3E:99:E2:5C:AD:6E:FB
  SHA1: F5:17:A2:4F:9A:48:C6:C9:F8:A2:00:26:9F:DC:0F:48:2C:AB:30:89
  SHA256:
 7E:37:CB:8B:4C:47:09:0C:AB:36:55:1B:A6:F4:5D:B8:40:68:0F:BA:16:6A:95:2D:B1:00:71:7F:43:05:3F:C

Alias name: affirmtrustnetworking
Certificate fingerprints:
  MD5:  42:65:CA:BE:01:9A:9A:4C:A9:8C:41:49:CD:C0:D5:7F
  SHA1: 29:36:21:02:8B:20:ED:02:F5:66:C5:32:D1:D6:ED:90:9F:45:00:2F
  SHA256:
 0A:81:EC:5A:92:97:77:F1:45:90:4A:F3:8D:5D:50:9F:66:B5:E2:C5:8F:CD:B5:31:05:8B:0E:17:F3:F0:B4:1
```

```
Alias name: izenpecom
Certificate fingerprints:
  MD5:  A6:B0:CD:85:80:DA:5C:50:34:A3:39:90:2F:55:67:73
  SHA1: 2F:78:3D:25:52:18:A7:4A:65:39:71:B5:2C:A2:9C:45:15:6F:E9:19
  SHA256:
 25:30:CC:8E:98:32:15:02:BA:D9:6F:9B:1F:BA:1B:09:9E:2D:29:9E:0F:45:48:BB:91:4F:36:3B:C0:D4:53:1

Alias name: amazon-ca-g4-legacy
Certificate fingerprints:
  MD5:  6C:E5:BD:67:A4:4F:E3:FD:C2:4C:46:E6:06:5B:6D:55
  SHA1: EA:E7:DE:F9:0A:BE:9F:0B:68:CE:B7:24:0D:80:74:03:BF:6E:B1:6E
  SHA256:
 CD:72:C4:7F:B4:AD:28:A4:67:2B:E1:86:47:D4:40:E9:3B:16:2D:95:DB:3C:2F:94:BB:81:D9:09:F7:91:24:5

Alias name: digicertassuredidrootg2
Certificate fingerprints:
  MD5:  92:38:B9:F8:63:24:82:65:2C:57:33:E6:FE:81:8F:9D
  SHA1: A1:4B:48:D9:43:EE:0A:0E:40:90:4F:3C:E0:A4:C0:91:93:51:5D:3F
  SHA256:
 7D:05:EB:B6:82:33:9F:8C:94:51:EE:09:4E:EB:FE:FA:79:53:A1:14:ED:B2:F4:49:49:45:2F:AB:7D:2F:C1:8

Alias name: comodoaaaservicesroot
Certificate fingerprints:
  MD5:  49:79:04:B0:EB:87:19:AC:47:B0:BC:11:51:9B:74:D0
  SHA1: D1:EB:23:A4:6D:17:D6:8F:D9:25:64:C2:F1:F1:60:17:64:D8:E3:49
  SHA256:
 D7:A7:A0:FB:5D:7E:27:31:D7:71:E9:48:4E:BC:DE:F7:1D:5F:0C:3E:0A:29:48:78:2B:C8:3E:E0:EA:69:9E:F

Alias name: entrustnetpremium2048secureserverca
Certificate fingerprints:
  MD5:  EE:29:31:BC:32:7E:9A:E6:E8:B5:F7:51:B4:34:71:90
  SHA1: 50:30:06:09:1D:97:D4:F5:AE:39:F7:CB:E7:92:7D:7D:65:2D:34:31
  SHA256:
 6D:C4:71:72:E0:1C:BC:B0:BF:62:58:0D:89:5F:E2:B8:AC:9A:D4:F8:73:80:1E:0C:10:B9:C8:37:D2:1E:B1:7

Alias name: trustcorrootcertca2
Certificate fingerprints:
  MD5:  A2:E1:F8:18:0B:BA:45:D5:C7:41:2A:BB:37:52:45:64
  SHA1: B8:BE:6D:CB:56:F1:55:B9:63:D4:12:CA:4E:06:34:C7:94:B2:1C:C0
  SHA256:
 07:53:E9:40:37:8C:1B:D5:E3:83:6E:39:5D:AE:A5:CB:83:9E:50:46:F1:BD:0E:AE:19:51:CF:10:FE:C7:C9:6

Alias name: entrust2048ca
```

```
Certificate fingerprints:
  MD5:  EE:29:31:BC:32:7E:9A:E6:E8:B5:F7:51:B4:34:71:90
  SHA1: 50:30:06:09:1D:97:D4:F5:AE:39:F7:CB:E7:92:7D:7D:65:2D:34:31
  SHA256:
 6D:C4:71:72:E0:1C:BC:B0:BF:62:58:0D:89:5F:E2:B8:AC:9A:D4:F8:73:80:1E:0C:10:B9:C8:37:D2:1E:B1:7

Alias name: trustcorrootcertca1
Certificate fingerprints:
  MD5:  6E:85:F1:DC:1A:00:D3:22:D5:B2:B2:AC:6B:37:05:45
  SHA1: FF:BD:CD:E7:82:C8:43:5E:3C:6F:26:86:5C:CA:A8:3A:45:5B:C3:0A
  SHA256:
 D4:0E:9C:86:CD:8F:E4:68:C1:77:69:59:F4:9E:A7:74:FA:54:86:84:B6:C4:06:F3:90:92:61:F4:DC:E2:57:5

Alias name: baltimorecybertrustroot
Certificate fingerprints:
  MD5:  AC:B6:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:E4
  SHA1: D4:DE:20:D0:5E:66:FC:53:FE:1A:50:88:2C:78:DB:28:52:CA:E4:74
  SHA256:
 16:AF:57:A9:F6:76:B0:AB:12:60:95:AA:5E:BA:DE:F2:2A:B3:11:19:D6:44:AC:95:CD:4B:93:DB:F3:F2:6A:E

Alias name: eecertificationcentrerootca
Certificate fingerprints:
  MD5:  43:5E:88:D4:7D:1A:4A:7E:FD:84:2E:52:EB:01:D4:6F
  SHA1: C9:A8:B9:E7:55:80:5E:58:E3:53:77:A7:25:EB:AF:C3:7B:27:CC:D7
  SHA256:
 3E:84:BA:43:42:90:85:16:E7:75:73:C0:99:2F:09:79:CA:08:4E:46:85:68:1F:F1:95:CC:BA:8A:22:9B:8A:7

Alias name: dstacescax6
Certificate fingerprints:
  MD5:  21:D8:4C:82:2B:99:09:33:A2:EB:14:24:8D:8E:5F:E8
  SHA1: 40:54:DA:6F:1C:3F:40:74:AC:ED:0F:EC:CD:DB:79:D1:53:FB:90:1D
  SHA256:
 76:7C:95:5A:76:41:2C:89:AF:68:8E:90:A1:C7:0F:55:6C:FD:6B:60:25:DB:EA:10:41:6D:7E:B6:83:1F:8C:4

Alias name: comodocertificationauthority
Certificate fingerprints:
  MD5:  5C:48:DC:F7:42:72:EC:56:94:6D:1C:CC:71:35:80:75
  SHA1: 66:31:BF:9E:F7:4F:9E:B6:C9:D5:A6:0C:BA:6A:BE:D1:F7:BD:EF:7B
  SHA256:
 0C:2C:D6:3D:F7:80:6F:A3:99:ED:E8:09:11:6B:57:5B:F8:79:89:F0:65:18:F9:80:8C:86:05:03:17:8B:AF:6

Alias name: thawteserverca
Certificate fingerprints:
  MD5:  EE:FE:61:69:65:6E:F8:9C:C6:2A:F4:D7:2B:63:EF:A2
```

```
  SHA1: 9F:AD:91:A6:CE:6A:C6:C5:00:47:C4:4E:C9:D4:A5:0D:92:D8:49:79
  SHA256:
 87:C6:78:BF:B8:B2:5F:38:F7:E9:7B:33:69:56:BB:CF:14:4B:BA:CA:A5:36:47:E6:1A:23:25:BC:10:55:31:6

Alias name: secomvalicertclass1ca
Certificate fingerprints:
  MD5:  65:58:AB:15:AD:57:6C:1E:A8:A7:B5:69:AC:BF:FF:EB
  SHA1: E5:DF:74:3C:B6:01:C4:9B:98:43:DC:AB:8C:E8:6A:81:10:9F:E4:8E
  SHA256:
 F4:C1:49:55:1A:30:13:A3:5B:C7:BF:FE:17:A7:F3:44:9B:C1:AB:5B:5A:0A:E7:4B:06:C2:3B:90:00:4C:01:0

Alias name: godaddyrootg2ca
Certificate fingerprints:
  MD5:  80:3A:BC:22:C1:E6:FB:8D:9B:3B:27:4A:32:1B:9A:01
  SHA1: 47:BE:AB:C9:22:EA:E8:0E:78:78:34:62:A7:9F:45:C2:54:FD:E6:8B
  SHA256:
 45:14:0B:32:47:EB:9C:C8:C5:B4:F0:D7:B5:30:91:F7:32:92:08:9E:6E:5A:63:E2:74:9D:D3:AC:A9:19:8E:D

Alias name: globalchambersignroot2008
Certificate fingerprints:
  MD5:  9E:80:FF:78:01:0C:2E:C1:36:BD:FE:96:90:6E:08:F3
  SHA1: 4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C
  SHA256:
 13:63:35:43:93:34:A7:69:80:16:A0:D3:24:DE:72:28:4E:07:9D:7B:52:20:BB:8F:BD:74:78:16:EE:BE:BA:C

Alias name: equifaxsecureebusinessca1
Certificate fingerprints:
  MD5:  14:C0:08:E5:A3:85:03:A3:BE:78:E9:67:4F:27:CA:EE
  SHA1: AE:E6:3D:70:E3:76:FB:C7:3A:EB:B0:A1:C1:D4:C4:7A:A7:40:B3:F4
  SHA256:
 2E:3A:2B:B5:11:25:05:83:6C:A8:96:8B:E2:CB:37:27:CE:9B:56:84:5C:6E:E9:8E:91:85:10:4A:FB:9A:F5:9

Alias name: quovadisrootca3
Certificate fingerprints:
  MD5:  31:85:3C:62:94:97:63:B9:AA:FD:89:4E:AF:6F:E0:CF
  SHA1: 1F:49:14:F7:D8:74:95:1D:DD:AE:02:C0:BE:FD:3A:2D:82:75:51:85
  SHA256:
 18:F1:FC:7F:20:5D:F8:AD:DD:EB:7F:E0:07:DD:57:E3:AF:37:5A:9C:4D:8D:73:54:6B:F4:F1:FE:D1:E1:8D:3

Alias name: usertrustecccertificationauthority
Certificate fingerprints:
  MD5:  FA:68:BC:D9:B5:7F:AD:FD:C9:1D:06:83:28:CC:24:C1
  SHA1: D1:CB:CA:5D:B2:D5:2A:7F:69:3B:67:4D:E5:F0:5A:1D:0C:95:7D:F0
```

```
  SHA256:
 4F:F4:60:D5:4B:9C:86:DA:BF:BC:FC:57:12:E0:40:0D:2B:ED:3F:BC:4D:4F:BD:AA:86:E0:6A:DC:D2:A9:AD:7

Alias name: quovadisrootca2
Certificate fingerprints:
  MD5:  5E:39:7B:DD:F8:BA:EC:82:E9:AC:62:BA:0C:54:00:2B
  SHA1: CA:3A:FB:CF:12:40:36:4B:44:B2:16:20:88:80:48:39:19:93:7C:F7
  SHA256:
 85:A0:DD:7D:D7:20:AD:B7:FF:05:F8:3D:54:2B:20:9D:C7:FF:45:28:F7:D6:77:B1:83:89:FE:A5:E5:C4:9E:8

Alias name: soneraclass2ca
Certificate fingerprints:
  MD5:  A3:EC:75:0F:2E:88:DF:FA:48:01:4E:0B:5C:48:6F:FB
  SHA1: 37:F7:6D:E6:07:7C:90:C5:B1:3E:93:1A:B7:41:10:B4:F2:E4:9A:27
  SHA256:
 79:08:B4:03:14:C1:38:10:0B:51:8D:07:35:80:7F:FB:FC:F8:51:8A:00:95:33:71:05:BA:38:6B:15:3D:D9:2

Alias name: twcarootcertificationauthority
Certificate fingerprints:
  MD5:  AA:08:8F:F6:F9:7B:B7:F2:B1:A7:1E:9B:EA:EA:BD:79
  SHA1: CF:9E:87:6D:D3:EB:FC:42:26:97:A3:B5:A3:7A:A0:76:A9:06:23:48
  SHA256:
 BF:D8:8F:E1:10:1C:41:AE:3E:80:1B:F8:BE:56:35:0E:E9:BA:D1:A6:B9:BD:51:5E:DC:5C:6D:5B:87:11:AC:4

Alias name: baltimorecybertrustca
Certificate fingerprints:
  MD5:  AC:B6:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:E4
  SHA1: D4:DE:20:D0:5E:66:FC:53:FE:1A:50:88:2C:78:DB:28:52:CA:E4:74
  SHA256:
 16:AF:57:A9:F6:76:B0:AB:12:60:95:AA:5E:BA:DE:F2:2A:B3:11:19:D6:44:AC:95:CD:4B:93:DB:F3:F2:6A:E

Alias name: cia-crt-g3-01-ca
Certificate fingerprints:
  MD5:  E3:66:DD:D6:A0:D5:40:8F:FF:29:E2:C0:CB:6E:62:1A
  SHA1: 2B:EE:2C:BA:A3:1D:B5:FE:60:40:41:95:08:ED:46:82:39:4D:ED:E2
  SHA256:
 20:48:AD:4C:EC:90:7F:FA:4A:15:D4:CE:45:E3:C8:E4:2C:EA:78:33:DC:C7:D3:40:48:FC:60:47:27:42:99:E

Alias name: entrustrootcertificationauthorityg2
Certificate fingerprints:
  MD5:  4B:E2:C9:91:96:65:0C:F4:0E:5A:93:92:A0:0A:FE:B2
  SHA1: 8C:F4:27:FD:79:0C:3A:D1:66:06:8D:E8:1E:57:EF:BB:93:22:72:D4
  SHA256:
 43:DF:57:74:B0:3E:7F:EF:5F:E4:0D:93:1A:7B:ED:F1:BB:2E:6B:42:73:8C:4E:6D:38:41:10:3D:3A:A7:F3:3
```

```
Alias name: verisignclass3g4ca
Certificate fingerprints:
  MD5:  3A:52:E1:E7:FD:6F:3A:E3:6F:F3:6F:99:1B:F9:22:41
  SHA1: 22:D5:D8:DF:8F:02:31:D1:8D:F7:9D:B7:CF:8A:2D:64:C9:3F:6C:3A
  SHA256:
 69:DD:D7:EA:90:BB:57:C9:3E:13:5D:C8:5E:A6:FC:D5:48:0B:60:32:39:BD:C4:54:FC:75:8B:2A:26:CF:7F:7

Alias name: xrampglobalcaroot
Certificate fingerprints:
  MD5:  A1:0B:44:B3:CA:10:D8:00:6E:9D:0F:D8:0F:92:0A:D1
  SHA1: B8:01:86:D1:EB:9C:86:A5:41:04:CF:30:54:F3:4C:52:B7:E5:58:C6
  SHA256:
 CE:CD:DC:90:50:99:D8:DA:DF:C5:B1:D2:09:B7:37:CB:E2:C1:8C:FB:2C:10:C0:FF:0B:CF:0D:32:86:FC:1A:A

Alias name: identrustcommercialrootca1
Certificate fingerprints:
  MD5:  B3:3E:77:73:75:EE:A0:D3:E3:7E:49:63:49:59:BB:C7
  SHA1: DF:71:7E:AA:4A:D9:4E:C9:55:84:99:60:2D:48:DE:5F:BC:F0:3A:25
  SHA256:
 5D:56:49:9B:E4:D2:E0:8B:CF:CA:D0:8A:3E:38:72:3D:50:50:3B:DE:70:69:48:E4:2F:55:60:30:19:E5:28:A

Alias name: camerfirmachamberscommerceca
Certificate fingerprints:
  MD5:  B0:01:EE:14:D9:AF:29:18:94:76:8E:F1:69:33:2A:84
  SHA1: 6E:3A:55:A4:19:0C:19:5C:93:84:3C:C0:DB:72:2E:31:30:61:F0:B1
  SHA256:
 0C:25:8A:12:A5:67:4A:EF:25:F2:8B:A7:DC:FA:EC:EE:A3:48:E5:41:E6:F5:CC:4E:E6:3B:71:B3:61:60:6A:C

Alias name: verisignclass3g2ca
Certificate fingerprints:
  MD5:  A2:33:9B:4C:74:78:73:D4:6C:E7:C1:F3:8D:CB:5C:E9
  SHA1: 85:37:1C:A6:E5:50:14:3D:CE:28:03:47:1B:DE:3A:09:E8:F8:77:0F
  SHA256:
 83:CE:3C:12:29:68:8A:59:3D:48:5F:81:97:3C:0F:91:95:43:1E:DA:37:CC:5E:36:43:0E:79:C7:A8:88:63:8

Alias name: deutschetelekomrootca2
Certificate fingerprints:
  MD5:  74:01:4A:91:B1:08:C4:58:CE:47:CD:F0:DD:11:53:08
  SHA1: 85:A4:08:C0:9C:19:3E:5D:51:58:7D:CD:D6:13:30:FD:8C:DE:37:BF
  SHA256:
 B6:19:1A:50:D0:C3:97:7F:7D:A9:9B:CD:AA:C8:6A:22:7D:AE:B9:67:9E:C7:0B:A3:B0:C9:D9:22:71:C1:70:D

Alias name: certumca
```

```
Certificate fingerprints:
  MD5:  2C:8F:9F:66:1D:18:90:B1:47:26:9D:8E:86:82:8C:A9
  SHA1: 62:52:DC:40:F7:11:43:A2:2F:DE:9E:F7:34:8E:06:42:51:B1:81:18
  SHA256:
 D8:E0:FE:BC:1D:B2:E3:8D:00:94:0F:37:D2:7D:41:34:4D:99:3E:73:4B:99:D5:65:6D:97:78:D4:D8:14:36:2

Alias name: cybertrustglobalroot
Certificate fingerprints:
  MD5:  72:E4:4A:87:E3:69:40:80:77:EA:BC:E3:F4:FF:F0:E1
  SHA1: 5F:43:E5:B1:BF:F8:78:8C:AC:1C:C7:CA:4A:9A:C6:22:2B:CC:34:C6
  SHA256:
 96:0A:DF:00:63:E9:63:56:75:0C:29:65:DD:0A:08:67:DA:0B:9C:BD:6E:77:71:4A:EA:FB:23:49:AB:39:3D:A

Alias name: globalsignrootca
Certificate fingerprints:
  MD5:  3E:45:52:15:09:51:92:E1:B7:5D:37:9F:B1:87:29:8A
  SHA1: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C
  SHA256:
 EB:D4:10:40:E4:BB:3E:C7:42:C9:E3:81:D3:1E:F2:A4:1A:48:B6:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:9

Alias name: secomevrootca1
Certificate fingerprints:
  MD5:  22:2D:A6:01:EA:7C:0A:F7:F0:6C:56:43:3F:77:76:D3
  SHA1: FE:B8:C4:32:DC:F9:76:9A:CE:AE:3D:D8:90:8F:FD:28:86:65:64:7D
  SHA256:
 A2:2D:BA:68:1E:97:37:6E:2D:39:7D:72:8A:AE:3A:9B:62:96:B9:FD:BA:60:BC:2E:11:F6:47:F2:C6:75:FB:3

Alias name: globalsignr3ca
Certificate fingerprints:
  MD5:  C5:DF:B8:49:CA:05:13:55:EE:2D:BA:1A:C3:3E:B0:28
  SHA1: D6:9B:56:11:48:F0:1C:77:C5:45:78:C1:09:26:DF:5B:85:69:76:AD
  SHA256:
 CB:B5:22:D7:B7:F1:27:AD:6A:01:13:86:5B:DF:1C:D4:10:2E:7D:07:59:AF:63:5A:7C:F4:72:0D:C9:63:C5:3

Alias name: staatdernederlandenrootcag3
Certificate fingerprints:
  MD5:  0B:46:67:07:DB:10:2F:19:8C:35:50:60:D1:0B:F4:37
  SHA1: D8:EB:6B:41:51:92:59:E0:F3:E7:85:00:C0:3D:B6:88:97:C9:EE:FC
  SHA256:
 3C:4F:B0:B9:5A:B8:B3:00:32:F4:32:B8:6F:53:5F:E1:72:C1:85:D0:FD:39:86:58:37:CF:36:18:7F:A6:F4:2

Alias name: staatdernederlandenrootcag2
Certificate fingerprints:
  MD5:  7C:A5:0F:F8:5B:9A:7D:6D:30:AE:54:5A:E3:42:A2:8A
```

```
  SHA1: 59:AF:82:79:91:86:C7:B4:75:07:CB:CF:03:57:46:EB:04:DD:B7:16
  SHA256:
 66:8C:83:94:7D:A6:3B:72:4B:EC:E1:74:3C:31:A0:E6:AE:D0:DB:8E:C5:B3:1B:E3:77:BB:78:4F:91:B6:71:6

Alias name: aolrootca2
Certificate fingerprints:
  MD5:  D6:ED:3C:CA:E2:66:0F:AF:10:43:0D:77:9B:04:09:BF
  SHA1: 85:B5:FF:67:9B:0C:79:96:1F:C8:6E:44:22:00:46:13:DB:17:92:84
  SHA256:
 7D:3B:46:5A:60:14:E5:26:C0:AF:FC:EE:21:27:D2:31:17:27:AD:81:1C:26:84:2D:00:6A:F3:73:06:CC:80:B

Alias name: dstrootcax3
Certificate fingerprints:
  MD5:  41:03:52:DC:0F:F7:50:1B:16:F0:02:8E:BA:6F:45:C5
  SHA1: DA:C9:02:4F:54:D8:F6:DF:94:93:5F:B1:73:26:38:CA:6A:D7:7C:13
  SHA256:
 06:87:26:03:31:A7:24:03:D9:09:F1:05:E6:9B:CF:0D:32:E1:BD:24:93:FF:C6:D9:20:6D:11:BC:D6:77:07:3

Alias name: trustcenteruniversalcai
Certificate fingerprints:
  MD5:  45:E1:A5:72:C5:A9:36:64:40:9E:F5:E4:58:84:67:8C
  SHA1: 6B:2F:34:AD:89:58:BE:62:FD:B0:6B:5C:CE:BB:9D:D9:4F:4E:39:F3
  SHA256:
 EB:F3:C0:2A:87:89:B1:FB:7D:51:19:95:D6:63:B7:29:06:D9:13:CE:0D:5E:10:56:8A:8A:77:E2:58:61:67:E

Alias name: aolrootca1
Certificate fingerprints:
  MD5:  14:F1:08:AD:9D:FA:64:E2:89:E7:1C:CF:A8:AD:7D:5E
  SHA1: 39:21:C1:15:C1:5D:0E:CA:5C:CB:5B:C4:F0:7D:21:D8:05:0B:56:6A
  SHA256:
 77:40:73:12:C6:3A:15:3D:5B:C0:0B:4E:51:75:9C:DF:DA:C2:37:DC:2A:33:B6:79:46:E9:8E:9B:FA:68:0A:E

Alias name: affirmtrustpremiumecc
Certificate fingerprints:
  MD5:  64:B0:09:55:CF:B1:D5:99:E2:BE:13:AB:A6:5D:EA:4D
  SHA1: B8:23:6B:00:2F:1D:16:86:53:01:55:6C:11:A4:37:CA:EB:FF:C3:BB
  SHA256:
 BD:71:FD:F6:DA:97:E4:CF:62:D1:64:7A:DD:25:81:B0:7D:79:AD:F8:39:7E:B4:EC:BA:9C:5E:84:88:82:14:2

Alias name: microseceszignorootca2009
Certificate fingerprints:
  MD5:  F8:49:F4:03:BC:44:2D:83:BE:48:69:7D:29:64:FC:B1
  SHA1: 89:DF:74:FE:5C:F4:0F:4A:80:F9:E3:37:7D:54:DA:91:E1:01:31:8E
```

```
  SHA256:
 3C:5F:81:FE:A5:FA:B8:2C:64:BF:A2:EA:EC:AF:CD:E8:E0:77:FC:86:20:A7:CA:E5:37:16:3D:F3:6E:DB:F3:7

Alias name: verisignclass1g3ca
Certificate fingerprints:
  MD5:  B1:47:BC:18:57:D1:18:A0:78:2D:EC:71:E8:2A:95:73
  SHA1: 20:42:85:DC:F7:EB:76:41:95:57:8E:13:6B:D4:B7:D1:E9:8E:46:A5
  SHA256:
 CB:B5:AF:18:5E:94:2A:24:02:F9:EA:CB:C0:ED:5B:B8:76:EE:A3:C1:22:36:23:D0:04:47:E4:F3:BA:55:4B:6

Alias name: certplusrootcag2
Certificate fingerprints:
  MD5:  A7:EE:C4:78:2D:1B:EE:2D:B9:29:CE:D6:A7:96:32:31
  SHA1: 4F:65:8E:1F:E9:06:D8:28:02:E9:54:47:41:C9:54:25:5D:69:CC:1A
  SHA256:
 6C:C0:50:41:E6:44:5E:74:69:6C:4C:FB:C9:F8:0F:54:3B:7E:AB:BB:44:B4:CE:6F:78:7C:6A:99:71:C4:2F:1

Alias name: certplusrootcag1
Certificate fingerprints:
  MD5:  7F:09:9C:F7:D9:B9:5C:69:69:56:D5:37:3E:14:0D:42
  SHA1: 22:FD:D0:B7:FD:A2:4E:0D:AC:49:2C:A0:AC:A6:7B:6A:1F:E3:F7:66
  SHA256:
 15:2A:40:2B:FC:DF:2C:D5:48:05:4D:22:75:B3:9C:7F:CA:3E:C0:97:80:78:B0:F0:EA:76:E5:61:A6:C7:43:3

Alias name: addtrustexternalca
Certificate fingerprints:
  MD5:  1D:35:54:04:85:78:B0:3F:42:42:4D:BF:20:73:0A:3F
  SHA1: 02:FA:F3:E2:91:43:54:68:60:78:57:69:4D:F5:E4:5B:68:85:18:68
  SHA256:
 68:7F:A4:51:38:22:78:FF:F0:C8:B1:1F:8D:43:D5:76:67:1C:6E:B2:BC:EA:B4:13:FB:83:D9:65:D0:6D:2F:F

Alias name: entrustrootcertificationauthority
Certificate fingerprints:
  MD5:  D6:A5:C3:ED:5D:DD:3E:00:C1:3D:87:92:1F:1D:3F:E4
  SHA1: B3:1E:B1:B7:40:E3:6C:84:02:DA:DC:37:D4:4D:F5:D4:67:49:52:F9
  SHA256:
 73:C1:76:43:4F:1B:C6:D5:AD:F4:5B:0E:76:E7:27:28:7C:8D:E5:76:16:C1:E6:E6:14:1A:2B:2C:BC:7D:8E:4

Alias name: verisignclass3ca
Certificate fingerprints:
  MD5:  EF:5A:F1:33:EF:F1:CD:BB:51:02:EE:12:14:4B:96:C4
  SHA1: A1:DB:63:93:91:6F:17:E4:18:55:09:40:04:15:C7:02:40:B0:AE:6B
  SHA256:
 A4:B6:B3:99:6F:C2:F3:06:B3:FD:86:81:BD:63:41:3D:8C:50:09:CC:4F:A3:29:C2:CC:F0:E2:FA:1B:14:03:0
```

```
Alias name: digicertassuredidrootca
Certificate fingerprints:
  MD5:  87:CE:0B:7B:2A:0E:49:00:E1:58:71:9B:37:A8:93:72
  SHA1: 05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43
  SHA256:
 3E:90:99:B5:01:5E:8F:48:6C:00:BC:EA:9D:11:1E:E7:21:FA:BA:35:5A:89:BC:F1:DF:69:56:1E:3D:C6:32:5

Alias name: globalsignrootcar3
Certificate fingerprints:
  MD5:  C5:DF:B8:49:CA:05:13:55:EE:2D:BA:1A:C3:3E:B0:28
  SHA1: D6:9B:56:11:48:F0:1C:77:C5:45:78:C1:09:26:DF:5B:85:69:76:AD
  SHA256:
 CB:B5:22:D7:B7:F1:27:AD:6A:01:13:86:5B:DF:1C:D4:10:2E:7D:07:59:AF:63:5A:7C:F4:72:0D:C9:63:C5:3

Alias name: globalsignrootcar2
Certificate fingerprints:
  MD5:  94:14:77:7E:3E:5E:FD:8F:30:BD:41:B0:CF:E7:D0:30
  SHA1: 75:E0:AB:B6:13:85:12:27:1C:04:F8:5F:DD:DE:38:E4:B7:24:2E:FE
  SHA256:
 CA:42:DD:41:74:5F:D0:B8:1E:B9:02:36:2C:F9:D8:BF:71:9D:A1:BD:1B:1E:FC:94:6F:5B:4C:99:F4:2C:1B:9

Alias name: verisignclass1ca
Certificate fingerprints:
  MD5:  86:AC:DE:2B:C5:6D:C3:D9:8C:28:88:D3:8D:16:13:1E
  SHA1: CE:6A:64:A3:09:E4:2F:BB:D9:85:1C:45:3E:64:09:EA:E8:7D:60:F1
  SHA256:
 51:84:7C:8C:BD:2E:9A:72:C9:1E:29:2D:2A:E2:47:D7:DE:1E:3F:D2:70:54:7A:20:EF:7D:61:0F:38:B8:84:2

Alias name: thawtepremiumserverca
Certificate fingerprints:
  MD5:  A6:6B:60:90:23:9B:3F:2D:BB:98:6F:D6:A7:19:0D:46
  SHA1: E0:AB:05:94:20:72:54:93:05:60:62:02:36:70:F7:CD:2E:FC:66:66
  SHA256:
 3F:9F:27:D5:83:20:4B:9E:09:C8:A3:D2:06:6C:4B:57:D3:A2:47:9C:36:93:65:08:80:50:56:98:10:5D:BC:E

Alias name: verisigntsaca
Certificate fingerprints:
  MD5:  F2:89:95:6E:4D:05:F0:F1:A7:21:55:7D:46:11:BA:47
  SHA1: 20:CE:B1:F0:F5:1C:0E:19:A9:F3:8D:B1:AA:8E:03:8C:AA:7A:C7:01
  SHA256:
 CB:6B:05:D9:E8:E5:7C:D8:82:B1:0B:4D:B7:0D:E4:BB:1D:E4:2B:A4:8A:7B:D0:31:8B:63:5B:F6:E7:78:1A:9

Alias name: thawteprimaryrootca
```

```
Certificate fingerprints:
  MD5:  8C:CA:DC:0B:22:CE:F5:BE:72:AC:41:1A:11:A8:D8:12
  SHA1: 91:C6:D6:EE:3E:8A:C8:63:84:E5:48:C2:99:29:5C:75:6C:81:7B:81
  SHA256:
 8D:72:2F:81:A9:C1:13:C0:79:1D:F1:36:A2:96:6D:B2:6C:95:0A:97:1D:B4:6B:41:99:F4:EA:54:B7:8B:FB:9

Alias name: visaecommerceroot
Certificate fingerprints:
  MD5:  FC:11:B8:D8:08:93:30:00:6D:23:F9:7E:EB:52:1E:02
  SHA1: 70:17:9B:86:8C:00:A4:FA:60:91:52:22:3F:9F:3E:32:BD:E0:05:62
  SHA256:
 69:FA:C9:BD:55:FB:0A:C7:8D:53:BB:EE:5C:F1:D5:97:98:9F:D0:AA:AB:20:A2:51:51:BD:F1:73:3E:E7:D1:2

Alias name: digicertglobalrootg3
Certificate fingerprints:
  MD5:  F5:5D:A4:50:A5:FB:28:7E:1E:0F:0D:CC:96:57:56:CA
  SHA1: 7E:04:DE:89:6A:3E:66:6D:00:E6:87:D3:3F:FA:D9:3B:E8:3D:34:9E
  SHA256:
 31:AD:66:48:F8:10:41:38:C7:38:F3:9E:A4:32:01:33:39:3E:3A:18:CC:02:29:6E:F9:7C:2A:C9:EF:67:31:D

Alias name: xrampglobalca
Certificate fingerprints:
  MD5:  A1:0B:44:B3:CA:10:D8:00:6E:9D:0F:D8:0F:92:0A:D1
  SHA1: B8:01:86:D1:EB:9C:86:A5:41:04:CF:30:54:F3:4C:52:B7:E5:58:C6
  SHA256:
 CE:CD:DC:90:50:99:D8:DA:DF:C5:B1:D2:09:B7:37:CB:E2:C1:8C:FB:2C:10:C0:FF:0B:CF:0D:32:86:FC:1A:A

Alias name: digicertglobalrootg2
Certificate fingerprints:
  MD5:  E4:A6:8A:C8:54:AC:52:42:46:0A:FD:72:48:1B:2A:44
  SHA1: DF:3C:24:F9:BF:D6:66:76:1B:26:80:73:FE:06:D1:CC:8D:4F:82:A4
  SHA256:
 CB:3C:CB:B7:60:31:E5:E0:13:8F:8D:D3:9A:23:F9:DE:47:FF:C3:5E:43:C1:14:4C:EA:27:D4:6A:5A:B1:CB:5

Alias name: valicertclass2ca
Certificate fingerprints:
  MD5:  A9:23:75:9B:BA:49:36:6E:31:C2:DB:F2:E7:66:BA:87
  SHA1: 31:7A:2A:D0:7F:2B:33:5E:F5:A1:C3:4E:4B:57:E8:B7:D8:F1:FC:A6
  SHA256:
 58:D0:17:27:9C:D4:DC:63:AB:DD:B1:96:A6:C9:90:6C:30:C4:E0:87:83:EA:E8:C1:60:99:54:D6:93:55:59:6

Alias name: geotrustprimaryca
Certificate fingerprints:
  MD5:  02:26:C3:01:5E:08:30:37:43:A9:D0:7D:CF:37:E6:BF
```

```
  SHA1: 32:3C:11:8E:1B:F7:B8:B6:52:54:E2:E2:10:0D:D6:02:90:37:F0:96
  SHA256:
 37:D5:10:06:C5:12:EA:AB:62:64:21:F1:EC:8C:92:01:3F:C5:F8:2A:E9:8E:E5:33:EB:46:19:B8:DE:B4:D0:6

Alias name: netlockaranyclassgoldfotanusitvany
Certificate fingerprints:
  MD5:  C5:A1:B7:FF:73:DD:D6:D7:34:32:18:DF:FC:3C:AD:88
  SHA1: 06:08:3F:59:3F:15:A1:04:A0:69:A4:6B:A9:03:D0:06:B7:97:09:91
  SHA256:
 6C:61:DA:C3:A2:DE:F0:31:50:6B:E0:36:D2:A6:FE:40:19:94:FB:D1:3D:F9:C8:D4:66:59:92:74:C4:46:EC:9

Alias name: geotrustglobalca
Certificate fingerprints:
  MD5:  F7:75:AB:29:FB:51:4E:B7:77:5E:FF:05:3C:99:8E:F5
  SHA1: DE:28:F4:A4:FF:E5:B9:2F:A3:C5:03:D1:A3:49:A7:F9:96:2A:82:12
  SHA256:
 FF:85:6A:2D:25:1D:CD:88:D3:66:56:F4:50:12:67:98:CF:AB:AA:DE:40:79:9C:72:2D:E4:D2:B5:DB:36:A7:3

Alias name: oistewisekeyglobalrootgbca
Certificate fingerprints:
  MD5:  A4:EB:B9:61:28:2E:B7:2F:98:B0:35:26:90:99:51:1D
  SHA1: 0F:F9:40:76:18:D3:D7:6A:4B:98:F0:A8:35:9E:0C:FD:27:AC:CC:ED
  SHA256:
 6B:9C:08:E8:6E:B0:F7:67:CF:AD:65:CD:98:B6:21:49:E5:49:4A:67:F5:84:5E:7B:D1:ED:01:9F:27:B8:6B:D

Alias name: certumtrustednetworkca2
Certificate fingerprints:
  MD5:  6D:46:9E:D9:25:6D:08:23:5B:5E:74:7D:1E:27:DB:F2
  SHA1: D3:DD:48:3E:2B:BF:4C:05:E8:AF:10:F5:FA:76:26:CF:D3:DC:30:92
  SHA256:
 B6:76:F2:ED:DA:E8:77:5C:D3:6C:B0:F6:3C:D1:D4:60:39:61:F4:9E:62:65:BA:01:3A:2F:03:07:B6:D0:B8:0

Alias name: starfieldservicesrootcertificateauthorityg2
Certificate fingerprints:
  MD5:  17:35:74:AF:7B:61:1C:EB:F4:F9:3C:E2:EE:40:F9:A2
  SHA1: 92:5A:8F:8D:2C:6D:04:E0:66:5F:59:6A:FF:22:D8:63:E8:25:6F:3F
  SHA256:
 56:8D:69:05:A2:C8:87:08:A4:B3:02:51:90:ED:CF:ED:B1:97:4A:60:6A:13:C6:E5:29:0F:CB:2A:E6:3E:DA:B

Alias name: comodorsacertificationauthority
Certificate fingerprints:
  MD5:  1B:31:B0:71:40:36:CC:14:36:91:AD:C4:3E:FD:EC:18
  SHA1: AF:E5:D2:44:A8:D1:19:42:30:FF:47:9F:E2:F8:97:BB:CD:7A:8C:B4
```

```
  SHA256:
 52:F0:E1:C4:E5:8E:C6:29:29:1B:60:31:7F:07:46:71:B8:5D:7E:A8:0D:5B:07:27:34:63:53:4B:32:B4:02:3

Alias name: comodoaaaca
Certificate fingerprints:
  MD5:  49:79:04:B0:EB:87:19:AC:47:B0:BC:11:51:9B:74:D0
  SHA1: D1:EB:23:A4:6D:17:D6:8F:D9:25:64:C2:F1:F1:60:17:64:D8:E3:49
  SHA256:
 D7:A7:A0:FB:5D:7E:27:31:D7:71:E9:48:4E:BC:DE:F7:1D:5F:0C:3E:0A:29:48:78:2B:C8:3E:E0:EA:69:9E:F

Alias name: identrustpublicsectorrootca1
Certificate fingerprints:
  MD5:  37:06:A5:B0:FC:89:9D:BA:F4:6B:8C:1A:64:CD:D5:BA
  SHA1: BA:29:41:60:77:98:3F:F4:F3:EF:F2:31:05:3B:2E:EA:6D:4D:45:FD
  SHA256:
 30:D0:89:5A:9A:44:8A:26:20:91:63:55:22:D1:F5:20:10:B5:86:7A:CA:E1:2C:78:EF:95:8F:D4:F4:38:9F:2

Alias name: certplusclass2primaryca
Certificate fingerprints:
  MD5:  88:2C:8C:52:B8:A2:3C:F3:F7:BB:03:EA:AE:AC:42:0B
  SHA1: 74:20:74:41:72:9C:DD:92:EC:79:31:D8:23:10:8D:C2:81:92:E2:BB
  SHA256:
 0F:99:3C:8A:EF:97:BA:AF:56:87:14:0E:D5:9A:D1:82:1B:B4:AF:AC:F0:AA:9A:58:B5:D5:7A:33:8A:3A:FB:C

Alias name: ttelesecglobalrootclass2ca
Certificate fingerprints:
  MD5:  2B:9B:9E:E4:7B:6C:1F:00:72:1A:CC:C1:77:79:DF:6A
  SHA1: 59:0D:2D:7D:88:4F:40:2E:61:7E:A5:62:32:17:65:CF:17:D8:94:E9
  SHA256:
 91:E2:F5:78:8D:58:10:EB:A7:BA:58:73:7D:E1:54:8A:8E:CA:CD:01:45:98:BC:0B:14:3E:04:1B:17:05:25:5

Alias name: accvraiz1
Certificate fingerprints:
  MD5:  D0:A0:5A:EE:05:B6:09:94:21:A1:7D:F1:B2:29:82:02
  SHA1: 93:05:7A:88:15:C6:4F:CE:88:2F:FA:91:16:52:28:78:BC:53:64:17
  SHA256:
 9A:6E:C0:12:E1:A7:DA:9D:BE:34:19:4D:47:8A:D7:C0:DB:18:22:FB:07:1D:F1:29:81:49:6E:D1:04:38:41:1

Alias name: digicerthighassuranceevrootca
Certificate fingerprints:
  MD5:  D4:74:DE:57:5C:39:B2:D3:9C:85:83:C5:C0:65:49:8A
  SHA1: 5F:B7:EE:06:33:E2:59:DB:AD:0C:4C:9A:E6:D3:8F:1A:61:C7:DC:25
  SHA256:
 74:31:E5:F4:C3:C1:CE:46:90:77:4F:0B:61:E0:54:40:88:3B:A9:A0:1E:D0:0B:A6:AB:D7:80:6E:D3:B1:18:C
```

```
Alias name: amzninternalinfoseccag3
Certificate fingerprints:
  MD5:  E9:34:94:02:BA:BB:31:6B:22:E6:2B:A9:C4:F0:26:04
  SHA1: B9:B1:CA:38:F7:BF:9C:D2:D4:95:E7:B6:5E:75:32:9B:A8:78:2E:F6
  SHA256:
 81:03:0B:C7:E2:54:DA:7B:F8:B7:45:DB:DD:41:15:89:B5:A3:81:86:FB:4B:29:77:1F:84:0A:18:D9:67:6D:6

Alias name: cia-crt-g3-02-ca
Certificate fingerprints:
  MD5:  FD:B9:23:FD:D3:EB:2D:3E:57:EF:56:FF:DB:D3:E4:B9
  SHA1: 96:4A:BB:A7:BD:DA:FC:97:34:C0:0A:2D:F0:05:98:F7:E6:C6:6F:09
  SHA256:
 93:F1:72:FB:BA:43:31:5C:06:EE:0F:9F:04:89:B8:F6:88:BC:75:15:3C:BE:B4:80:AC:A7:14:3A:F6:FC:4A:C

Alias name: entrustrootcertificationauthorityec1
Certificate fingerprints:
  MD5:  B6:7E:1D:F0:58:C5:49:6C:24:3B:3D:ED:98:18:ED:BC
  SHA1: 20:D8:06:40:DF:9B:25:F5:12:25:3A:11:EA:F7:59:8A:EB:14:B5:47
  SHA256:
 02:ED:0E:B2:8C:14:DA:45:16:5C:56:67:91:70:0D:64:51:D7:FB:56:F0:B2:AB:1D:3B:8E:B0:70:E5:6E:DF:F

Alias name: securitycommunicationrootca
Certificate fingerprints:
  MD5:  F1:BC:63:6A:54:E0:B5:27:F5:CD:E7:1A:E3:4D:6E:4A
  SHA1: 36:B1:2B:49:F9:81:9E:D7:4C:9E:BC:38:0F:C6:56:8F:5D:AC:B2:F7
  SHA256:
 E7:5E:72:ED:9F:56:0E:EC:6E:B4:80:00:73:A4:3F:C3:AD:19:19:5A:39:22:82:01:78:95:97:4A:99:02:6B:6

Alias name: globalsignca
Certificate fingerprints:
  MD5:  3E:45:52:15:09:51:92:E1:B7:5D:37:9F:B1:87:29:8A
  SHA1: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C
  SHA256:
 EB:D4:10:40:E4:BB:3E:C7:42:C9:E3:81:D3:1E:F2:A4:1A:48:B6:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:9

Alias name: trustcenterclass2caii
Certificate fingerprints:
  MD5:  CE:78:33:5C:59:78:01:6E:18:EA:B9:36:A0:B9:2E:23
  SHA1: AE:50:83:ED:7C:F4:5C:BC:8F:61:C6:21:FE:68:5D:79:42:21:15:6E
  SHA256:
 E6:B8:F8:76:64:85:F8:07:AE:7F:8D:AC:16:70:46:1F:07:C0:A1:3E:EF:3A:1F:F7:17:53:8D:7A:BA:D3:91:B

Alias name: camerfirmachambersofcommerceroot
```

```
Certificate fingerprints:
  MD5:  B0:01:EE:14:D9:AF:29:18:94:76:8E:F1:69:33:2A:84
  SHA1: 6E:3A:55:A4:19:0C:19:5C:93:84:3C:C0:DB:72:2E:31:30:61:F0:B1
  SHA256:
 0C:25:8A:12:A5:67:4A:EF:25:F2:8B:A7:DC:FA:EC:EE:A3:48:E5:41:E6:F5:CC:4E:E6:3B:71:B3:61:60:6A:C

Alias name: geotrustprimarycag3
Certificate fingerprints:
  MD5:  B5:E8:34:36:C9:10:44:58:48:70:6D:2E:83:D4:B8:05
  SHA1: 03:9E:ED:B8:0B:E7:A0:3C:69:53:89:3B:20:D2:D9:32:3A:4C:2A:FD
  SHA256:
 B4:78:B8:12:25:0D:F8:78:63:5C:2A:A7:EC:7D:15:5E:AA:62:5E:E8:29:16:E2:CD:29:43:61:88:6C:D1:FB:D

Alias name: geotrustprimarycag2
Certificate fingerprints:
  MD5:  01:5E:D8:6B:BD:6F:3D:8E:A1:31:F8:12:E0:98:73:6A
  SHA1: 8D:17:84:D5:37:F3:03:7D:EC:70:FE:57:8B:51:9A:99:E6:10:D7:B0
  SHA256:
 5E:DB:7A:C4:3B:82:A0:6A:87:61:E8:D7:BE:49:79:EB:F2:61:1F:7D:D7:9B:F9:1C:1C:6B:56:6A:21:9E:D7:6

Alias name: hongkongpostrootca1
Certificate fingerprints:
  MD5:  A8:0D:6F:39:78:B9:43:6D:77:42:6D:98:5A:CC:23:CA
  SHA1: D6:DA:A8:20:8D:09:D2:15:4D:24:B5:2F:CB:34:6E:B2:58:B2:8A:58
  SHA256:
 F9:E6:7D:33:6C:51:00:2A:C0:54:C6:32:02:2D:66:DD:A2:E7:E3:FF:F1:0A:D0:61:ED:31:D8:BB:B4:10:CF:B

Alias name: affirmtrustpremiumeccca
Certificate fingerprints:
  MD5:  64:B0:09:55:CF:B1:D5:99:E2:BE:13:AB:A6:5D:EA:4D
  SHA1: B8:23:6B:00:2F:1D:16:86:53:01:55:6C:11:A4:37:CA:EB:FF:C3:BB
  SHA256:
 BD:71:FD:F6:DA:97:E4:CF:62:D1:64:7A:DD:25:81:B0:7D:79:AD:F8:39:7E:B4:EC:BA:9C:5E:84:88:82:14:2

Alias name: hellenicacademicandresearchinstitutionsrootca2015
Certificate fingerprints:
  MD5:  CA:FF:E2:DB:03:D9:CB:4B:E9:0F:AD:84:FD:7B:18:CE
  SHA1: 01:0C:06:95:A6:98:19:14:FF:BF:5F:C6:B0:B6:95:EA:29:E9:12:A6
  SHA256:
 A0:40:92:9A:02:CE:53:B4:AC:F4:F2:FF:C6:98:1C:E4:49:6F:75:5E:6D:45:FE:0B:2A:69:2B:CD:52:52:3F:3
```

# IoT Analytics

Die Aktion AWS IoT Analytics (`iotAnalytics`) sendet Daten von einer MQTT-Nachricht an einen AWS IoT Analytics Kanal.

## Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des `iotanalytics:BatchPutMessage` Vorgangs übernehmen AWS IoT kann. Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.

  Die an die von Ihnen angegebene Rolle angefügte Richtlinie sollte wie im folgenden Beispiel aussehen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iotanalytics:BatchPutMessage",
            "Resource": [
                "arn:aws:iotanalytics:us-west-2:account-id:channel/mychannel"
            ]
        }
    ]
}
```

## Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`batchMode`

(Optional) Gibt an, ob die Aktion als Batch verarbeitet werden soll. Der Standardwert ist `false`.

Wenn `batchMode` dies der `true` Fall ist und die SQL-Anweisung für die Regel ein Array ergibt, wird jedes Array-Element als separate Nachricht übermittelt, wenn es `BatchPutMessage`an den AWS IoT Analytics Channel weitergegeben wird. Das resultierende Array darf nicht mehr als 100 Nachrichten enthalten.

Unterstützt Ersatzvorlagen: Nein

`channelName`

Der Name des AWS IoT Analytics Kanals, in den die Daten geschrieben werden sollen.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`roleArn`

Die IAM-Rolle, die den Zugriff auf den AWS IoT Analytics Kanal ermöglicht. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

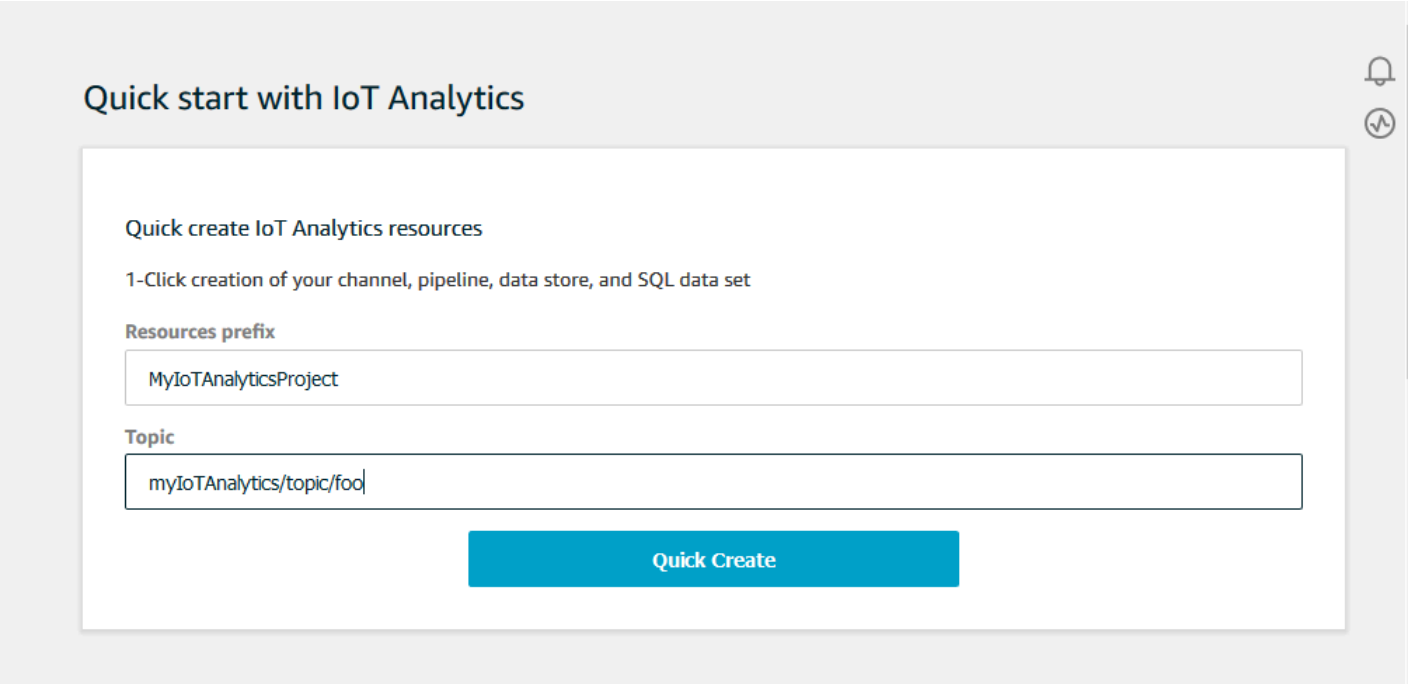
Das folgende JSON-Beispiel definiert eine AWS IoT Analytics Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "iotAnalytics": {
                    "channelName": "mychannel",
                    "roleArn": "arn:aws:iam::123456789012:role/analyticsRole",
                }
            }
        ]
    }
}
```

## Weitere Informationen finden Sie auch unter

- Was ist AWS IoT Analytics? im AWS IoT Analytics Benutzerhandbuch

- Die AWS IoT Analytics Konsole verfügt außerdem über eine Schnellstartfunktion, mit der Sie mit einem Klick einen Kanal, einen Datenspeicher, eine Pipeline und einen Datenspeicher erstellen können. Weitere Informationen finden Sie unter AWS IoT Analytics Schnellstartanleitung für die Konsole im AWS IoT Analytics Benutzerhandbuch.




## AWS IoT Events

Die Aktion AWS IoT Events (`iotEvents`) sendet Daten von einer MQTT-Nachricht an eine AWS IoT Events Eingabe.

> **Important**
>
> Wenn die Payload AWS IoT Core ohne den gesendet wird oder wenn sich der `Input attribute Key` Schlüssel nicht in demselben JSON-Pfad befindet, der im Schlüssel angegeben ist, führt dies dazu, dass die IoT-Regel mit dem Fehler `Failed to send message to Iot Events` fehlschlägt.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des `iotevents:BatchPutMessage` Vorgangs übernehmen AWS IoT kann. Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.

## Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`batchMode`

(Optional) Gibt an, ob die Ereignisaktionen als Batch verarbeitet werden sollen. Der Standardwert ist `false`.

Wenn dies der `true` Fall `batchMode` ist und die SQL-Anweisung für die Regel ein Array ergibt, wird jedes Array-Element als separate Nachricht behandelt, wenn es durch einen Aufruf `BatchPutMessage`an AWS IoT Events gesendet wird. Das resultierende Array darf nicht mehr als 10 Nachrichten enthalten.

Wenn `batchMode` `true` ist, können Sie kein `messageId` angeben.

Unterstützt Ersatzvorlagen: Nein

`inputName`

Der Name der AWS IoT Events Eingabe.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`messageId`

(Optional) Verwenden Sie diese Option, um zu überprüfen, ob nur eine Eingabe (Nachricht) mit einem bestimmten Wert von einem AWS IoT Events Detektor verarbeitet `messageId` wird. Sie können die `${newuuid()}` Ersatzvorlage verwenden, um für jede Anfrage eine eindeutige ID zu generieren.

Wenn `batchMode` `true` ist, können Sie `messageId` nicht angeben--ein neuer UUID-Wert wird zugewiesen.

Unterstützt Ersatzvorlagen: Ja

`roleArn`

Die IAM-Rolle, die es ermöglicht AWS IoT , eine Eingabe an einen AWS IoT Events Detektor zu senden. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

### Beispiele

Das folgende JSON-Beispiel definiert eine IoT-Ereignis-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "iotEvents": {
                    "inputName": "MyIoTEventsInput",
                    "messageId": "${newuuid()}",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_events"
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist AWS IoT Events? im AWS IoT Events Developer Guide

## AWS IoT SiteWise

Die Aktion AWS IoT SiteWise (`iotSiteWise`) sendet Daten aus einer MQTT-Nachricht an die Asset-Eigenschaften in. AWS IoT SiteWise

Sie können einem Tutorial folgen, das Ihnen zeigt, wie Sie Daten von AWS IoT Dingen aufnehmen können. Weitere Informationen finden Sie im Tutorial Daten AWS IoT SiteWise aus AWS IoT Dingen

aufnehmen oder im Abschnitt Daten mithilfe von AWS IoT Kernregeln aufnehmen im AWS IoT SiteWise Benutzerhandbuch.

## Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des Vorgangs übernehmen AWS IoT kann. `iotsitewise:BatchPutAssetPropertyValue` Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  Sie können die folgende Beispiel-Vertrauensrichtlinie mit der Rolle verknüpfen.

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

  Um die Sicherheit zu erhöhen, können Sie in der `Condition` Eigenschaft einen Pfad zur AWS IoT SiteWise Asset-Hierarchie angeben. Das folgende Beispiel ist eine Vertrauensrichtlinie, die einen Komponentenhierarchiepfad angibt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iotsitewise:BatchPutAssetPropertyValue",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iotsitewise:assetHierarchyPath": [
                        "/root node asset ID",
                        "/root node asset ID/*"
                    ]
                }
```

```
            }
        }
    ]
}
```

- Wenn Sie AWS IoT SiteWise mit dieser Aktion Daten an senden, müssen Ihre Daten die Anforderungen des `BatchPutAssetPropertyValue` Vorgangs erfüllen. Weitere Informationen finden Sie unter BatchPutAssetPropertyValue in der AWS IoT SiteWise -API-Referenz.

## Parameter

Wenn Sie mit dieser Aktion eine AWS IoT Regel erstellen, müssen Sie die folgenden Informationen angeben:

`putAssetPropertyValueEntries`

Eine Liste mit Werteinträgen für die Komponenteneigenschaft, die jeweils die folgenden Informationen enthalten:

`propertyAlias`

(Optional) Der Eigenschaftenalias, der Ihrer Komponenteneigenschaft zugeordnet ist. Geben Sie entweder einen `propertyAlias` oder sowohl eine `assetId` als auch eine `propertyId` an. Weitere Informationen zu Eigenschaftsaliasnamen finden Sie unter Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften im AWS IoT SiteWise -Benutzerhandbuch.

Unterstützt Ersatzvorlagen: Ja

`assetId`

(Optional) Die ID des AWS IoT SiteWise Assets. Geben Sie entweder einen `propertyAlias` oder sowohl eine `assetId` als auch eine `propertyId` an.

Unterstützt Ersatzvorlagen: Ja

`propertyId`

(Optional) Die ID der Komponenteneigenschaft. Geben Sie entweder einen `propertyAlias` oder sowohl eine `assetId` als auch eine `propertyId` an.

Unterstützt Ersatzvorlagen: Ja

`entryId`

(Optional) Ein eindeutiger Bezeichner für diesen Eintrag. Definieren Sie die `entryId`, um besser zu nachzuverfolgen, welche Nachricht ggf. einen Fehler verursacht hat. Standardmäßig wird eine neue UUID verwendet.

Unterstützt Ersatzvorlagen: Ja

`propertyValues`

Eine Liste der einzufügenden Eigenschaftswerte, die jeweils Zeitstempel, Qualität und Wert (Timestamp, Quality and Value, TQV) im folgenden Format enthalten:

`timestamp`

Eine Zeitstempelstruktur, die die folgenden Informationen enthält:

`timeInSeconds`

Eine Zeichenfolge, die die Zeit in Sekunden in der Unix-Epochenzeit enthält. Wenn Ihre Nachrichtennutzlast keinen Zeitstempel hat, können Sie timestamp() verwenden, der die aktuelle Zeit in Millisekunden zurückgibt. Um diese Zeit in Sekunden zu konvertieren, können Sie die folgende Ersetzungsvorlage verwenden: **`${floor(timestamp() / 1E3)}`**.

Unterstützt Ersatzvorlagen: Ja

`offsetInNanos`

(Optional) Eine Zeichenfolge, die den Zeitversatz in Nanosekunden von der Zeit in Sekunden enthält. Wenn Ihre Nachrichtennutzlast keinen Zeitstempel hat, können Sie timestamp() verwenden, der die aktuelle Zeit in Millisekunden zurückgibt. Um den Nanosekunden-Zeitversatz von diesem Zeitpunkt zu berechnen, können Sie die folgende Ersetzungsvorlage verwenden: **`${(timestamp() % 1E3) * 1E6}`**.

Unterstützt Ersatzvorlagen: Ja

In Bezug auf die Unix-Epochenzeit werden nur Einträge AWS IoT SiteWise akzeptiert, die einen Zeitstempel von bis zu 7 Tagen in der Vergangenheit und bis zu 5 Minuten in der future haben.

`quality`

(Optional) Eine Zeichenfolge, die die Qualität des Werts beschreibt. Zulässige Werte: `GOOD`, `BAD`, `UNCERTAIN`.

Unterstützt Ersatzvorlagen: Ja

`value`

Eine Wertestruktur, die eines der folgenden Wertfelder enthält, je nach Datentyp der Komponenteneigenschaft:

`booleanValue`

(Optional) Eine Zeichenfolge, die den booleschen Wert des Werteintrags enthält.

Unterstützt Ersatzvorlagen: Ja

`doubleValue`

(Optional) Eine Zeichenfolge, die den doppelten Wert des Werteintrags enthält.

Unterstützt Ersatzvorlagen: Ja

`integerValue`

(Optional) Eine Zeichenfolge, die den Ganzzahlwert des Werteintrags enthält.

Unterstützt Ersatzvorlagen: Ja

`stringValue`

(Optional) Der Zeichenfolgenwert des Werteintrags.

Unterstützt Ersatzvorlagen: Ja

`roleArn`

Der ARN der IAM-Rolle, die die AWS IoT Berechtigung zum Senden eines Vermögenseigenschaftswerts an AWS IoT SiteWise erteilt. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine grundlegende SiteWise IoT-Aktion in einer AWS IoT Regel.

```
{
```

```
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "iotSiteWise": {
                    "putAssetPropertyValueEntries": [
                        {
                            "propertyAlias": "/some/property/alias",
                            "propertyValues": [
                                {
                                    "timestamp": {
                                        "timeInSeconds": "${my.payload.timeInSeconds}"
                                    },
                                    "value": {
                                        "integerValue": "${my.payload.value}"
                                    }
                                }
                            ]
                        }
                    ],
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_sitewise"
                }
            }
        ]
    }
}
```

Das folgende JSON-Beispiel definiert eine SiteWise IoT-Aktion in einer AWS IoT Regel. In diesem Beispiel wird das Thema als Eigenschaftsalias und die `timestamp()` Funktion verwendet. Wenn Sie beispielsweise Daten in `/company/windfarm/3/turbine/7/rpm` veröffentlichen, sendet diese Aktion die Daten an die Komponenteneigenschaft mit einem Eigenschaftsalias, der dem von Ihnen angegebenen Thema entspricht.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM '/company/windfarm/+/turbine/+/+'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "iotSiteWise": {
```

```
                    "putAssetPropertyValueEntries": [
                        {
                            "propertyAlias": "${topic()}",
                            "propertyValues": [
                                {
                                    "timestamp": {
                                        "timeInSeconds": "${floor(timestamp() / 1E3)}",
                                        "offsetInNanos": "${(timestamp() % 1E3) * 1E6}"
                                    },
                                    "value": {
                                        "doubleValue": "${my.payload.value}"
                                    }
                                }
                            ]
                        }
                    ],
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_sitewise"
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist AWS IoT SiteWise? im AWS IoT SiteWise Benutzerhandbuch
- Daten mithilfe von AWS IoT Core Regeln im AWS IoT SiteWise Benutzerhandbuch aufnehmen
- Daten aus AWS IoT Dingen AWS IoT SiteWise aus dem Benutzerhandbuch aufnehmen AWS IoT SiteWise
- Problembehandlung bei einer AWS IoT SiteWise Regelaktion im AWS IoT SiteWise Benutzerhandbuch

## Firehose

Die Aktion Firehose (`firehose`) sendet Daten aus einer MQTT-Nachricht an einen Amazon Data Firehose-Stream.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des AWS IoT Vorgangs übernehmen kann. `firehose:PutRecord` Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.
- Wenn Sie Firehose verwenden, um Daten an einen Amazon S3-Bucket zu senden, und Sie einen AWS KMS Kunden verwenden, der es geschafft hat, ruhende Daten in Amazon S3 AWS KMS key zu verschlüsseln, muss Firehose Zugriff auf Ihren Bucket und die Erlaubnis haben, diesen im Namen des AWS KMS key Anrufers zu verwenden. Weitere Informationen finden Sie unter Grant Firehose access to a Amazon S3 destination im Amazon Data Firehose Developer Guide.

## Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`batchMode`

(Optional) Ob der Firehose-Stream als Batch bereitgestellt werden soll, indem Sie `PutRecordBatch`. Der Standardwert ist `false`.

Wenn `batchMode` `true` ist und die SQL-Anweisung der Regel zu einem Array ausgewertet wird, bildet jedes Array-Element einen Datensatz in der `PutRecordBatch`-Anforderung. Das resultierende Array darf nicht mehr als 500 Datensätze enthalten.

Unterstützt Ersatzvorlagen: Nein

`deliveryStreamName`

Der Firehose-Stream, in den die Nachrichtendaten geschrieben werden sollen.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`separator`

(Optional) Ein Zeichentrennzeichen, das verwendet wird, um Datensätze zu trennen, die in den Firehose geschrieben wurden. Wenn Sie diesen Parameter auslassen, verwendet der Stream kein Trennzeichen. Gültige Werte: `,` (Komma), `\t` (Tab), `\n` (Newline), `\r\n` (Windows Newline).

Unterstützt Ersatzvorlagen: Nein

`roleArn`

Die IAM-Rolle, die den Zugriff auf den Firehose-Stream ermöglicht. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine Firehose-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "firehose": {
                    "deliveryStreamName": "my_firehose_stream",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_firehose"
                }
            }
        ]
    }
}
```

Das folgende JSON-Beispiel definiert eine Firehose-Aktion mit Ersatzvorlagen in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "firehose": {
                    "deliveryStreamName": "${topic()}",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_firehose"
                }
            }
```

```
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist Amazon Data Firehose? im Amazon Data Firehose Developer Guide

## Kinesis Data Streams

Die Aktion Kinesis Data Streams (`kinesis`) schreibt Daten aus einer MQTT-Nachricht in Amazon Kinesis Data Streams.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des AWS IoT Vorgangs übernehmen kann. `kinesis:PutRecord` Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.
- Wenn Sie einen AWS KMS vom Kunden verwalteten AWS KMS key (KMS-Schlüssel) verwenden, um ruhende Daten in Kinesis Data Streams zu verschlüsseln, muss der Service über die Erlaubnis verfügen, den im Namen des AWS KMS key Anrufers zu verwenden. Weitere Informationen finden Sie unter Berechtigungen zur Verwendung von benutzergenerierten AWS KMS keys im Amazon Kinesis Data Streams Entwicklerhandbuch.

### Parameter

Wenn Sie mit dieser Aktion eine AWS IoT Regel erstellen, müssen Sie die folgenden Informationen angeben:

`stream`

Der Kinesis Data Stream, in den die Daten geschrieben werden

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`partitionKey`

Der Partitionsschlüssel, mit dem bestimmt wird, in welchen Shard die Daten geschrieben werden. Der Partitionsschlüssel besteht in der Regel aus einem Ausdruck (z. B. `${topic()}` oder `${timestamp()}`).

Unterstützt Ersatzvorlagen: Ja

`roleArn`

Der ARN der IAM-Rolle, die die AWS IoT Berechtigung zum Zugriff auf den Kinesis-Datenstream gewährt. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine Kinesis Data Streams Streams-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "kinesis": {
                    "streamName": "my_kinesis_stream",
                    "partitionKey": "${topic()}",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_kinesis"
                }
            }
        ]
    }
}
```

Das folgende JSON-Beispiel definiert eine Kinesis-Aktion mit Ersatzvorlagen in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
```

```
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "kinesis": {
                    "streamName": "${topic()}",
                    "partitionKey": "${timestamp()}",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_kinesis"
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist Amazon Kinesis Data Streams? im Entwicklerhandbuch für Amazon Kinesis Data Streams

## Lambda

Eine Lambda (`lambda`) -Aktion ruft eine AWS Lambda Funktion auf und übergibt eine MQTT-Nachricht. AWS IoT ruft Lambda-Funktionen asynchron auf.

Sie können einem Tutorial folgen, das Ihnen veranschaulicht, wie Sie eine Regel mit einer Lambda-Aktion erstellen und testen. Weitere Informationen finden Sie unter Tutorial: Formatieren einer Benachrichtigung mithilfe einer AWS Lambda Funktion.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- AWS IoT Um eine Lambda-Funktion aufzurufen, müssen Sie eine Richtlinie konfigurieren, die die `lambda:InvokeFunction` Berechtigung dazu erteilt. AWS IoT Sie können nur eine Lambda-Funktion aufrufen, die in derselben AWS-Region definiert ist, in der Ihre Lambda-Richtlinie existiert. Lambda-Funktionen verwenden ressourcenbasierte Richtlinien, daher müssen Sie die Richtlinie an die Lambda-Funktion selbst anhängen.

  Verwenden Sie den folgenden AWS CLI Befehl, um eine Richtlinie anzuhängen, die die Berechtigung erteilt. `lambda:InvokeFunction` Ersetzen Sie in diesem Befehl:

- *function_name*mit dem Namen der Lambda-Funktion. Sie fügen eine neue Berechtigung hinzu, um die Ressourcenrichtlinie der Funktion zu aktualisieren.
- *region*mit dem AWS-Region der Funktion.
- *account-id*mit der AWS-Konto Nummer, unter der die Regel definiert ist.
- *rule-name*mit dem Namen der AWS IoT Regel, für die Sie die Lambda-Aktion definieren.
- *unique_id*mit einer eindeutigen Anweisungskennung.

> **Important**
>
> Wenn Sie eine Berechtigung für einen AWS IoT Prinzipal hinzufügen, ohne das `source-arn` oder anzugeben, kann jeder `source-account` AWS-Konto , der mit Ihrer Lambda-Aktion eine Regel erstellt, Regeln aktivieren, von denen aus Ihre Lambda-Funktion aufgerufen wird. AWS IoT

Weitere Informationen finden Sie unter AWS Lambda Berechtigungen.

```
aws lambda add-permission \
    --function-name function_name \
    --region region \
    --principal iot.amazonaws.com \
    --source-arn arn:aws:iot:region:account-id:rule/rule_name \
    --source-account account-id
    --statement-id unique_id
    --action "lambda:InvokeFunction"
```

- Wenn Sie die AWS IoT Konsole verwenden, um eine Regel für die Lambda-Regelaktion zu erstellen, wird die Lambda-Funktion automatisch ausgelöst. Wenn Sie AWS CloudFormation stattdessen mit dem verwenden `AWS::IoT::TopicRule LambdaAction`, müssen Sie eine `AWS::lambda::Permission`Ressource hinzufügen. Die Ressource erteilt Ihnen dann die Erlaubnis, die Lambda-Funktion auszulösen.

  Der folgende Code zeigt ein Beispiel für das Hinzufügen dieser Ressource. Ersetzen Sie in diesem Beispiel:

  - *function_name*mit dem Namen der Lambda-Funktion.
  - *region*mit dem AWS-Region der Funktion.
  - *account-id*mit der AWS-Konto Nummer, unter der die Regel definiert ist.

- *rule-name*mit dem Namen der AWS IoT Regel, für die Sie die Lambda-Aktion definieren.

```
Type: AWS::Lambda::Permission
Properties:
  Action: lambda:InvokeFunction
  FunctionName: !Ref function_name
  Principal: "iot.amazonaws.com"
  SourceAccount: account-id
  SourceArn: arn:aws:iot:region:account-id:rule/rule_name
```

- Wenn Sie einen AWS KMS Kunden verwenden, der es geschafft hat AWS KMS key , ruhende Daten in Lambda zu verschlüsseln, muss der Dienst über die Erlaubnis verfügen, den im Namen des AWS KMS key Anrufers zu verwenden. Weitere Informationen finden Sie unter Verschlüsselung im Ruhezustand im Entwicklerhandbuch für AWS Lambda .

## Parameter

Wenn Sie mit dieser Aktion eine AWS IoT Regel erstellen, müssen Sie die folgenden Informationen angeben:

`functionArn`

Der ARN der aufzurufenden Lambda-Funktion. AWS IoT muss die Erlaubnis haben, die Funktion aufzurufen. Weitere Informationen finden Sie unter Voraussetzungen.

Wenn Sie für Ihre Lambda-Funktion keine Version oder keinen Alias angeben, wird die neueste Version der Funktion heruntergefahren. Sie können eine Version oder einen Alias angeben, wenn Sie eine bestimmte Version Ihrer Lambda-Funktion herunterfahren möchten. Um eine Version oder einen Alias anzugeben, fügen Sie die Version oder den Alias dem ARN der Lambda-Funktion hinzu.

```
arn:aws:lambda:us-east-2:123456789012:function:myLambdaFunction:someAlias
```

Weitere Informationen über Versionsverwaltung und Aliasse finden Sie unter AWS Lambda Funktions-Versionsverwaltung und Aliasse.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

## Beispiele

Das folgende JSON-Beispiel definiert eine Lambda-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "lambda": {
                    "functionArn": "arn:aws:lambda:us-
east-2:123456789012:function:myLambdaFunction"
                 }
            }
        ]
    }
}
```

Das folgende JSON-Beispiel definiert eine Lambda-Aktion mit Ersatzvorlagen in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "lambda": {
                    "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:
${topic()}"
                }
            }
        ]
    }
}
```

## Weitere Informationen finden Sie auch unter

- Was ist? AWS Lambda im AWS Lambda Developer Guide

- Tutorial: Formatieren einer Benachrichtigung mithilfe einer AWS Lambda Funktion

## Ort

Die Aktion Standort (`location`) sendet Ihre geografischen Standortdaten an Amazon Location Service.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des `geo:BatchUpdateDevicePosition` Vorgangs übernehmen AWS IoT kann. Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.

### Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`deviceId`

Die eindeutige ID des Geräts, das die Standortdaten bereitstellt. Weitere Informationen finden Sie unter `DeviceId` in der Amazon Location Service API-Referenz.

Unterstützt Ersatzvorlagen: Ja

`latitude`

Eine Zeichenfolge, die einen doppelten Wert ergibt, der den Breitengrad des Gerätestandorts darstellt.

Unterstützt Ersatzvorlagen: Ja

`longitude`

Eine Zeichenfolge, die einen doppelten Wert ergibt, der den Längengrad des Gerätestandorts darstellt.

Unterstützt Ersatzvorlagen: Ja

`roleArn`

Die IAM-Rolle, die Zugriff auf die Amazon-Location-Service-Domain gewährt. Weitere Informationen finden Sie unter Voraussetzungen.

`timestamp`

Der Zeitpunkt, zu dem die Standortdaten erfasst wurden. Der Standardwert ist der Zeitpunkt, zu dem die MQTT-Nachricht verarbeitet wurde.

Der `timestamp` Wert besteht aus den folgenden beiden Werten:

- `value`: Ein Ausdruck, der einen Wert für lange Epochenzeit zurückgibt. Sie können die the section called “time_to_epoch (Zeichenfolge, Zeichenfolge)” Funktion verwenden, um aus einem Datums- oder Uhrzeitwert, der in der Nachrichtennutzlast übergeben wurde, einen gültigen Zeitstempel zu erstellen. Unterstützt Ersatzvorlagen: Ja
- `unit`: (Optional) Die Genauigkeit des Zeitstempelwerts, die sich aus dem unter `value` beschriebenen Ausdruck ergibt. Zulässige Werte: `SECONDS` | `MILLISECONDS` | `MICROSECONDS` | `NANOSECONDS`. Der Standardwert ist `MILLISECONDS`. Unterstützt Ersatzvorlagen: API und AWS CLI nur.

`trackerName`

Der Name der Tracker-Ressource in Amazon Location, in der der Standort aktualisiert wird. Weitere Informationen finden Sie unter Tracker im Amazon Location Service Entwicklerhandbuch.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

## Beispiele

Das folgende JSON-Beispiel definiert eine Location-Aktion in einer AWS IoT Regel.

```
{
 "topicRulePayload": {
  "sql": "SELECT * FROM 'some/topic'",
  "ruleDisabled": false,
  "awsIotSqlVersion": "2016-03-23",
  "actions": [
   {
```

```
    "location": {
     "roleArn": "arn:aws:iam::123454962127:role/service-role/ExampleRole",
     "trackerName": "MyTracker",
     "deviceId": "001",
     "sampleTime": {
      "value": "${timestamp()}",
      "unit": "MILLISECONDS"
     },
     "latitude": "-12.3456",
     "longitude": "65.4321"
    }
   }
  ]
 }
}
```

Das folgende JSON-Beispiel definiert eine Location-Aktion mit Ersatzvorlagen in einer AWS IoT Regel.

```
{
 "topicRulePayload": {
  "sql": "SELECT * FROM 'some/topic'",
  "ruleDisabled": false,
  "awsIotSqlVersion": "2016-03-23",
  "actions": [
   {
    "location": {
     "roleArn": "arn:aws:iam::123456789012:role/service-role/ExampleRole",
     "trackerName": "${TrackerName}",
     "deviceId": "${DeviceID}",
     "timestamp": {
      "value": "${timestamp()}",
      "unit": "MILLISECONDS"
     },
     "latitude": "${get(position, 0)}",
     "longitude": "${get(position, 1)}"
    }
   }
  ]
 }
}
```

Das folgende Beispiel für eine MQTT-Nutzlast zeigt, wie Ersatzvorlagen im vorherigen Beispiel auf Daten zugreifen. Sie können den get-device-position-history CLI-Befehl verwenden, um zu überprüfen, ob die MQTT-Nutzlastdaten in Ihrem Standort-Tracker geliefert werden.

```
{
 "TrackerName": "mytracker",
 "DeviceID": "001",
 "position": [
  "-12.3456",
  "65.4321"
 ]
}
```

```
aws location get-device-position-history --device-id 001 --tracker-name mytracker
```

```
{
 "DevicePositions": [
  {
   "DeviceId": "001",
   "Position": [
    -12.3456,
    65.4321
   ],
   "ReceivedTime": "2022-11-11T01:31:54.464000+00:00",
   "SampleTime": "2022-11-11T01:31:54.308000+00:00"
  }
 ]
}
```

### Weitere Informationen finden Sie auch unter

- Was ist Amazon Location Service? im Amazon Location Service Entwicklerhandbuch.

## OpenSearch

Die Aktion OpenSearch (`openSearch`) schreibt Daten aus MQTT-Nachrichten in eine Amazon OpenSearch Service-Domain. Sie können dann Tools wie OpenSearch Dashboards verwenden, um Daten in OpenSearch Service abzufragen und zu visualisieren.

## Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des `es:ESHttpPut` Vorgangs übernehmen AWS IoT kann. Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.
- Wenn Sie einen Kunden einsetzen, der es geschafft hat, ruhende Daten im OpenSearch Service AWS KMS key zu verschlüsseln, muss der Service über die Erlaubnis verfügen, den KMS-Schlüssel im Namen des Anrufers zu verwenden. Weitere Informationen finden Sie unter Verschlüsselung ruhender Daten für Amazon OpenSearch Service im Amazon OpenSearch Service Developer Guide.

## Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`endpoint`

Der Endpunkt Ihrer Amazon OpenSearch Service-Domain.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`index`

Der OpenSearch Index, in dem Sie Ihre Daten speichern möchten.

Unterstützt Ersatzvorlagen: Ja

`type`

Der Typ des Dokuments, das Sie speichern

> **Note**
>
> Für OpenSearch Versionen nach 1.0 muss der Wert des `type` Parameters sein`_doc`. Weitere Informationen finden Sie in der OpenSearch -Dokumentation.

Unterstützt Ersatzvorlagen: Ja

`id`

Der eindeutige Bezeichner für jedes Dokument

Unterstützt Ersatzvorlagen: Ja

`roleARN`

Die IAM-Rolle, die den Zugriff auf die OpenSearch Service-Domäne ermöglicht. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Einschränkungen

Die Aktion OpenSearch (`openSearch`) kann nicht verwendet werden, um Daten an VPC-Elasticsearch-Cluster zu liefern.

## Beispiele

Das folgende JSON-Beispiel definiert eine OpenSearch Aktion in einer AWS IoT Regel und wie Sie die Felder für die `OpenSearch` Aktion angeben können. Weitere Informationen finden Sie unter OpenSearchAction.

```
{
    "topicRulePayload": {
        "sql": "SELECT *, timestamp() as timestamp FROM 'iot/test'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "openSearch": {
                    "endpoint": "https://my-endpoint",
                    "index": "my-index",
                    "type": "_doc",
                    "id": "${newuuid()}",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_os"
                }
            }
        ]
    }
```

```
}
```

Das folgende JSON-Beispiel definiert eine OpenSearch Aktion mit Ersatzvorlagen in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "openSearch": {
                    "endpoint": "https://my-endpoint",
                    "index": "${topic()}",
                    "type": "${type}",
                    "id": "${newuuid()}",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_os"
                }
            }
        ]
    }
}
```

> **Note**
>
> Das ersetzte `type` Feld funktioniert für OpenSearch Version 1.0. Für alle Versionen nach 1.0 `type` muss der Wert von sein`_doc`.

### Weitere Informationen finden Sie auch unter

Was ist Amazon OpenSearch Service? im Amazon OpenSearch Service Developer Guide

## Wiederveröffentlichen

Die Aktion neu veröffentlichen (`republish`) veröffentlicht eine MQTT-Nachricht erneut in einem anderen MQTT-Thema.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des Vorgangs übernehmen AWS IoT kann. `iot:Publish` Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.

## Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`headers`

Header-Informationen für MQTT Version 5.0.

Weitere Informationen finden Sie unter RepublishAction und MqttHeaders in der AWS -API-Referenz.

`topic`

Das MQTT-Thema, für das die Nachricht erneut veröffentlicht werden soll

Um in einem reservierten Thema, das mit $ beginnt, erneut zu veröffentlichen, verwenden Sie stattdessen `$$`. Um zum Beispiel das Thema Geräteschatten `$aws/things/MyThing/shadow/update` neu zu veröffentlichen, geben Sie das Thema als `$$aws/things/MyThing/shadow/update` an.

> **Note**
>
> Das erneute Veröffentlichen zu reservierten Jobthemen wird nicht unterstützt.
> AWS IoT Device Defender Reserve-Themen unterstützen keine HTTP-Veröffentlichung.

Unterstützt Ersatzvorlagen: Ja

`qos`

(Optional) Das QoS (Quality of Service)-Niveau, das verwendet werden soll, wenn Nachrichten erneut veröffentlicht werden. Zulässige Werte: `0`, `1`. Der Standardwert ist `0`. Weitere Informationen zu MQTT QoS finden Sie unter MQTT.

Unterstützt Ersatzvorlagen: Nein

`roleArn`

Die IAM-Rolle, die das Veröffentlichen im MQTT-Thema ermöglicht AWS IoT . Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine Aktion zum erneuten Veröffentlichen in einer Regel. AWS IoT

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "republish": {
                    "topic": "another/topic",
                    "qos": 1,
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_republish"
                }
            }
        ]
    }
}
```

Das folgende JSON-Beispiel definiert eine Aktion zur erneuten Veröffentlichung mit Ersatzvorlagen in einer Regel. AWS IoT

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "republish": {
```

```
                    "topic": "${topic()}/republish",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_republish"
                }
            }
        ]
    }
}
```

Das folgende JSON-Beispiel definiert eine Aktion zur erneuten Veröffentlichung `headers` in einer Regel. AWS IoT

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "republish": {
                    "topic": "${topic()}/republish",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_republish",
                    "headers": {
                        "payloadFormatIndicator": "UTF8_DATA",
                        "contentType": "rule/contentType",
                        "correlationData": "cnVsZSBjb3JyZWxhdGlvbiBkYXRh",
                        "userProperties": [
                            {
                                "key": "ruleKey1",
                                "value": "ruleValue1"
                            },
                            {
                                "key": "ruleKey2",
                                "value": "ruleValue2"
                            }
                        ]
                    }
                }
            }
        ]
    }
}
```

> **Note**
>
> Die ursprüngliche Quell-IP wird bei der Aktion zur erneuten Veröffentlichung nicht weitergegeben.

## S3

Die S3 (`s3`) Aktion schreibt die Daten aus einer MQTT-Nachricht in einen Amazon Simple Storage Service (Amazon S3)-Bucket.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des `s3:PutObject` Vorgangs übernehmen AWS IoT kann. Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.
- Wenn Sie einen AWS KMS Kunden verwenden, der AWS KMS key zur Verschlüsselung ruhender Daten in Amazon S3 verwaltet wird, muss der Service über die Erlaubnis verfügen, den im Namen des AWS KMS key Anrufers zu verwenden. Weitere Informationen finden Sie unter AWS Verwaltet AWS KMS keys und vom Kunden verwaltet AWS KMS keys im Amazon Simple Storage Service Developer Guide.

### Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`bucket`

Der Amazon S3-Bucket, in den die Daten geschrieben werden

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`cannedacl`

(Optional) Die vordefinierte Amazon S3-ACL, der den Zugriff auf das Objekt steuert, das vom Objektschlüssel identifiziert wurde. Weitere Informationen, einschließlich der zulässigen Werte, finden Sie unter Vordefinierter ACL.

Unterstützt Ersatzvorlagen: Nein

`key`

Der Pfad zur Datei, in die die Daten geschrieben werden.

Nehmen wir ein Beispiel, bei dem dieser Parameter `${topic()}/${timestamp()}` ist und die Regel eine Nachricht mit dem Thema `some/topic` empfängt. Wenn der aktuelle Zeitstempel `1460685389` ist, dann schreibt diese Aktion die Daten in eine Datei namens `1460685389` im Ordner `some/topic` des S3-Buckets.

> **Note**
>
> Wenn Sie einen statischen Schlüssel verwenden, wird bei jedem Aufruf der Regel eine einzelne Datei AWS IoT überschrieben. Wir empfehlen Ihnen, den Zeitstempel der Nachricht oder einen anderen eindeutigen Nachrichtenbezeichner zu verwenden, damit für jede empfangene Nachricht eine neue Datei in Amazon S3 gespeichert wird.

Unterstützt Ersatzvorlagen: Ja

`roleArn`

Die IAM-Rolle, die den Zugriff auf den Amazon S3-Bucket ermöglicht. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine S3-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
```

```
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "s3": {
                    "bucketName": "amzn-s3-demo-bucket",
                    "cannedacl": "public-read",
                    "key": "${topic()}/${timestamp()}",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_s3"
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist Amazon S3? im Entwicklerhandbuch für Amazon Simple Storage Service

## Salesforce-IoT

Die Salesforce IoT (`salesforce`) Aktion sendet Daten aus der die Regel auslösenden MQTT-Nachricht an einen Salesforce IoT-Eingabe-Stream.

### Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`url`

Die vom Salesforce IoT-Eingabe-Stream veröffentlichte URL. Die URL steht auf der Salesforce IoT-Plattform zur Verfügung, wenn Sie einen Eingabe-Stream erstellen. Weitere Informationen finden Sie in der Dokumentation zu Salesforce IoT

Unterstützt Ersatzvorlagen: Nein

`token`

Das Token, das zum Authentifizieren des Zugriffs auf den angegebenen Salesforce IoT-Eingabe-Stream verwendet wird. Das Token steht auf der Salesforce IoT-Plattform zur Verfügung, wenn

Sie einen Eingabe-Stream erstellen. Weitere Informationen finden Sie in der Dokumentation zu Salesforce IoT

Unterstützt Ersatzvorlagen: Nein

### Beispiele

Das folgende JSON-Beispiel definiert eine Salesforce IoT-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "salesforce": {
                    "token": "ABCDEFGHI123456789abcdefghi123456789",
                    "url": "https://ingestion-cluster-id.my-env.sfdcnow.com/streams/
stream-id/connection-id/my-event"
                }
            }
        ]
    }
}
```

## SNS

Die Aktion SNS (`sns`) sendet die Daten aus einer MQTT-Nachricht als Amazon Simple Notification Service (Amazon SNS) Push-Nachricht.

Sie können einem Tutorial folgen, das Ihnen veranschaulicht, wie Sie eine Regel mit einer SNS-Aktion erstellen und testen. Weitere Informationen finden Sie unter Tutorial: Eine SNS Amazon-Benachrichtigung senden.

> **Note**
>
> Die SNS-Aktion unterstützt keine Amazon SNS-FIFO-Themen (First-In-First-Out). Da die Regeln-Engine ein vollständig verteilter Dienst ist, gibt es keine Garantie für die Reihenfolge der Nachrichten, wenn die SNS-Aktion aufgerufen wird.

## Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des Vorgangs übernehmen AWS IoT kann. `sns:Publish` Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.
- Wenn Sie einen vom AWS KMS Kunden verwalteten Dienst AWS KMS key zur Verschlüsselung ruhender Daten in Amazon SNS verwenden, muss der Service über die Erlaubnis verfügen, den im Namen des Anrufers AWS KMS key zu verwenden. Weitere Informationen dazu erhalten Sie unter Schlüsselverwaltung im Entwicklerhandbuch für Amazon Simple Notification Service.

## Parameter

Wenn Sie mit dieser Aktion eine AWS IoT Regel erstellen, müssen Sie die folgenden Informationen angeben:

`targetArn`

Das SNS-Thema oder das individuelle Gerät, an das die Pushbenachrichtigung gesendet wird

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`messageFormat`

(Optional) Das Nachrichtenformat. Amazon SNS verwendet diese Einstellung, um zu bestimmen, ob die Nutzlast analysiert werden soll und ob die relevanten plattformspezifischen Teile der Nutzlast extrahiert werden. Zulässige Werte: `JSON`, `RAW`. Standardeinstellung: `RAW`.

Unterstützt Ersatzvorlagen: Nein

`roleArn`

Die IAM-Rolle, die den Zugriff auf SNS ermöglicht. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine SNS-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "sns": {
                    "targetArn": "arn:aws:sns:us-east-2:123456789012:my_sns_topic",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_sns"
                }
            }
        ]
    }
}
```

Das folgende JSON-Beispiel definiert eine SNS-Aktion mit Ersatzvorlagen in einer Regel. AWS IoT

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "sns": {
                    "targetArn": "arn:aws:sns:us-east-1:123456789012:${topic()}",
                    "messageFormat": "JSON",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_sns"
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist Amazon Simple Notification Service? im Amazon Simple Notification Service-Entwicklerhandbuch
- Tutorial: Eine SNS Amazon-Benachrichtigung senden

## SQS

Die SQS (`sqs`) Aktion sendet Daten von einer MQTT-Nachricht an eine Amazon Simple Queue Service (Amazon SQS) Warteschlange.

> **Note**
>
> Die SQS-Aktion unterstützt keine Amazon SQS FIFO- (First-In-First-Out) Warteschlangen. Da die Regeln-Engine ein vollständig verteilter Service ist, gibt es keine Garantie für die Nachrichtenreihenfolge, wenn die SQS-Aktion ausgelöst wird.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des Vorgangs übernehmen AWS IoT kann. `sqs:SendMessage` Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.
- Wenn Sie einen AWS KMS Kunden einsetzen, der es geschafft hat AWS KMS key , ruhende Daten in Amazon SQS zu verschlüsseln, muss der Service über die Erlaubnis verfügen, den im Namen des AWS KMS key Anrufers zu verwenden. Weitere Informationen finden Sie unter Schlüsselverwaltung im Amazon Simple Queue Service Entwicklerhandbuch.

### Parameter

Wenn Sie mit dieser Aktion eine AWS IoT Regel erstellen, müssen Sie die folgenden Informationen angeben:

`queueUrl`

Die URL der Amazon SQS-Warteschlange, in die die Daten geschrieben werden Die Region in dieser URL muss nicht mit Ihrer AWS-Region AWS IoT Regel identisch sein.

> **Note**
>
> Bei AWS-Regionen Verwendung der SQS-Regelaktion können zusätzliche Gebühren für die grenzüberschreitende Datenübertragung anfallen. Weitere Informationen finden Sie unter Amazon SQS SQS-Preise.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`useBase64`

Setzen Sie diesen Parameter auf `true`, um die Regelaktion so zu konfigurieren, dass sie die Nachrichtendaten Base64-kodiert, bevor sie in die Amazon SQS-Warteschlange geschrieben werden. Standardeinstellung: `false`.

Unterstützt Ersatzvorlagen: Nein

`roleArn`

Die IAM-Rolle, die den Zugriff auf die Amazon SQS-Warteschlange ermöglicht. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine SQS-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "sqs": {
```

```
                    "queueUrl": "https://sqs.us-east-2.amazonaws.com/123456789012/
my_sqs_queue",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_sqs"
                }
            }
        ]
    }
}
```

Das folgende JSON-Beispiel definiert eine SQS-Aktion mit Ersatzvorlagen in einer Regel. AWS IoT

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "sqs": {
                    "queueUrl": "https://sqs.us-east-2.amazonaws.com/123456789012/
${topic()}",
                    "useBase64": true,
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_sqs"
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist Amazon Simple Queue Service? im Amazon Simple Queue Service-Entwicklerhandbuch?

## Step Functions

Die Aktion Step Functions (`stepFunctions`) startet eine AWS Step Functions Zustandsmaschine.

### Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung des `states:StartExecution` Vorgangs übernehmen AWS IoT kann. Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.

## Parameter

Wenn Sie eine AWS IoT Regel mit dieser Aktion erstellen, müssen Sie die folgenden Informationen angeben:

`stateMachineName`

Der Name des zu startenden Step Functions-Zustandsautomaten.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

`executionNamePrefix`

(Optional) Der Name, der der Ausführung des Zustandsautomaten gegeben wird, besteht aus diesem Präfix, gefolgt von einer UUID. Step Functions erstellt einen eindeutigen Namen für jede Zustandsautomaten-Ausführung, sofern keiner angegeben wird.

Unterstützt Ersatzvorlagen: Ja

`roleArn`

Der ARN der Rolle, die die AWS IoT Erlaubnis zum Starten der Zustandsmaschine erteilt. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

## Beispiele

Das folgende JSON-Beispiel definiert eine Step Functions Functions-Aktion in einer AWS IoT Regel.

```
{
    "topicRulePayload": {
        "sql": "SELECT * FROM 'some/topic'",
        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
```

```
            {
                "stepFunctions": {
                    "stateMachineName": "myStateMachine",
                    "executionNamePrefix": "myExecution",
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_step_functions"
                }
            }
        ]
    }
}
```

### Weitere Informationen finden Sie auch unter

- Was ist AWS Step Functions? im AWS Step Functions Developer Guide

## Timestream

Die Timestream-Regelaktion schreibt Attribute (Kennzahlen) aus einer MQTT-Nachricht in eine Amazon Timestream-Tabelle. Für weitere Informationen über Amazon Timestream, siehe Was ist Amazon Timestream?

> **Note**
>
> Amazon Timestream ist nicht in allen AWS-Region s verfügbar. Wenn Amazon Timestream in Ihrer Region nicht verfügbar ist, wird es nicht in der Liste der Regelaktionen angezeigt.

Die Attribute, die diese Regel in der Timestream-Datenbank speichert, sind diejenigen, die sich aus der Abfrageanweisung der Regel ergeben. Der Wert jedes Attributs im Ergebnis der Abfrageanweisung wird analysiert, um auf seinen Datentyp zu schließen (wie bei einer the section called “Dynamo DBv2” Aktion). Der Wert jedes Attributs wird in einen eigenen Datensatz in der Timestream-Tabelle geschrieben. Um den Datentyp eines Attributs anzugeben oder zu ändern, verwenden Sie die `cast()` Funktion in der Abfrageanweisung. Weitere Informationen zum Inhalt der einzelnen Timestream-Datensätze finden Sie unter the section called “Timestream-Datensatzinhalte”.

> **Note**
>
> Mit SQL V2 (23.03.2016) werden numerische Werte, die ganze Zahlen sind, wie z. B. `10.0`, in ihre Integer-Darstellung (`10`) umgewandelt. Sie explizit in einen `Decimal` Wert

umzuwandeln, z. B. mithilfe der Funktion cast (), verhindert dieses Verhalten nicht — das Ergebnis ist immer noch ein `Integer` Wert. Dies kann zu Typkonflikten führen, die verhindern, dass Daten in der Timestream-Datenbank aufgezeichnet werden. Um ganzzahlige numerische Werte als `Decimal` Werte zu verarbeiten, verwenden Sie SQL V1 (2015-10-08) für die Regelabfrageanweisung.

**Note**

Die maximale Anzahl von Werten, die eine Timestream-Regelaktion in eine Amazon Timestream-Tabelle schreiben kann, ist 100. Weitere Informationen finden Sie unter Amazon Timestream Quota's Referenz.

## Voraussetzungen

Diese Regelaktion hat die folgenden Anforderungen:

- Eine IAM-Rolle, die die Ausführung der `timestream:DescribeEndpoints` AND-Operationen übernehmen AWS IoT kann. `timestream:WriteRecords` Weitere Informationen finden Sie unter Gewähren Sie einer AWS IoT Regel den Zugriff, den sie benötigt.

  In der AWS IoT Konsole können Sie eine Rolle auswählen, aktualisieren oder erstellen, um die Ausführung dieser Regelaktion AWS IoT zu ermöglichen.
- Wenn Sie einen Kunden verwenden AWS KMS , um Daten im Ruhezustand in Timestream zu verschlüsseln, muss der Dienst die Erlaubnis haben, das im Namen des AWS KMS key Anrufers zu verwenden. Weitere Informationen finden Sie unter So verwenden AWS Dienste KMS. AWS

## Parameter

Wenn Sie mit dieser Aktion eine AWS IoT Regel erstellen, müssen Sie die folgenden Informationen angeben:

**`databaseName`**

Der Name einer Amazon-Timestream-Datenbank, die über die Tabelle verfügt, in der die von dieser Aktion erstellten Datensätze empfangen werden sollen. Siehe auch **`tableName`**.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

**`dimensions`**

Metadatenattribute der Zeitreihen, die in jedem Messdatensatz geschrieben werden. Beispielsweise sind der Name und die Availability Zone einer EC2 Instanz oder der Name des Herstellers einer Windturbine Dimensionen.

**`name`**

Der Name der Metadatendimension. Dies ist der Name der Spalte im Datensatz der Datenbanktabelle.

Dimensionen können nicht benannt werden: `measure_name`, `measure_value`, oder `time`. Diese Namen sind vorbehalten. Dimensionsnamen dürfen nicht mit `ts_` oder `measure_value` beginnen und dürfen keinen Doppelpunkt (`:`) enthalten.

Unterstützt Ersatzvorlagen: Nein

**`value`**

Der Wert, der in diese Spalte des Datenbankdatensatzes geschrieben werden soll.

Unterstützt Ersatzvorlagen: Ja

**`roleArn`**

Der Amazon-Ressourcenname (ARN) der Rolle, die AWS IoT die Berechtigung zum Schreiben in die Timestream-Datenbanktabelle gewährt. Weitere Informationen finden Sie unter Voraussetzungen.

Unterstützt Ersatzvorlagen: Nein

**`tableName`**

Der Name der Datenbanktabelle, in die die Messdatensätze geschrieben werden sollen. Siehe auch **`databaseName`**.

Unterstützt Ersatzvorlagen: API und nur AWS CLI

**`timestamp`**

Der Wert, der für den Zeitstempel des Eintrags verwendet werden soll. Wenn das Feld leer ist, wird die Zeit verwendet, zu der der Eintrag verarbeitet wurde.

`unit`

Die Genauigkeit des Zeitstempelwerts, die sich aus dem unter `value` beschriebenen Ausdruck ergibt.

Zulässige Werte: `SECONDS` | `MILLISECONDS` | `MICROSECONDS` | `NANOSECONDS`. Der Standardwert ist `MILLISECONDS`.

`value`

Ein Ausdruck, der einen Wert für lange Epochenzeit zurückgibt.

Sie können die the section called “time_to_epoch (Zeichenfolge, Zeichenfolge)” Funktion verwenden, um einen gültigen Zeitstempel aus einem Datums- oder Uhrzeitwert zu erstellen, der in der Nachrichtennutzlast übergeben wurde.

## Timestream-Datensatzinhalte

Die durch diese Aktion in die Amazon Timestream-Tabelle geschriebenen Daten umfassen einen Zeitstempel, Metadaten aus der Timestream-Regelaktion und das Ergebnis der Abfrageanweisung der Regel.

Für jedes Attribut (Kennzahl) im Ergebnis der Abfrageanweisung schreibt diese Regelaktion einen Datensatz mit diesen Spalten in die angegebene Timestream-Tabelle.

| Spaltenname | Attribut Typ | Wert | Kommentare |
|---|---|---|---|
| *dimension-name* | DIMENSION | Der im Aktionseintrag für die Timestream-Regel angegebene Wert. | Jede im Regelaktionseintrag angegebene Dimension erstellt eine Spalte in der Timestream-Datenbank mit dem Namen der Dimension. |
| measure_name | MEASURE_NAME | Der Name des Attributs | Der Name des Attributs im Ergebnis der Abfrageanweisung, dessen Wert in der `measure_value::` *data-type* Spalte angegeben ist. |

| Spaltenname | Attribut Typ | Wert | Kommentare |
| --- | --- | --- | --- |
| measure_value: *data-type* | MESS_WERT | Der Wert des Attributs im Ergebnis der Abfrageanweisung. Der Name des Attributs steht in der `measure_name` Spalte. | Der Wert wird interpretiert* und als die am besten geeignete Übereinst immung von: `bigint`, `boolean`, `double`, oder `varchar` gewertet. Amazon Timestream erstellt für jeden Datentyp eine separate Spalte. Der Wert in der Nachricht kann mithilfe der `cast()` Funktion in der Abfragean weisung der Regel in einen anderen Datentyp umgewande lt werden. |
| time | TIMESTAMP (ZEITSTEMPEL) | Das Datum und die Uhrzeit des Datensatz es in der Datenbank. | Dieser Wert wird von der Regel-Engine oder der `timestamp` Eigenschaft zugewiesen, sofern sie definiert ist. |

* Der aus der Nachrichtennutzlast gelesene Attributwert wird wie folgt interpretiert. Eine Veranschaulichung der einzelnen Fälle finden Sie in der the section called “Beispiele”.

- Ein Wert von `true` oder `false` ohne Anführungszeichen wird als `boolean` Typ interpretiert.
- Eine dezimale Zahl wird als `double` Typ interpretiert.
- Ein numerischer Wert ohne Dezimalpunkt wird als `bigint` Typ interpretiert.
- Eine Zeichenfolge in Anführungszeichen wird als `varchar` Typ interpretiert.

- Objekte und Array-Werte werden in JSON-Zeichenketten konvertiert und als `varchar` Typ gespeichert.

## Beispiele

Das folgende JSON-Beispiel definiert eine Timestream-Regelaktion mit einer Ersatzvorlage in einer Regel. AWS IoT

```
{
  "topicRulePayload": {
    "sql": "SELECT * FROM 'iot/topic'",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
      {
        "timestream": {
          "roleArn": "arn:aws:iam::123456789012:role/aws_iot_timestream",
          "tableName": "devices_metrics",
          "dimensions": [
            {
              "name": "device_id",
              "value": "${clientId()}"
            },
            {
              "name": "device_firmware_sku",
              "value": "My Static Metadata"
            }
          ],
          "databaseName": "record_devices"
        }
      }
    ]
  }
}
```

Die Verwendung der im vorherigen Beispiel definierten Timestream-Themenregelaktion mit der folgenden Nachrichtennutzlast führt zu den Amazon Timestream-Datensätzen, die in der folgenden Tabelle aufgeführt sind.

```
{
  "boolean_value": true,
```

```
  "integer_value": 123456789012,
  "double_value": 123.456789012,
  "string_value": "String value",
  "boolean_value_as_string": "true",
  "integer_value_as_string": "123456789012",
  "double_value_as_string": "123.456789012",
  "array_of_integers": [23,36,56,72],
  "array of strings": ["red", "green","blue"],
  "complex_value": {
    "simple_element": 42,
    "array_of_integers": [23,36,56,72],
    "array of strings": ["red", "green","blue"]
  }
}
```

In der folgenden Tabelle werden die Datenbankspalten und Datensätze angezeigt, die durch die Verwendung der angegebenen Themenregelaktion zur Verarbeitung der vorherigen Nachrichtennutzlast erstellt wurden. Die `device_firmware_sku` und `device_id` Spalten sind die DIMENSIONEN, die in der Themenregelaktion definiert sind. Die Timestream-Themenregelaktion erstellt die `time` Spalte und die `measure_name` und `measure_value::*` Spalten, die sie mit den Werten aus dem Ergebnis der Abfrageanweisung der Themenregelaktion füllt.

| device_firmware_sku | Gerät_ID | measure_name | Messwert::bigint | Messwert::varchar | Messwert::doppelt | Messwert::boolean | time |
|---|---|---|---|---|---|---|---|
| Meine statischen Metadaten | iotconsole-159 -0 EXAMPLE78 | komplexer_Wert | - | {"simple_element":42,"array_of_integers":[23,36,56,72],"array of strings":["red","green","blue"]} | - | - | 2020-08-26 22:42:16.423000000 |

| device_firmware_sku | Gerät_ID | measure_name | Messwert::bigint | Messwert::varchar | Messwert::doppelt | Messwert::boolean | time |
|---|---|---|---|---|---|---|---|
| Meine statischen Metadaten | iot-Konsole-159 -0 EXAMPLE78 | Integer_Wert_als_Zeichenfolge | - | 123456789012 | - | - | 2020-08-26 22:42:16.423000000 |
| Meine statischen Metadaten | iot-Konsole-159 -0 EXAMPLE78 | boolescher_Wert | - | - | - | TRUE | 2020-08-26 22:42:16.423000000 |
| Meine statischen Metadaten | iot-Konsole-159 -0 EXAMPLE78 | Integer_Wert | 123456789012 | - | - | - | 2020-08-26 22:42:16.423000000 |
| Meine statischen Metadaten | iot-Konsole-159 -0 EXAMPLE78 | Zeichenfolge_Wert | - | Zeichenfolge_Wert | - | - | 2020-08-26 22:42:16.423000000 |
| Meine statischen Metadaten | iot-Konsole-159 -0 EXAMPLE78 | Array_von_ganzen_Zahlen | - | [23,36,56,72] | - | - | 2020-08-26 22:42:16.423000000 |
| Meine statischen Metadaten | iot-Konsole-159 -0 EXAMPLE78 | Zeichenfolgen-Array | - | ["red","green","blue"] | - | - | 2020-08-26 22:42:16.423000000 |
| Meine statischen Metadaten | iot-Konsole-159 -0 EXAMPLE78 | boolescher_Wert_als_Zeichenfolge | - | TRUE | - | - | 2020-08-26 22:42:16.423000000 |

| device_firmware_sku | Gerät_ID | measure_name | Messwert::bigint | Messwert::varchar | Messwert::doppelt | Messwert::boolean | time |
|---|---|---|---|---|---|---|---|
| Meine statischen Metadaten | iot-Konsole-159 -0 EXAMPLE78 | doppelter_Wert | - | - | 123,456789012 | - | 2020-08-26 22:42:16.423000000 |
| Meine statischen Metadaten | IoT-Konsole-159 -0 EXAMPLE78 | doppelterWert_als_Zeichenfolge | - | 123,45679 | - | - | 2020-08-26 22:42:16.423000000 |

## Fehlerbehebung bei einer Regel

Wenn Sie ein Problem mit Ihren Regeln haben, empfehlen wir Ihnen, Logs zu aktivieren. CloudWatch Sie können Ihre Protokolle analysieren, um festzustellen, ob es sich um ein Berechtigungsproblem handelt oder ob z. B. eine WHERE-Klausel-Bedingung nicht zutraf. Weitere Informationen finden Sie unter CloudWatch Logs einrichten.

## Mithilfe von Regeln auf kontoübergreifende Ressourcen zugreifen AWS IoT

Sie können AWS IoT Regeln für den kontoübergreifenden Zugriff konfigurieren, sodass Daten, die zu MQTT-Themen eines Kontos aufgenommen wurden, an die AWS Dienste wie Amazon SQS und Lambda eines anderen Kontos weitergeleitet werden können. Im Folgenden wird erklärt, wie AWS IoT Regeln für die kontoübergreifende Datenaufnahme eingerichtet werden, und zwar von einem MQTT-Thema in einem Konto bis hin zu einem Ziel in einem anderen Konto.

Kontoübergreifende Regeln können mithilfe ressourcenbasierter Berechtigungen für die Zielressource konfiguriert werden. Daher können nur Ziele, die ressourcenbasierte Berechtigungen unterstützen, für den kontoübergreifenden Zugriff mit Regeln aktiviert werden. AWS IoT Zu den unterstützten Zielen gehören Amazon SQS, Amazon SNS, Amazon S3 und AWS Lambda.

> **Note**
>
> Für die unterstützten Ziele, mit Ausnahme von Amazon SQS, müssen Sie die Regel in derselben Weise AWS-Region wie die Ressource eines anderen Dienstes definieren, damit die Regelaktion mit dieser Ressource interagieren kann. Weitere Informationen zu AWS IoT Regelaktionen finden Sie unter AWS IoT Regelaktionen. Weitere Informationen zur SQS-Aktion einer Regel finden Sie unter???.

## Voraussetzungen

- Vertrautheit mit AWS IoT Regeln
- Ein Verständnis von IAM-Benutzern, -Rollen und ressourcenbasierten Berechtigungen
- Nach der AWS CLI Installation

## Kontoübergreifende Einrichtung für Amazon SQS

Szenario: Konto A sendet Daten aus einer MQTT-Nachricht an die Amazon SQS-Warteschlange von Konto B.

| AWS-Konto | Konto bezeichnet als | Beschreibung |
|---|---|---|
| *1111-1111-1111* | Konto A | Regelaktion: `sqs:SendMessage` |
| *2222-2222-2222* | Konto B | Amazon-SQS-Warteschlange<br>• ARN: *arn:aws:sqs:region:2222-2222-2222:ExampleQueue*<br>• URL: *https://sqs.region.amazonaws.com/2222-2222-2222/ExampleQueue* |

> **Note**
>
> Ihre Amazon SQS SQS-Zielwarteschlange muss sich nicht in derselben Warteschlange AWS-Region wie Ihre AWS IoT Regel befinden. Weitere Informationen zur SQS-Aktion der Regel finden Sie unter. ???

Erledigen der Aufgaben von Konto A

> **Hinweis**
>
> Um die folgenden Befehle auszuführen, muss Ihr IAM-Benutzer über die Berechtigung `iot:CreateTopicRule` mit dem Amazon Resource Name (ARN) der Regel als Ressource und über die Berechtigung `iam:PassRole` Aktion mit einer Ressource als ARN der Rolle verfügen.

1. Konfigurieren Sie AWS CLI unter Verwendung des IAM-Benutzers von Konto A.
2. Erstellen Sie eine IAM-Rolle, die der AWS IoT Regel-Engine vertraut, und fügen Sie eine Richtlinie hinzu, die den Zugriff auf die Amazon SQS SQS-Warteschlange von Konto B ermöglicht. Beispielbefehle und Richtliniendokumente finden Sie unter Gewährung AWS IoT des erforderlichen Zugriffs.
3. Um eine Regel zu erstellen, die an ein Thema angehängt ist, führen Sie den create-topic-rule Befehl aus.

   ```
   aws iot create-topic-rule --rule-name myRule --topic-rule-payload file://./my-rule.json
   ```

   Im Folgenden finden Sie ein Beispiel für eine Nutzlastdatei mit einer Regel, die alle an das `iot/test` Thema gesendeten Nachrichten in die angegebene Amazon SQS-Warteschlange einfügt. Die SQL-Anweisung filtert die Nachrichten und der Rollen-ARN gewährt AWS IoT die Berechtigung, die Nachricht zur Amazon SQS-Warteschlange hinzuzufügen.

   ```
   {
    "sql": "SELECT * FROM 'iot/test'",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
   ```

```
  {
   "sqs": {
    "queueUrl": "https://sqs.region.amazonaws.com/2222-2222-2222/ExampleQueue",
    "roleArn": "arn:aws:iam::1111-1111-1111:role/my-iot-role",
    "useBase64": false
   }
  }
 ]
}
```

Weitere Informationen zur Definition einer Amazon SQS-Aktion in einer AWS IoT Regel finden Sie unter AWS IoT Regelaktionen — Amazon SQS.

Erledigen der Aufgaben von Konto B

1. Konfigurieren Sie AWS CLI mithilfe des IAM-Benutzers von Konto B.
2. Um Konto A Berechtigungen für die Amazon SQS-Warteschlangenressource zu erteilen, führen Sie den Befehl add-permission aus.

```
aws sqs add-permission --queue-url https://sqs.region.amazonaws.com/2222-2222-2222/ExampleQueue --label SendMessagesToMyQueue --aws-account-ids 1111-1111-1111 --actions SendMessage
```

## Kontoübergreifende Einrichtung für Amazon SNS

Szenario: Konto A sendet Daten von einer MQTT-Nachricht an ein Amazon SNS Thema von Konto B.

| AWS-Konto | Konto bezeichnet als | Beschreibung |
|---|---|---|
| *1111-1111-1111* | Konto A | Regelaktion: `sns:Publish` |
| *2222-2222-2222* | Konto B | ARN des Amazon-SNS-Themas: *arn:aws:sns:region:2222-2222-2222:ExampleTopic* |

Erledigen der Aufgaben von Konto A

> **Hinweise**
>
> Um die folgenden Befehle auszuführen, sollte Ihr IAM-Benutzer über Berechtigungen für die `iot:CreateTopicRule` Regel ARN als Ressource und über Berechtigungen für die `iam:PassRole` Aktion mit einer Ressource als Rolle ARN verfügen.

1. Konfigurieren Sie AWS CLI unter Verwendung des IAM-Benutzers von Konto A.
2. Erstellen Sie eine IAM-Rolle, die der AWS IoT Regel-Engine vertraut, und fügen Sie eine Richtlinie hinzu, die den Zugriff auf das Amazon SNS SNS-Thema von Konto B ermöglicht. Befehle und Richtliniendokumente finden Sie beispielsweise unter Gewährung AWS IoT des erforderlichen Zugriffs.
3. Um eine Regel zu erstellen, die an ein Thema angehängt ist, führen Sie den create-topic-rule Befehl aus.

   ```
   aws iot create-topic-rule --rule-name myRule --topic-rule-payload file://./my-rule.json
   ```

   Im Folgenden finden Sie ein Beispiel für eine Nutzlastdatei mit einer Regel, die alle an das `iot/test` Thema gesendeten Nachrichten in die angegebene -Amazon SNS Thema einfügt. Die SQL-Anweisung filtert die Nachrichten, und die Rollen-ARN gewährt AWS IoT Berechtigungen zum Senden der Nachricht an das Amazon SNS Thema.

   ```
   {
    "sql": "SELECT * FROM 'iot/test'",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
     {
      "sns": {
       "targetArn": "arn:aws:sns:region:2222-2222-2222:ExampleTopic",
       "roleArn": "arn:aws:iam::1111-1111-1111:role/my-iot-role"
      }
     }
    ]
   }
   ```

Weitere Informationen zur Definition einer Amazon SNS-Aktion in einer AWS IoT Regel finden Sie unter AWS IoT Regelaktionen — Amazon SNS.

Erledigen der Aufgaben von Konto B

1. Konfigurieren Sie AWS CLI mithilfe des IAM-Benutzers von Konto B.
2. Um Konto A die Erlaubnis für die Amazon SNS-Themenressource zu erteilen, führen Sie den Befehl add-permission aus.

```
aws sns add-permission --topic-arn arn:aws:sns:region:2222-2222-2222:ExampleTopic
 --label Publish-Permission --aws-account-id 1111-1111-1111 --action-name Publish
```

## Kontoübergreifende Einrichtung für Amazon S3

Szenario: Konto A sendet Daten von einer MQTT-Nachricht an einen Amazon-S3-Bucket von Konto B.

| AWS-Konto | Konto bezeichnet als | Beschreibung |
|---|---|---|
| *1111-1111-1111* | Konto A | Regelaktion: `s3:PutObject` |
| *2222-2222-2222* | Konto B | Amazon S3-Bucket ARN: *arn:aws:s3:::amzn-s3-demo-bucket* |

Erledigen der Aufgaben von Konto A

> **Hinweis**
>
> Um die folgenden Befehle auszuführen, sollte Ihr IAM-Benutzer über Berechtigungen für `iot:CreateTopicRule` mit der Regel ARN als Ressource und über Berechtigungen für `iam:PassRole` Aktionen mit einer Ressource als Rolle ARN verfügen.

1. Konfigurieren Sie AWS CLI unter Verwendung des IAM-Benutzers von Konto A.

2. Erstellen Sie eine IAM-Rolle, die der AWS IoT Regel-Engine vertraut, und fügen Sie eine Richtlinie hinzu, die den Zugriff auf den Amazon S3 S3-Bucket von Konto B ermöglicht. Befehle und Richtliniendokumente finden Sie beispielsweise unter Gewährung AWS IoT des erforderlichen Zugriffs.
3. Führen Sie den create-topic-rule Befehl aus, um eine Regel zu erstellen, die an Ihren Ziel-S3-Bucket angehängt ist.

   ```
   aws iot create-topic-rule --rule-name my-rule --topic-rule-payload file://./my-rule.json
   ```

   Im Folgenden finden Sie ein Beispiel für eine Nutzlastdatei mit einer Regel, die alle an das `iot/test` Thema gesendeten Nachrichten in den angegebenen Amazon S3-Bucket einfügt. Die SQL-Anweisung filtert die Nachrichten und der Rollen-ARN gewährt AWS IoT die Berechtigung zum Hinzufügen der Nachricht zum Amazon S3-Bucket.

   ```
   {
    "sql": "SELECT * FROM 'iot/test'",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
     {
      "s3": {
       "bucketName": "amzn-s3-demo-bucket",
       "key": "${topic()}/${timestamp()}",
       "roleArn": "arn:aws:iam::1111-1111-1111:role/my-iot-role"
      }
     }
    ]
   }
   ```

   Weitere Informationen zur Definition einer Amazon S3-Aktion in einer AWS IoT Regel finden Sie unter AWS IoT Regelaktionen — Amazon S3.

Erledigen der Aufgaben von Konto B

1. Konfigurieren Sie AWS CLI mithilfe des IAM-Benutzers von Konto B.
2. Erstellen Sie eine Bucket-Richtlinie, die dem Prinzipal von Konto A vertraut.

Im Folgenden finden Sie ein Beispiel für eine Payload-Datei, die eine Bucket-Richtlinie definiert, die dem Prinzipal eines anderen Kontos vertraut.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AddCannedAcl",
   "Effect": "Allow",
   "Principal": {
    "AWS": [
     "arn:aws:iam::1111-1111-1111:root"
    ]
   },
   "Action": "s3:PutObject",
   "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
  }
 ]
}
```

Weitere Informationen finden Sie unter Beispiele für Bucket-Richtlinien.

3. Um die Bucket-Richtlinie an den angegebenen Bucket anzuhängen, führen Sie den put-bucket-policy Befehl aus.

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://./amzn-s3-demo-bucket-policy.json
```

4. Damit der kontoübergreifende Zugriff funktioniert, stellen Sie sicher, dass Sie die richtigen Einstellungen für Blockieren des gesamten öffentlichen Zugangs ausgewählt haben. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit in Amazon S3.

## Kontoübergreifende Einrichtung für AWS Lambda

Szenario: Konto A ruft eine AWS Lambda Funktion von Konto B auf und übergibt eine MQTT-Nachricht.

| AWS-Konto | Konto bezeichnet als | Beschreibung |
| --- | --- | --- |
| *1111-1111-1111* | Konto A | Regelaktion: `lambda:InvokeFunction` |
| *2222-2222-2222* | Konto B | ARN der Lambda-Funktion: *arn:aws:lambda:region:2222-2222-2222:function:example-function* |

Erledigen der Aufgaben von Konto A

> **Hinweise**
>
> Um die folgenden Befehle ausführen zu können, sollte Ihr IAM-Benutzer über Berechtigungen für `iot:CreateTopicRule` mit der Regel ARN als Ressource und über Berechtigungen für `iam:PassRole` Aktionen mit der Ressource als Rolle ARN verfügen.

1. Konfigurieren Sie AWS CLI unter Verwendung des IAM-Benutzers von Konto A.
2. Führen Sie den create-topic-rule Befehl aus, um eine Regel zu erstellen, die den kontoübergreifenden Zugriff auf die Lambda-Funktion von Konto B definiert.

   ```
   aws iot create-topic-rule --rule-name my-rule --topic-rule-payload file://./my-rule.json
   ```

   Im Folgenden finden Sie ein Beispiel für eine Nutzlastdatei mit einer Regel, die alle an das `iot/test` Thema gesendeten Nachrichten in die angegebene Lambda-Funktion einfügt. Die SQL-Anweisung filtert die Nachrichten und die Rolle ARN erteilt AWS IoT die Berechtigung, die Daten an die Lambda-Funktion zu übergeben.

   ```
   {
    "sql": "SELECT * FROM 'iot/test'",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
     {
      "lambda": {
       "functionArn": "arn:aws:lambda:region:2222-2222-2222:function:example-function"
   ```

```
    }
   }
  ]
}
```

Weitere Informationen zum Definieren einer AWS Lambda Aktion in einer AWS IoT Regel finden Sie unter AWS IoT Regelaktionen — Lambda.

Erledigen der Aufgaben von Konto B

1. Konfigurieren Sie AWS CLI mithilfe des IAM-Benutzers von Konto B.
2. Führen Sie den Befehl add-permission von Lambda aus, um AWS IoT Regeln die Erlaubnis zur Aktivierung der Lambda-Funktion zu erteilen. Um den folgenden Befehl auszuführen, sollte Ihr IAM-Benutzer über die entsprechende Berechtigung für `lambda:AddPermission` Aktion verfügen.

```
aws lambda add-permission --function-name example-function --region us-east-1 --
principal iot.amazonaws.com --source-arn arn:aws:iot:region:1111-1111-1111:rule/
example-rule --source-account 1111-1111-1111 --statement-id "unique_id" --action
 "lambda:InvokeFunction"
```

Optionen:

--Prinzipal

Dieses Feld gibt AWS IoT (dargestellt durch`iot.amazonaws.com`) die Erlaubnis, die Lambda-Funktion aufzurufen.

--source-arn

Dieses Feld bestätigt, dass diese Lambda-Funktion nur `arn:aws:iot:region:1111-1111-1111:rule/example-rule` in AWS IoT Triggern und keine andere Regel in demselben oder einem anderen Konto diese Lambda-Funktion aktivieren kann.

--source-account

Dieses Feld bestätigt, dass diese Lambda-Funktion nur im Namen des `1111-1111-1111` Kontos AWS IoT aktiviert wird.

> **Hinweise**
>
> Wenn Sie in der Konsole Ihrer AWS Lambda Funktion unter Konfiguration die Fehlermeldung „Die Regel konnte nicht gefunden werden“ sehen, ignorieren Sie die Fehlermeldung und fahren Sie mit dem Testen der Verbindung fort.

# Fehlerbehandlung (Fehleraktion)

Wenn eine Nachricht von einem Gerät AWS IoT empfangen wird, prüft die Regel-Engine, ob die Nachricht einer Regel entspricht. Ist dies der Fall, wird die Abfrageanweisung der Regel evaluiert und die Aktionen der Regel aktiviert. Dabei wird das Ergebnis der Abfrageanweisung übergeben.

Wenn bei der Aktivierung einer Aktion ein Problem auftritt, aktiviert die Regel-Engine eine Fehleraktion, falls eine solche für die Regel angegeben ist. Dies kann der Fall sein, wenn:

- Eine Regel verfügt nicht über die Berechtigung, auf einen Amazon S3-Bucket zuzugreifen.
- Ein Benutzerfehler führt dazu, dass der für DynamoDB bereitgestellte Durchsatz überschritten wird.

> **Note**
>
> Die in diesem Thema behandelte Fehlerbehandlung bezieht sich auf Regelaktionen. Um SQL-Probleme, einschließlich externer Funktionen, zu debuggen, können Sie die AWS IoT Protokollierung einrichten. Weitere Informationen finden Sie unter ???.

## Nachrichtenformat für Fehleraktion

Eine einzelne Nachricht wird pro Regel und Nachricht generiert. Wenn beispielsweise zwei Regelaktionen in derselben Regel fehlschlagen, empfängt die Fehleraktion eine Nachricht, die beide Fehler enthält.

Die Fehlermeldung der Aktion kann in etwa wie im folgenden Beispiel aussehen.

```
{
  "ruleName": "TestAction",
  "topic": "testme/action",
```

```
  "cloudwatchTraceId": "7e146a2c-95b5-6caf-98b9-50e3969734c7",
  "clientId": "iotconsole-1511213971966-0",
  "base64OriginalPayload":
 "ewogICJtZXNzYWdlIjogIkhlbGxvIHZyb20gQVdTIElvVCBjb25zb2xlIgp9",
  "failures": [
    {
      "failedAction": "S3Action",
      "failedResource": "us-east-1-s3-verify-user",
      "errorMessage": "Failed to put S3 object. The error received was The
 specified bucket does not exist (Service: Amazon S3; Status Code: 404; Error
 Code: NoSuchBucket; Request ID: 9DF5416B9B47B9AF; S3 Extended Request ID:
 yMah1cwPhqTH267QLPhTKeVPKJB8BO5ndBHzOmWtxLTM6uAvwYYuqieAKyb6qRPTxP1tHXCoR4Y=).
 Message arrived on: error/action, Action: s3, Bucket: us-
east-1-s3-verify-user, Key: \"aaa\". Value of x-amz-id-2:
 yMah1cwPhqTH267QLPhTKeVPKJB8BO5ndBHzOmWtxLTM6uAvwYYuqieAKyb6qRPTxP1tHXCoR4Y="
    }
  ]
}
```

ruleName

Der Name der Regel, die die Fehleraktion ausgelöst hat.

Thema

Das Thema, in dem die ursprüngliche Nachricht empfangen wurde.

cloudwatchTraceId

Eine eindeutige Identität, die sich auf den Fehler bezieht, meldet sich an CloudWatch.

clientId

Die Client-ID des Herausgebers der Nachricht.

Base64 OriginalPayload

Die ursprüngliche Nachrichtennutzlast, Base64-kodiert.

failures

failedAction

Der Name der Aktion, die nicht abgeschlossen werden konnte (z. B. „S3Action”).

failedResource

Der Name der Ressource (z. B. der Name eines S3-Buckets).

errorMessage

Die Beschreibung und Erläuterung des Fehlers.

## Beispiel für Fehleraktion

Hier finden Sie ein Beispiel für eine Regel, der eine Fehleraktion hinzugefügt wurde. Die folgende Regel weist eine Aktion, die Nachrichtendaten in eine DynamoDB-Tabelle schreibt, und eine Fehleraktion auf, die Daten in einen Amazon S3-Bucket schreibt:

```
{
    "sql" : "SELECT * FROM ..."
    "actions" : [{
        "dynamoDB" : {
            "table" : "PoorlyConfiguredTable",
            "hashKeyField" : "AConstantString",
            "hashKeyValue" : "AHashKey"}}
    ],
    "errorAction" : {
        "s3" : {
            "roleArn": "arn:aws:iam::123456789012:role/aws_iot_s3",
            "bucketName" : "message-processing-errors",
            "key" : "${replace(topic(), '/', '-') + '-' + timestamp() + '-' +
 newuuid()}"
        }
    }
}
```

Sie können jede Funktion oder Ersetzungsvorlage in der SQL-Anweisung einer Fehleraktion verwenden, einschließlich der externen Funktionen: `aws_lambda()`, `get_dynamodb()`, `get_thing_shadow()`, `get_secret()machinelearning_predict()`, und `decode()`. Wenn eine Fehleraktion den Aufruf einer externen Funktion erfordert, kann der Aufruf der Fehleraktion zu einer zusätzlichen Rechnung für die externe Funktion führen.

Die folgenden externen Funktionen werden äquivalent zu einer Regelaktion abgerechnet: `aws_lambdaget_dynamodb()`, und. `get_thing_shadow()` Außerdem wird Ihnen die `decode()` Funktion nur dann in Rechnung gestellt, wenn Sie eine Protobuf-Nachricht in JSON dekodieren. Weitere Informationen finden Sie auf der AWS IoT Core Seite mit den Preisen.

Weitere Informationen zu Regeln und zur Angabe einer Fehleraktion finden Sie unter AWS IoT Regel erstellen.

Weitere Informationen CloudWatch zur Überwachung des Erfolgs oder Fehlers von Regeln finden Sie unterAWS IoT Metriken und Dimensionen.

## Senken der Messaging-Kosten mit Basic Ingest

Sie können Basic Ingest verwenden, um Gerätedaten sicher an den AWS-Services Support von zu sendenAWS IoT Regelaktionen, ohne dass Messaging-Kosten anfallen. Basic Ingest optimiert den Datenfluss durch Entfernen der Message Broker für Veröffentlichungen/Abonnements aus dem Aufnahmepfad.

Basic Ingest kann Nachrichten von Ihren Geräten oder Anwendungen senden. Die Nachrichten verfügen über Themennamen, die für die ersten drei Ebenen mit `$aws/rules/`*`rule_name`* beginnen, wobei *`rule_name`* der Name der AWS IoT -Regel ist, die Sie aufrufen möchten.

Sie können eine vorhandene Regel mit Basic Ingest verwenden, indem Sie das Basic Ingest-Präfix (`$aws/rules/`*`rule_name`*) dem Nachrichtenthema hinzufügen, mit dem Sie die Regel normalerweise aufrufen. Wenn Sie beispielsweise eine Regel mit dem Namen `BuildingManager` haben, die bei Nachrichten mit Themen wie `Buildings/Building5/Floor2/Room201/Lights` (`"sql": "SELECT * FROM 'Buildings/#'"`) aufgerufen wird, können Sie dieselbe Regel mit Basic Ingest durch Senden einer Nachricht mit dem Thema `$aws/rules/BuildingManager/Buildings/Building5/Floor2/Room201/Lights` aufrufen.

> **Note**
>
> - Ihre Geräte und Regeln können keine reservierten Basic Ingest-Themen abonnieren. Beispielsweise werden die AWS IoT Device Defender `num-messages-received` Metriken nicht ausgegeben, da sie das Abonnieren von Themen nicht unterstützen. Weitere Informationen finden Sie unter Reservierte Themen.
> - Wenn Sie einen Publish/Subscribe-Broker benötigen, um Nachrichten an mehrere Abonnenten zu verteilen (z. B. um Nachrichten an andere Geräte und die Rules Engine zu übermitteln), sollten Sie weiterhin den AWS IoT Message Broker für die Nachrichtenverteilung verwenden. Stellen Sie jedoch sicher, dass Sie Ihre Nachrichten zu anderen Themen als Basic Ingest-Themen veröffentlichen.

# Verwenden von Basic Ingest

Stellen Sie vor der Verwendung von Basic Ingest sicher, dass Ihr Gerät oder Ihre Anwendung eine Richtlinie mit Veröffentlichungsberechtigungen auf `$aws/rules/*` nutzt. Oder Sie können in der Richtlinie Berechtigungen für einzelne Regeln angeben. `$aws/rules/rule_name/*` Andernfalls können Ihre Geräte und Anwendungen weiterhin ihre bestehenden Verbindungen mit AWS IoT Core nutzen.

Wenn die Nachricht die Regel-Engine erreicht, besteht kein Unterschied hinsichtlich der Implementierung oder Fehlerbehandlung zwischen von Basic Ingest und von Message Broker-Abonnements aufgerufenen Regeln.

Sie können Regeln für die Verwendung mit Basic Ingest erstellen. Beachten Sie Folgendes:

- Das erste Präfix eines Basic Ingest-Themas (`$aws/rules/rule_name`) ist für die topic(Decimal)-Funktion nicht verfügbar.
- Wenn Sie eine Regel definieren, die nur mit Basic Ingest aufgerufen wird, ist die `FROM`-Klausel im `sql`-Feld der `rule`-Definition optional. Sie ist weiterhin erforderlich, wenn die Regel auch von anderen Regeln aufgerufen wird, die über den Message Broker gesendet werden müssen (etwa weil diese anderen Nachrichten an mehrere Abonnenten verteilt werden müssen). Weitere Informationen finden Sie unter AWS IoT SQL-Referenz.
- Die ersten drei Ebenen des Basic Ingest-Themas (`$aws/rules/rule_name`) zählen nicht für die Längenbeschränkung von 8 Segmenten oder von insgesamt 256 Zeichen für ein Thema. Davon abgesehen gelten dieselben Einschränkungen, wie in den AWS IoT -Einschränkungen dokumentiert.
- Wenn eine Nachricht mit einem Basic Ingest-Thema empfangen wird, das eine inaktive Regel oder eine Regel angibt, die nicht existiert, wird ein Fehlerprotokoll in einem CloudWatch Amazon-Protokoll erstellt, das Ihnen beim Debuggen hilft. Weitere Informationen finden Sie unter Protokolleinträge zur Regel-Engine. Es wird eine `RuleNotFound`-Metrik angezeigt, und Sie können dafür Alarme erstellen. Weitere Informationen finden Sie unter „Regelmetriken“ in Regelmetriken.
- Sie können nach wie vor mit QoS 1 auf Basic Ingest-Themen veröffentlichen. Sie erhalten eine, PUBACK nachdem die Nachricht erfolgreich an die Regel-Engine übermittelt wurde. Der Empfang einer PUBACK bedeutet nicht, dass Ihre Regelaktionen erfolgreich abgeschlossen wurden. Sie können bei der Ausführung einer Aktion eine Fehleraktion zur Fehlerbehebung konfigurieren. Weitere Informationen finden Sie unter Fehlerbehandlung (Fehleraktion).

# AWS IoT SQL-Referenz

AWS IoT In werden Regeln mit einer SQL-ähnlichen Syntax definiert. SQL-Anweisungen bestehen aus drei Typen von Klauseln:

SELECT

(Erforderlich) Extrahiert Informationen aus der Nutzlast einer eingehenden Nachricht und führt Veränderungen an den Informationen durch. Die zu verwendenden Nachrichten werden durch den in der FROM-Klausel angegebenen Themenfilter identifiziert.

Die SELECT-Klausel unterstützt Datentypen, Operatoren, Funktionen, Literale, Case-Anweisungen, JSON-Erweiterungen, Ersetzungsvorlagen Verschachtelte Objektabfragen und Binäre Nutzlasten.

FROM

Der MQTT-Themenfilter, der Nachrichten identifiziert, aus denen Daten extrahiert werden sollen. Die Regel wird für jede Meldung aktiviert, die an ein MQTT-Topic gesendet wird, das dem hier angegebenen Themenfilter entspricht. Erforderlich für Regeln, die durch Meldungen aktiviert werden, die den Message Broker durchlaufen. Optional für Regeln, die nur unter Verwendung von Basic Ingest ausgelöst werden.

WHERE

(Optional) Fügt eine Bedingungslogik hinzu, die bestimmt, ob die von einer Regel angegebenen Aktionen ausgeführt werden.

Die WHERE-Klausel unterstützt Datentypen, Operatoren, Funktionen, Literale, Case-Anweisungen, JSON-Erweiterungen, Ersetzungsvorlagen und Verschachtelte Objektabfragen.

Ein Beispiel für eine SQL-Anweisung sieht folgendermaßen aus:

```
SELECT color AS rgb FROM 'topic/subtopic' WHERE temperature > 50
```

Ein Beispiel für eine MQTT-Nachricht (auch eingehende Nutzlast genannt) sieht folgendermaßen aus:

```
{
    "color":"red",
    "temperature":100
```

```
}
```

Wenn diese Nachricht im Topic `'topic/subtopic'` veröffentlicht wird, wird die Regel ausgelöst und die SQL-Anweisung wird ausgewertet. Die SQL-Anweisung extrahiert den Wert der Eigenschaft `color`, wenn die Eigenschaft `"temperature"` größer als 50 ist. Die WHERE-Klausel legt die Bedingung `temperature > 50` fest. Das Schlüsselwort `AS` benennt die Eigenschaft `"color"` in `"rgb"` um. Das Ergebnis (auch ausgehende Nutzlast genannt) sieht folgendermaßen aus:

```
{
    "rgb":"red"
}
```

Diese Daten werden anschließend an die Regelaktion weitergeleitet, die die Daten für eine weitere Verarbeitung versendet. Weitere Informationen zu Regelaktionen unter AWS IoT Regelaktionen.

> **Note**
>
> Kommentare werden derzeit in der AWS IoT SQL-Syntax nicht unterstützt.
> Attributnamen mit Leerzeichen können nicht als Feldnamen in der SQL-Anweisung verwendet werden. Die eingehende Nutzlast kann zwar Attributnamen mit Leerzeichen enthalten, solche Namen können jedoch nicht in der SQL-Anweisung verwendet werden. Sie werden jedoch an die ausgehende Nutzlast weitergegeben, wenn Sie einen Platzhalter (*) für den Feldnamen verwenden.

## SELECT-Klausel

Die AWS IoT SELECT-Klausel entspricht im Wesentlichen der ANSI SQL SELECT-Klausel, mit einigen geringfügigen Unterschieden.

Die SELECT-Klausel unterstützt Datentypen, Operatoren, Funktionen, Literale, Case-Anweisungen, JSON-Erweiterungen, Ersetzungsvorlagen, Verschachtelte Objektabfragen und Binäre Nutzlasten.

Sie können die SELECT-Klausel verwenden, um Informationen aus eingehenden MQTT-Nachrichten zu extrahieren. Sie können `SELECT *` auch zum Abrufen der gesamten Nutzlast einer eingehenden Nachricht verwenden. Zum Beispiel:

```
Incoming payload published on topic 'topic/subtopic': {"color":"red", "temperature":50}
```

```
SQL statement: SELECT * FROM 'topic/subtopic'
Outgoing payload: {"color":"red", "temperature":50}
```

Wenn die Nutzlast ein JSON-Objekt ist, können Sie auf Schlüssel im Objekt verweisen. die ausgehende Nutzlast enthält das Schlüssel-Wert-Paar. Zum Beispiel:

```
Incoming payload published on topic 'topic/subtopic': {"color":"red", "temperature":50}
SQL statement: SELECT color FROM 'topic/subtopic'
Outgoing payload: {"color":"red"}
```

Sie können Schlüssel mithilfe des Schlüsselworts „AS“ umbenennen. Zum Beispiel:

```
Incoming payload published on topic 'topic/subtopic':{"color":"red", "temperature":50}
SQL:SELECT color AS my_color FROM 'topic/subtopic'
Outgoing payload: {"my_color":"red"}
```

Sie können mehrere Elemente durch ein Komma getrennt auswählen. Zum Beispiel:

```
Incoming payload published on topic 'topic/subtopic': {"color":"red", "temperature":50}
SQL: SELECT color as my_color, temperature as fahrenheit FROM 'topic/subtopic'
Outgoing payload: {"my_color":"red","fahrenheit":50}
```

Sie können mehrere Elemente auswählen, indem Sie „*“ einbeziehen, um die Elemente zur eingehenden Nutzlast hinzuzufügen. Zum Beispiel:

```
Incoming payload published on topic 'topic/subtopic': {"color":"red", "temperature":50}
SQL: SELECT *, 15 as speed FROM 'topic/subtopic'
Outgoing payload: {"color":"red", "temperature":50, "speed":15}
```

Sie können das Schlüsselwort `"VALUE"` verwenden, um ausgehende Nutzlasten zu erzeugen, die keine JSON-Objekte sind. Mit der SQL-Version `2015-10-08` können Sie nur ein Element auswählen. Mit der SQL-Version `2016-03-23` oder höher können Sie auch ein Array auswählen, das als Objekt der obersten Ebene ausgegeben werden soll.

Example

```
Incoming payload published on topic 'topic/subtopic': {"color":"red", "temperature":50}
SQL: SELECT VALUE color FROM 'topic/subtopic'
Outgoing payload: "red"
```

Mit der Syntax `'.'` können Sie verschachtelte JSON-Objekte in der eingehenden Nutzlast analysieren. Zum Beispiel:

```
Incoming payload published on topic 'topic/subtopic': {"color":
{"red":255,"green":0,"blue":0}, "temperature":50}
SQL: SELECT color.red as red_value FROM 'topic/subtopic'
Outgoing payload: {"red_value":255}
```

Informationen über die Verwendung von JSON-Objekt- und Eigenschaftsnamen, die reservierte Zeichen wie Zahlen oder den Bindestrich (Minuszeichen) enthalten, unter JSON-Erweiterungen

Mit Funktionen (siehe Funktionen) können Sie die eingehende Nutzlast umwandeln. Sie können Klammern zum Gruppieren verwenden. Zum Beispiel:

```
Incoming payload published on topic 'topic/subtopic': {"color":"red", "temperature":50}
SQL: SELECT (temperature - 32) * 5 / 9 AS celsius, upper(color) as my_color FROM
 'topic/subtopic'
Outgoing payload: {"celsius":10,"my_color":"RED"}
```

## FROM-Klausel

Die FROM-Klausel abonniert für die Regel ein Thema oder einen Themenfilter. Schließen Sie das Thema oder den Themenfilter in einfache Anführungszeichen (') ein. Die Regel wird für jede Nachricht ausgelöst, die an ein MQTT-Topic gesendet wird, das mit dem hier angegebenen Topic-Filter übereinstimmt. Sie können eine Gruppe ähnlicher Themen mithilfe eines Themenfilters abonnieren.

Beispiel:

Eingehende Nutzlast veröffentlicht für Topic `'topic/subtopic'`: `{temperature: 50}`

Eingehende Nutzlast veröffentlicht für Topic `'topic/subtopic-2'`: `{temperature: 50}`

SQL: `"SELECT temperature AS t FROM 'topic/subtopic'"`.

Die Regel wird für `'topic/subtopic'` abonniert, daher wird die eingehende Nutzlast an die Regel übergeben. Die ausgehende Nutzlast, die an die Regelaktionen übergeben wird, lautet: `{t: 50}`. Die Regel hat `'topic/subtopic-2'` nicht abonniert, sodass die Regel nicht für die Nachricht ausgelöst wird, die für `'topic/subtopic-2'` veröffentlicht wird.

Beispiel:# Platzhalter

Sie können das Platzhalterzeichen „#“ (mehrere Ebenen) verwenden, um mehrere bestimmte Pfadelemente abzugleichen.

Eingehende Nutzlast veröffentlicht für Topic `'topic/subtopic'`: `{temperature: 50}`

Eingehende Nutzlast veröffentlicht für Topic `'topic/subtopic-2'`: `{temperature: 60}`

Eingehende Nutzlast veröffentlicht für Topic `'topic/subtopic-3/details'`: `{temperature: 70}`

Eingehende Nutzlast veröffentlicht für Topic `'topic-2/subtopic-x'`: `{temperature: 80}`

SQL: `"SELECT temperature AS t FROM 'topic/#'"`.

Die Regel abonniert jedes Thema, das mit 1 beginnt. Sie wird also dreimal ausgeführt`'topic'`, wobei ausgehende Nutzdaten von `{t: 50}` (für Thema/Unterthema), (für Thema/Unterthema), (für Thema/Unterthema-2) und `{t: 60}` (für) für ihre Aktionen gesendet werden. `{t: 70}` topic/subtopic-3/details Sie wird nicht auf `'topic-2/subtopic-x'` abonniert, so dass die Regel nicht für die `{temperature: 80}`-Nachricht ausgelöst wird.

Beispiel: +-Platzhalter

Sie können das Platzhalterzeichen „+“ (einzelne Ebene) verwenden, um ein beliebiges Pfadelement abzugleichen:

Eingehende Nutzlast veröffentlicht für Topic `'topic/subtopic'`: `{temperature: 50}`

Eingehende Nutzlast veröffentlicht für Topic `'topic/subtopic-2'`: `{temperature: 60}`

Eingehende Nutzlast veröffentlicht für Topic `'topic/subtopic-3/details'`: `{temperature: 70}`

Eingehende Nutzlast veröffentlicht für Topic `'topic-2/subtopic-x'`: `{temperature: 80}`

SQL: `"SELECT temperature AS t FROM 'topic/+'"`.

Für die Regel sind alle Topics mit zwei Pfadelementen abonniert, bei denen `'topic'` das erste Element ist. Die Regel wird für Nachrichten ausgeführt, die an `'topic/subtopic'` und `'topic/`

`subtopic-2'` gesendet werden, aber nicht an `'topic/subtopic-3/details'` (sie hat mehr Ebenen als der Themenfilter) oder `'topic-2/subtopic-x'` (sie beginnt nicht mit `topic`).

## WHERE-Klausel

Die WHERE-Klausel bestimmt, ob die durch eine Regel angegeben Aktionen ausgeführt werden. Wenn die WHERE-Klausel wahr ist, werden die Regelaktionen ausgeführt. Andernfalls werden die Regelaktionen nicht ausgeführt.

Die WHERE-Klausel unterstützt Datentypen, Operatoren, Funktionen, Literale, Case-Anweisungen, JSON-Erweiterungen, Ersetzungsvorlagen und Verschachtelte Objektabfragen.

Beispiel:

Eingehende Nutzlast veröffentlicht für `topic/subtopic`: `{"color":"red", "temperature":40}`

SQL: `SELECT color AS my_color FROM 'topic/subtopic' WHERE temperature > 50 AND color <> 'red'`.

In diesem Fall wird die Regel ausgelöst. Die durch die Regel angegebenen Aktionen werden jedoch nicht ausgeführt. Es gibt keine ausgehende Nutzlast.

In der WHERE-Klausel können Sie Funktionen und Operatoren verwenden. Sie können jedoch nicht auf Aliase verweisen, die in SELECT mit dem Schlüsselwort AS erstellt wurden. Die WHERE-Klausel wird zuerst ausgewertet, um zu bestimmen, ob SELECT ausgewertet wurde.

Beispiel mit Nicht-JSON-Nutzdaten:

Eingehende Nicht-JSON-Nutzdaten, veröffentlicht unter `topic/subtopic`: `80`

SQL: `` `SELECT decode(encode(*, 'base64'), 'base64') AS value FROM 'topic/subtopic' WHERE decode(encode(*, 'base64'), 'base64') > 50 ``

In diesem Fall wird die Regel ausgelöst und durch die Regel angegebene Aktionen werden ausgeführt. Die ausgehende Nutzlast wird durch die SELECT-Klausel in eine JSON-Nutzlast umgewandelt. `{"value":80}`

## Datentypen

Die AWS IoT Regel-Engine unterstützt alle JSON-Datentypen.

Unterstützte Datentypen

| Typ | Bedeutung |
| --- | --- |
| `Int` | Eine separate `Int`. Maximal 34 Ziffern. |
| `Decimal` | Ein `Decimal`-Wert mit genau 34 Zeichen mit einer Mindestgröße von 1E-999 (nicht Null) und einer Maximalgröße von 9.999...E999.<br><br>**Note**<br>Einige Funktionen geben `Decimal`-Werte mit doppelter Genauigkeit anstelle von genau 34 Zeichen aus. Mit SQL V2 (23.03.2016) werden numerische Werte, die ganze Zahlen sind, wie z. B.`10.0`, als `Int` Wert (`10`) statt als erwarteter `Decimal` Wert () verarbeitet. `10.0` Um ganzzahlige numerische Werte zuverlässig als `Decimal`-Werte zu verarbeiten, verwenden Sie SQL V1 (2015-10-08) für die Regelabfrageanweisung. |
| `Boolean` | `True` oder `False`. |
| `String` | Eine UTF-8-Zeichenfolge |
| `Array` | Eine Serie von Werten, die nicht den gleichen Typ aufweisen müssen |
| `Object` | Ein JSON-Wert, der aus einem Schlüssel und einem Wert besteht. Schlüssel müssen Zeichenfolgen sein. Werte können jeden Typ aufweisen. |
| `Null` | `Null` wie von JSON definiert. Dies ist ein tatsächlicher Wert, der die Abwesenheit eines |

| Typ | Bedeutung |
| --- | --- |
| | Werts darstellt. Sie können einen `Null`-Wert explizit erstellen, indem Sie das Schlüssel wort `Null` in Ihrer SQL-Anweisung verwenden . Beispiel: `"SELECT NULL AS n FROM 'topic/subtopic'"` |
| `Undefined` | Kein Wert. Dies kann in JSON nicht explizit dargestellt werden, außer durch Auslassen des Werts. Z. B. im Objekt `{"foo": null}` gibt der Schlüssel "foo" NULL zurück, der Schlüssel "bar" jedoch `Undefined` . Intern behandelt die SQL-Sprache `Undefined` als Wert, kann jedoch nicht in JSON dargestellt werden. Bei einer Serialisierung in JSON sind die Ergebniss e daher `Undefined` .<br>`{"foo":null, "bar":undefined}`<br>wird in JSON serialisiert als:<br>`{"foo":null}`<br>Dementsprechend wird `Undefined` in eine leere Zeichenfolge konvertiert, wenn es selbst konvertiert wird. Funktionen, die mit ungültige n Argumenten aufgerufen werden (z. B. falsche Typen, falsche Anzahl an Argumenten usw.), geben `Undefined` zurück. |

## Konversionen

Die folgende Tabelle listet die Ergebnisse auf, wenn ein Wert eines Typs in einen anderen Typ konvertiert wird (wenn ein Wert mit dem falschen Typ an eine Funktion übergeben wird). Wenn beispielsweise der absoluten Wertfunktion "abs" (die `Int` oder `Decimal` erwartet) ein `String`-Wert

übergeben wird, versucht diese, den `String`-Wert nach diesen Regeln in einen `Decimal`-Wert umzuwandeln. In diesem Fall wird "abs("-5.123")" als "abs(-5.123)" behandelt.

> **Note**
>
> Konversionen in `Array`, `Object`, `Null` oder `Undefined` werden nicht versucht.

In Dezimalwerte

| Argumenttyp | Ergebnis |
|---|---|
| `Int` | Ein Wert vom Typ `Decimal` ohne Dezimaltr ennzeichen |
| `Decimal` | Der Quellwert |
| `Boolean` | `Undefined` . (Sie können die cast-Funktion explizit zum Umwandeln von true = 1.0, false = 0.0 verwenden.) |
| `String` | Die SQL-Engine versucht, die Zeichenfo lge als `Decimal` zu analysieren. AWS IoT versucht, Zeichenketten zu analysieren, die dem regulären Ausdruck entsprechen:. `^-?\d +(\.\d+)?((?i)E-?\d+)?$` „0“, „-1,2“ und „5E-12“ sind Beispiele für Zeichenfolgen, die automatisch in Werte des Typs `Decimal` umgewandelt werden. |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Null`. |
| Undefined | `Undefined` . |

In Ganzzahlen

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Der Quellwert |
| `Decimal` | Der Quellwert, auf den nächsten `Int`-Wert gerundet. |
| `Boolean` | `Undefined` . (Sie können die cast-Funktion explizit zum Umwandeln von true = 1.0, false = 0.0 verwenden.) |
| `String` | Die SQL-Engine versucht, die Zeichenfolge als zu analysieren. `Decimal` AWS IoT versucht, Zeichenketten zu analysieren, die dem regulären Ausdruck entsprechen:. `^-?\d+(\.\d+)?((?i)E-?\d+)?$` „0", „-1.2", „5E-12" sind alles Beispiele für Zeichenketten, die automatisch in `Decimal` s umgewandelt werden. AWS IoT versucht, das in a umzuwandeln`Decimal`, und schneidet dann die `String` Dezimalstellen ab, um eine zu bilden. `Decimal` `Int` |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Null`. |
| Undefined | `Undefined` . |

In Boolesche Werte

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Undefined` . (Sie können die `cast`-Funktion explizit zum Umwandeln von 0 = False, any_nonzero_value = True verwenden.) |
| `Decimal` | `Undefined` . (Sie können die cast-Funk tion explizit zum Umwandeln von 0 = False, any_nonzero_value = True verwenden.) |
| `Boolean` | Der ursprüngliche Wert |
| `String` | "true"=wahr und "false"=falsch (ohne Beachtung der Groß- und Kleinschreibung). Andere Zeichenfolgenwerte sind `Undefined` . |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

In Zeichenfolgen

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Eine Zeichenfolgendarstellung des `Int`-Werts in Standardnotation |
| `Decimal` | Eine Zeichenfolge, die den `Decimal`-Wert in Standardnotation darstellt |
| `Boolean` | "true" oder "false". Alles in Kleinbuchstaben. |
| `String` | Der ursprüngliche Wert |

| Argumenttyp | Ergebnis |
| --- | --- |
| Array | Das in JSON serialisierte `Array`. Die resultier ende Zeichenfolge ist eine durch Kommata getrennte Liste in eckigen Klammern. Ein `String` ist von Anführungszeichen umschloss en. `Decimal`, `Int`, `Boolean` und `Null` sind dies nicht. |
| Object | Das in JSON serialisierte Objekt. Die resultier ende Zeichenfolge ist eine durch Kommata getrennte Liste von Schlüssel-Wert-Paaren, die mit geschweiften Klammern beginnt und endet. Ein `String` ist von Anführungszeichen umschlossen. `Decimal`, `Int`, `Boolean` und `Null` sind dies nicht. |
| Null | `Undefined` . |
| Undefined | Undefined |

## Operatoren

Die folgenden Operatoren können in SELECT- und WHERE-Klauseln verwendet werden.

### AND-Operator

Gibt ein Ergebnis vom Typ `Boolean` zurück. Führt einen logischen AND-Vorgang aus. Gibt "true" zurück, wenn die Operanden links und rechts wahr sind. Ansonsten wird „false“ zurückgegeben. Operanden vom Typ `Boolean` oder die Zeichenfolgenoperanden „true“ oder „false“ (ohne Beachtung der Groß- und Kleinschreibung) sind erforderlich.

Syntax: *`expression`* `AND` *`expression`*.

AND-Operator

| Left Operator | Right operator | Output |
| --- | --- | --- |
| `Boolean` | `Boolean` | `Boolean`. True, wenn beide Operanden True sind. Ansonsten „false“. |
| `String/Boolean` | `String/Boolean` | Wenn alle Zeichenfolgen „true“ oder „false“ (ohne Beachtung der Groß- und Kleinschreibung) sind, werden sie in den Typ `Boolean` konvertiert und normal als *`boolean`* `AND` *`boolean`* verarbeitet. |
| Anderer Wert | Anderer Wert | `Undefined` . |

## OR-Operator

Gibt ein Ergebnis vom Typ `Boolean` zurück. Führt einen logischen OR-Vorgang aus. Gibt „true” zurück, wenn der linke oder der rechte Operand wahr ist. Ansonsten wird „false“ zurückgegeben. Operanden vom Typ `Boolean` oder die Zeichenfolgenoperanden „true“ oder „false“ (ohne Beachtung der Groß- und Kleinschreibung) sind erforderlich.

Syntax: *`expression`* `OR` *`expression`*.

OR-Operator

| Left operator | Right operator | Output |
| --- | --- | --- |
| `Boolean` | `Boolean` | `Boolean`. True, wenn einer der Operanden True ist. Ansonsten „false“. |
| `String/Boolean` | `String/Boolean` | Wenn alle Zeichenfolgen „true“ oder „false“ (ohne Beachtung der Groß- und Kleinschreibung) sind, werden sie in boolesche Werte konvertiert und normal als *`boolean`* `OR` *`boolean`* verarbeitet. |
| Anderer Wert | Anderer Wert | `Undefined` . |

## NOT-Operator

Gibt ein Ergebnis vom Typ `Boolean` zurück. Führt einen logischen NOT-Vorgang aus. Gibt „true" zurück, wenn der Operand falsch ist. Gibt andernfalls „true" zurück. Ein `Boolean` Operand oder der Zeichenfolgenoperand „true" oder „false" (ohne Beachtung der Groß- und Kleinschreibung) ist erforderlich.

Syntax: `NOT` *`expression`*.

NOT-Operator

| Operand | Output |
|---|---|
| `Boolean` | `Boolean`. True, wenn der Operand False ist. Verwenden Sie andernfalls "true". |
| `String` | Ist die Zeichenfolge „true" oder „false" (ohne Beachtung der Groß- und Kleinschreibung), wird sie in den entsprechenden booleschen Wert konvertiert und der gegenteilige Wert wird zurückgegeben. |
| Anderer Wert | `Undefined` . |

## IN-Operator

Gibt ein Ergebnis vom Typ `Boolean` zurück. Sie können den IN-Operator in einer WHERE-Klausel verwenden, um zu überprüfen, ob ein Wert mit einem Wert in einem Array übereinstimmt. Er gibt „true" zurück, wenn die Übereinstimmung gefunden wird, andernfalls „false".

Syntax: *`expression`* `IN` *`expression`*.

IN-Operator

| Left operator | Right operator | Output |
|---|---|---|
| `Int/Decimal/String/A` | `Array` | Stimmt, wenn das `Object` Element `Integer` `Decimal` `StringArray////`im Array gefunden wird. Ansonsten „false". |

Beispiel:

```
SQL: "select * from 'a/b' where 3 in arr"

JSON: {"arr":[1, 2, 3, "three", 5.7, null]}
```

In diesem Beispiel `where 3 in arr` wird die Bedingungsklausel als wahr ausgewertet, da 3 in dem genannten Array vorhanden ist`arr`. Daher `select * from 'a/b'` wird in der SQL-Anweisung ausgeführt. Dieses Beispiel zeigt auch, dass das Array heterogen sein kann.

## EXISTS-Operator

Gibt ein Ergebnis vom Typ `Boolean` zurück. Sie können den EXISTS-Operator in einer Bedingungsklausel verwenden, um zu testen, ob Elemente in einer Unterabfrage vorhanden sind. Er gibt true zurück, wenn die Unterabfrage ein oder mehrere Elemente zurückgibt, und false, wenn die Unterabfrage keine Elemente zurückgibt.

Syntax: *`expression`*.

Beispiel:

```
SQL: "select * from 'a/b' where exists (select * from arr as a where a = 3)"

JSON: {"arr":[1, 2, 3]}
```

In diesem Beispiel `where exists (select * from arr as a where a = 3)` wird die Bedingungsklausel als wahr ausgewertet, weil 3 in dem genannten Array vorhanden ist. `arr` Daher `select * from 'a/b'` wird in der SQL-Anweisung ausgeführt.

Beispiel:

```
SQL: select * from 'a/b' where exists (select * from e as e where foo = 2)

JSON: {"foo":4,"bar":5,"e":[{"foo":1},{"foo":2}]}
```

In diesem Beispiel `where exists (select * from e as e where foo = 2)` wird die Bedingungsklausel als wahr ausgewertet, da das Array e innerhalb des JSON-Objekts das Objekt enthält`{"foo":2}`. Daher `select * from 'a/b'` wird in der SQL-Anweisung ausgeführt.

## >-Operator

Gibt ein Ergebnis vom Typ `Boolean` zurück. Gibt "true" zurück, wenn der linke Operand größer ist als der rechte Operand. Beide Operanden werden in den Typ `Decimal` konvertiert und anschließend verglichen.

Syntax: *`expression`* `>` *`expression`*.

>-Operator

| Left operator | Right operator | Output |
|---|---|---|
| `Int/Decimal` | `Int/Decimal` | `Boolean`. „true“, wenn der linke Operand größer ist als der rechte Operand. Ansonsten „false“. |
| `String/Int/Deci` | `String/Int/Deci` | Wenn alle Zeichenfolgen in den Typ `Decimal` konvertiert werden können: `Boolean`. Gibt "true" zurück, wenn der linke Operand größer ist als der rechte Operand. Ansonsten „false“. |
| Anderer Wert | `Undefined .` | `Undefined .` |

## >=-Operator

Gibt ein Ergebnis vom Typ `Boolean` zurück. Gibt "true" zurück, wenn der linke Operand mindestens genauso groß ist wie der rechte Operand. Beide Operanden werden in den Typ `Decimal` konvertiert und anschließend verglichen.

Syntax: *`expression`* `>=` *`expression`*.

>=-Operator

| Left operator | Right operator | Output |
|---|---|---|
| `Int/Decimal` | `Int/Decimal` | `Boolean`. „true“, wenn der linke Operand mindestens genauso groß ist wie der rechte Operand. Ansonsten „false“. |
| `String/Int/Deci` | `String/Int/Deci` | Wenn alle Zeichenfolgen in den Typ `Decimal` konvertiert werden können: `Boolean`. Gibt "true" zurück, wenn |

| Left operator | Right operator | Output |
| --- | --- | --- |
| | | der linke Operand mindestens genauso groß ist wie der rechte Operand. Ansonsten „false“. |
| Anderer Wert | `Undefined` . | `Undefined` . |

## <-Operator

Gibt ein Ergebnis vom Typ `Boolean` zurück. Gibt "true" zurück, wenn der linke Operand kleiner ist als der rechte Operand. Beide Operanden werden in den Typ `Decimal` konvertiert und anschließend verglichen.

Syntax: *`expression`* `<` *`expression`*.

<-Operator

| Left operator | Right operator | Output |
| --- | --- | --- |
| `Int/Decimal` | `Int/Decimal` | `Boolean`. „true“, wenn der linke Operand kleiner ist als der rechte Operand. Ansonsten „false“. |
| `String/Int/Deci` | `String/Int/Deci` | Wenn alle Zeichenfolgen in den Typ `Decimal` konvertiert werden können: `Boolean`. Gibt "true" zurück, wenn der linke Operand kleiner ist als der rechte Operand. Ansonsten „false“. |
| Anderer Wert | `Undefined` | `Undefined` |

## <=-Operator

Gibt ein Ergebnis vom Typ `Boolean` zurück. Gibt "true" zurück, wenn der linke Operand höchstens genauso groß ist wie der rechte Operand. Beide Operanden werden in den Typ `Decimal` konvertiert und anschließend verglichen.

Syntax: *`expression`* `<=` *`expression`*.

**<=**-Operator

| Left operator | Right operator | Output |
|---|---|---|
| `Int/Decimal` | `Int/Decimal` | `Boolean`. „true“, wenn der linke Operand höchstens genauso groß ist wie der rechte Operand. Ansonsten „false“. |
| `String/Int/Deci` | `String/Int/Deci` | Wenn alle Zeichenfolgen in den Typ `Decimal` konvertiert werden können: `Boolean`. Gibt "true" zurück, wenn der linke Operand höchstens genauso groß ist wie der rechte Operand. Ansonsten „false“. |
| Anderer Wert | `Undefined` | `Undefined` |

## **<>**-Operator

Gibt ein Ergebnis vom Typ `Boolean` zurück. Gibt „true” zurück, wenn die Operanden links und rechts nicht gleich sind. Ansonsten wird "false" zurückgegeben.

Syntax: *`expression`* `<>` *`expression`*.

**<>**-Operator

| Left operator | Right operator | Output |
|---|---|---|
| `Int` | `Int` | "True", wenn der linke Operand und der rechte Operand nicht gleich sind; ansonsten "false". Ansonsten „false“. |
| `Decimal` | `Decimal` | "True", wenn der linke Operand und der rechte Operand nicht gleich sind; ansonsten "false". Ansonsten "false". Der Typ `Int` wird vor dem Vergleichen in den Typ `Decimal` umgewandelt. |
| `String` | `String` | "True", wenn der linke Operand und der rechte Operand nicht gleich sind; ansonsten "false". Ansonsten „false“. |
| Array | Array | "True", wenn die Elemente in den einzelnen Operanden nicht gleich sind und nicht in der gleichen Reihenfolge vorliegen. Ansonsten "false". |

| Left operator | Right operator | Output |
|---|---|---|
| Object | Object | "True", wenn die Schlüssel und Werte der einzelnen Operanden nicht gleich sind. Ansonsten „false“. Die Reihenfolge der Schlüssel/Werte ist nicht wichtig. |
| Null | Null | Falsch. |
| Beliebiger Wert | `Undefined` | Undefined |
| `Undefined` | Beliebiger Wert | Undefined |
| Falscher Typ | Falscher Typ | true |

## =-Operator

Gibt ein Ergebnis vom Typ `Boolean` zurück. Gibt „true” zurück, wenn die Operanden links und rechts gleich sind. Ansonsten wird "false" zurückgegeben.

Syntax: *`expression`* = *`expression`*.

=-Operator

| Left operator | Right operator | Output |
|---|---|---|
| `Int` | `Int` | "True", wenn der linke Operand und der rechte Operand nicht gleich sind. Ansonsten „false“. |
| `Decimal` | `Decimal` | "True", wenn der linke Operand und der rechte Operand nicht gleich sind. Ansonsten "false". Der Typ `Int` wird vor dem Vergleichen in den Typ `Decimal` umgewandelt. |
| `String` | `String` | "True", wenn der linke Operand und der rechte Operand nicht gleich sind. Ansonsten „false“. |
| Array | Array | "True", wenn die Elemente in den einzelnen Operanden gleich sind und in der gleichen Reihenfolge vorliegen. Ansonsten „false“. |

| Left operator | Right operator | Output |
|---|---|---|
| Object | Object | "True", wenn die Schlüssel und Werte der einzelnen Operanden gleich sind. Ansonsten „false“. Die Reihenfolge der Schlüssel/Werte ist nicht wichtig. |
| Beliebiger Wert | `Undefined` | `Undefined` . |
| `Undefined` | Beliebiger Wert | `Undefined` . |
| Falscher Typ | Falscher Typ | "false" |

## +-Operator

"+" ist ein überladener Operator. Er kann zum Verketten von Zeichenfolgen oder zum Addieren verwendet werden.

Syntax: *`expression`* + *`expression`*.

+-Operator

| Left operator | Right operator | Output |
|---|---|---|
| `String` | Beliebiger Wert | Konvertiert den rechten Operanden in eine Zeichenfolge und hängt ihn an den linken Operanden an |
| Beliebiger Wert | `String` | Konvertiert den linken Operanden in eine Zeichenfolge und hängt den rechten Operanden an den konvertierten linken Operanden an |
| `Int` | `Int` | `Int` Wert. Addiert Operanden. |
| `Int/Decimal` | `Int/Decimal` | `Decimal` Wert. Addiert Operanden. |
| Anderer Wert | Anderer Wert | `Undefined` . |

## --Operator

Subtrahiert den rechten Operanden vom linken Operanden

Syntax: *expression* - *expression*.

--Operator

| Left operator | Right operator | Output |
|---|---|---|
| `Int` | `Int` | `Int` Wert. Subtrahiert den rechten Operanden vom linken Operanden. |
| `Int/Decimal` | `Int/Decimal` | `Decimal` Wert. Subtrahiert den rechten Operanden vom linken Operanden. |
| `String/Int/Deci` | `String/Int/Deci` | Wenn alle Zeichenfolgen korrekt zu Dezimalwerten konvertiert wurden, wird ein `Decimal`-Wert zurückgeg eben. Subtrahiert den rechten Operanden vom linken Operanden. Gibt andernfalls `Undefined` zurück. |
| Anderer Wert | Anderer Wert | `Undefined` . |
| Anderer Wert | Anderer Wert | `Undefined` . |

## *-Operator

Multipliziert den linken Operanden mit dem rechten Operanden

Syntax: *expression* * *expression*.

*-Operator

| Left operator | Right operator | Output |
|---|---|---|
| `Int` | `Int` | `Int` Wert. Multipliziert den linken Operanden mit dem rechten Operanden |
| `Int/Decimal` | `Int/Decimal` | `Decimal` Wert. Multipliziert den linken Operanden mit dem rechten Operanden |
| `String/Int/Deci` | `String/Int/Deci` | Wenn alle Zeichenfolgen korrekt zu Dezimalwerten konvertiert wurden, wird ein `Decimal`-Wert zurückgeg |

| Left operator | Right operator | Output |
| --- | --- | --- |
| | | eben. Multipliziert den linken Operanden mit dem rechten Operanden Gibt andernfalls `Undefined` zurück. |
| Anderer Wert | Anderer Wert | `Undefined` . |

## /-Operator

Dividiert den linken Operanden durch den rechten Operanden

Syntax: *expression* / *expression*.

/-Operator

| Left operator | Right operator | Output |
| --- | --- | --- |
| `Int` | `Int` | `Int` Wert. Dividiert den linken Operanden durch den rechten Operanden |
| `Int/Decimal` | `Int/Decimal` | `Decimal` Wert. Dividiert den linken Operanden durch den rechten Operanden |
| `String/Int/Deci` | `String/Int/Deci` | Wenn alle Zeichenfolgen korrekt zu Dezimalwerten konvertiert wurden, wird ein `Decimal`-Wert zurückgeg eben. Dividiert den linken Operanden durch den rechten Operanden Gibt andernfalls `Undefined` zurück. |
| Anderer Wert | Anderer Wert | `Undefined` . |

## %-Operator

Gibt den Rest zurück, der beim Dividieren des linken Operanden durch den rechten Operanden entsteht.

Syntax: *expression* % *expression*.

%-Operator

| Left operator | Right operator | Output |
|---|---|---|
| `Int` | `Int` | `Int` Wert. Gibt den Rest zurück, der beim Dividieren des linken Operanden durch den rechten Operanden entsteht. |
| `String/Int/Deci` | `String/Int/Deci` | Wenn alle Zeichenfolgen korrekt zu Dezimalwerten konvertiert wurden, wird ein `Decimal`-Wert zurückgeg eben. Gibt den Rest zurück, der beim Dividieren des linken Operanden durch den rechten Operanden entsteht. Andernfalls `Undefined` . |
| Anderer Wert | Anderer Wert | `Undefined` . |

## Funktionen

Verwenden Sie die folgenden integrierten Funktionen in den SELECT- oder WHERE-Klauseln Ihrer SQL-Ausdrücke.

### abs(Decimal)

Gibt den absoluten Wert einer Zahl zurück. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `abs(-5)` gibt 5 zurück.

| Argumenttyp | Ergebnis |
|---|---|
| `Int` | `Int`, der absolute Wert des Arguments |
| `Decimal` | `Decimal`, der absolute Wert des Arguments |
| `Boolean` | `Undefined` . |
| `String` | `Decimal`: das Ergebnis ist der absolute Wert des Arguments. Wenn die Zeichenfo lge nicht konvertiert werden kann, ist das Ergebnis `Undefined` . |

| Argumenttyp | Ergebnis |
| --- | --- |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## accountid()

Gibt die ID des Kontos zurück, das diese Regel als `String` besitzt. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`accountid()` = "123456789012"

## acos(Decimal)

Gibt den umgekehrten Kosinus einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `acos(0)` = 1,5707963267948966

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), der umgekehrte Kosinus des Arguments . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), der umgekehrte Kosinus des Arguments . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |

| Argumenttyp | Ergebnis |
| --- | --- |
| `Boolean` | `Undefined` . |
| `String` | `Decimal`, der umgekehrte Kosinus des Arguments. Wenn die Zeichenfolge nicht konvertiert werden kann, ist das Ergebnis `Undefined` . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## asin(Decimal)

Gibt den umgekehrten Sinus einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `asin(0)` = 0,0

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), der umgekehrte Sinus des Arguments . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), der umgekehrte Sinus des Arguments . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |

| Argumenttyp | Ergebnis |
| --- | --- |
| `Boolean` | `Undefined` . |
| `String` | `Decimal` (mit doppelter Genauigkeit), der umgekehrte Sinus des Arguments. Wenn die Zeichenfolge nicht konvertiert werden kann, ist das Ergebnis `Undefined` . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## atan(Decimal)

Gibt den umgekehrten Tangens einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor Anwendung des Features auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `atan(0)` = 0,0

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), der umgekehrte Tangens des Arguments . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), der umgekehrte Tangens des Arguments . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |

| Argumenttyp | Ergebnis |
| --- | --- |
| `Boolean` | `Undefined` . |
| `String` | `Decimal`, der umgekehrte Tangens des Arguments. Wenn die Zeichenfolge nicht konvertiert werden kann, ist das Ergebnis `Undefined` . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## atan2(Decimal, Decimal)

Gibt den Winkel im Bogenmaß zwischen der positiven x-Achse und dem Punkt (x, y) an, der in den beiden Argumenten definiert ist.  Der Winkel ist positiv für Winkel gegen den Uhrzeigersinn (obere Halbebene, y > 0) und negativ für Winkel im Uhrzeigersinn (untere Halbebene, y < 0). `Decimal` Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `atan2(1, 0)` = 1,5707963267948966

| Argumenttyp | Argumenttyp | Ergebnis |
| --- | --- | --- |
| `Int/Decimal` | `Int/Decimal` | `Decimal` (mit doppelter Genaui Winkel zwischen der x-Achse u festgelegten Punkt (x, y) |
| `Int/Decimal/String` | `Int/Decimal/String` | `Decimal`, der umgekehrte Tang des beschriebenen Punkts. Wer Zeichenfolge nicht konvertiert w ist das Ergebnis `Undefined` . |

| Argumenttyp | Argumenttyp | Ergebnis |
| --- | --- | --- |
| Anderer Wert | Anderer Wert | `Undefined` . |

## aws_lambda(functionArn, inputJson)

Ruft die angegebene Lambda-Funktion. Dabei wird `inputJson` an die Lambda-Funktion übergeben und das von der Lambda-Funktion generierte JSON-Objekt zurückgegeben.

Argumente

| Argument | Beschreibung |
| --- | --- |
| `functionArn` | Der ARN der aufzurufenden Lambda-Funktion. Die Lambda-Funktion muss JSON-Daten zurückgeben. |
| `inputJson` | Die an die Lambda-Funktion übergebene JSON-Eingabe. Um Abfragen und Literale verschachtelter Objekte zu übergeben, müssen Sie die SQL-Version 2016-03-23 verwenden. |

Sie müssen AWS IoT `lambda:InvokeFunction` Berechtigungen erteilen, um die angegebene Lambda-Funktion aufzurufen. Das folgende Beispiel zeigt, wie die `lambda:InvokeFunction`-Berechtigung mit AWS CLI erteilt wird:

```
aws lambda add-permission --function-name "function_name"
--region "region"
--principal iot.amazonaws.com
--source-arn arn:aws:iot:us-east-1:account_id:rule/rule_name
--source-account "account_id"
--statement-id "unique_id"
--action "lambda:InvokeFunction"
```

Im Folgenden werden die Argumente für den Befehl add-permission aufgeführt:

--function-name

Der Name der Lambda-Funktion. Sie fügen eine neue Berechtigung hinzu, um die Ressourcenrichtlinie der Funktion zu aktualisieren.

--Region

Die AWS-Region Ihres Accounts.

--Prinzipal

Der Prinzipal, der die Berechtigung erhält. Dies sollte dazu dienen`iot.amazonaws.com`, die AWS IoT Erlaubnis zum Aufrufen einer Lambda-Funktion zu gewähren.

--source-arn

Der ARN der Regel. Sie können den get-topic-rule AWS CLI Befehl verwenden, um den ARN einer Regel abzurufen.

--source-account

Der AWS-Konto Ort, an dem die Regel definiert ist.

--statement-id

Ein eindeutiger Anweisungsbezeichner

--action

Die Lambda-Aktionen, die Sie in dieser Anweisung zulassen möchten. Um AWS IoT den Aufruf einer Lambda-Funktion zu erlauben, geben Sie `lambda:InvokeFunction` an.

> **Important**
>
> Wenn Sie eine Berechtigung für einen AWS IoT Prinzipal hinzufügen, ohne das `source-arn` oder anzugeben, kann jede`source-account`, AWS-Konto die mit Ihrer Lambda-Aktion eine Regel erstellt, Regeln auslösen, von denen aus Ihre Lambda-Funktion aufgerufen wird. AWS IoT Weitere Informationen finden Sie unter Lambda-Berechtigungsmodell.

Bei einer JSON-Nachrichtennutzlast wie:

```
{
    "attribute1": 21,
    "attribute2": "value"
}
```

Die `aws_lambda`-Funktion kann verwendet werden, um die Lambda-Funktion wie folgt aufzurufen.

```
SELECT
aws_lambda("arn:aws:lambda:us-east-1:account_id:function:lambda_function",
 {"payload":attribute1}) as output FROM 'topic-filter'
```

Wenn Sie möchten, dass die vollständige MQTT-Nachrichtnutzlast übergeben wird, können Sie die JSON-Nutzlast mit „*“ angeben.

```
SELECT
aws_lambda("arn:aws:lambda:us-east-1:account_id:function:lambda_function", *) as output
 FROM 'topic-filter'
```

`payload.inner.element` wählt Daten von der zu Thema „Thema/Unterthema” veröffentlichten Nachrichten aus.

`some.value` wählt Daten aus der Ausgabe aus, die von der Lambda Funktion generiert wurde.

> **Note**
>
> Die Regeln-Engine begrenzt die Ausführungsdauer von Lambda-Funktionen. Aufrufe von Lambda-Funktionen über Regeln sollten innerhalb von 2.000 Millisekunden abgeschlossen werden.

## bitand(Int, Int)

Führt Bit für Bit AND für die Bit-Darstellungen der beiden `Int`(-konvertierten) Argumente durch. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `bitand(13, 5)` = 5

| Argumenttyp | Argumenttyp | Ergebnis |
|---|---|---|
| `Int` | `Int` | `Int`, ein bitweises AND der beid Argumente |
| `Int/Decimal` | `Int/Decimal` | `Int`, ein bitweises AND der beid Argumente Alle Zahlen, die nich Typ `Int` sind, werden auf den n |

| Argumenttyp | Argumenttyp | Ergebnis |
| --- | --- | --- |
| | | `Int`-Wert abgerundet. Wenn ein Argumente nicht in einen `Int`-W konvertiert werden kann, ist das `Undefined` . |
| `Int/Decimal/String` | `Int/Decimal/String` | `Int`, ein bitweises AND der beid Argumente Alle Zeichenfolgen w Dezimal-Werte konvertiert und a nächsten `Int`-Wert abgerundet. Konvertierung fehlschlägt, ist da `Undefined` . |
| Anderer Wert | Anderer Wert | `Undefined` . |

## bitor(Int, Int)

Führt eine bBit für Bit einen OR-Vorgang für die Bit-Darstellungen der beiden Argumente durch. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `bitor(8, 5)` = 13

| Argumenttyp | Argumenttyp | Ergebnis |
| --- | --- | --- |
| `Int` | `Int` | `Int`, das bitweise OR der beide Argumente |
| `Int/Decimal` | `Int/Decimal` | `Int`, das bitweise OR der beide Argumente Alle Zahlen, die nich `Int` sind, werden auf den nächs Wert abgerundet. Wenn die Kon fehlschlägt, ist das Ergebnis Un |
| `Int/Decimal/String` | `Int/Decimal/String` | `Int`, das bitweise OR für die be Argumente. Alle Zeichenfolgen in Dezimal-Werte konvertiert un nächsten `Int`-Wert abgerundet. |

| Argumenttyp | Argumenttyp | Ergebnis |
| --- | --- | --- |
| | | Konvertierung fehlschlägt, ist da `Undefined` . |
| Anderer Wert | Anderer Wert | `Undefined` . |

## bitxor(Int, Int)

Führt Bit für Bit eine XOR-Maßnahme für die Bit-Darstellungen der beiden `Int`(-konvertierten) Argumente durch. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `bitor(13, 5)` = 8

| Argumenttyp | Argumenttyp | Ergebnis |
| --- | --- | --- |
| `Int` | `Int` | `Int`, ein bitweises XOR für die Argumente |
| `Int/Decimal` | `Int/Decimal` | `Int`, ein bitweises XOR für die Argumente Zahlen, die nicht vor sind, werden auf den nächsten abgerundet. |
| `Int/Decimal/String` | `Int/Decimal/String` | `Int`, ein bitweises XOR für die Argumente. Zeichenfolgen werd Dezimal-Werte konvertiert und a nächsten `Int`-Wert abgerundet. Konvertierung fehlschlägt, ist da `Undefined` . |
| Anderer Wert | Anderer Wert | `Undefined` . |

## bitnot(Int)

Führt Bit für Bit einen NOT-Vorgang für die Bit-Darstellungen des `Int`(-konvertierten) Arguments durch. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `bitnot(13) = 2`

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Int`, ein bitweises NOT des Arguments. |
| `Decimal` | `Int`, ein bitweises NOT des Arguments. Der `Decimal`-Wert wird auf den nächsten `Int`-Wert abgerundet. |
| `String` | `Int`, ein bitweises NOT des Arguments. Zeichenfolgen werden in Dezimal-Werte konvertiert und auf den nächsten `Int`-Wert abgerundet. Wenn eine Konvertierung fehlschlägt, ist das Ergebnis `Undefined` . |
| Anderer Wert | Anderer Wert. |

## cast()

Konvertiert einen Wert von einem Datentyp in einen anderen. Diese Umwandlung verhält sich größtenteils wie die Standardkonvertierungen. Zusätzlich verfügt sie jedoch über die Möglichkeit, Zahlen von oder zu booleschen Werten umzuwandeln. Wenn Sie AWS IoT nicht feststellen können, wie ein Typ in einen anderen umgewandelt werden soll, lautet das Ergebnis. `Undefined` Unterstützt von SQL Version 2015-10-08 und höher. Format: Besetzung (*`value`*als*`type`*).

Beispiel:

`cast(true as Int) = 1`

Die folgenden Schlüsselwörter können beim Aufrufen von `cast` unter Umständen nach „as“ angezeigt werden:

Für SQL-Version 2015-10-08 und 2016-03-23

| Stichwort | Ergebnis |
| --- | --- |
| `String` | Wandelt einen Wert in `String` um. |
| Nvarchar | Wandelt einen Wert in `String` um. |

| Stichwort | Ergebnis |
| --- | --- |
| Text | Wandelt einen Wert in `String` um. |
| Ntext | Wandelt einen Wert in `String` um. |
| varchar | Wandelt einen Wert in `String` um. |
| `Int` | Wandelt einen Wert in `Int` um. |
| Ganzzahl | Wandelt einen Wert in `Int` um. |
| Double | Überträgt den Wert auf `Decimal` (mit doppelter Genauigkeit). |

Außerdem für SQL-Version 2016-03-23

| Stichwort | Ergebnis |
| --- | --- |
| `Decimal` | Wandelt einen Wert in `Decimal` um. |
| Bool | Wandelt einen Wert in `Boolean` um. |
| `Boolean` | Wandelt einen Wert in `Boolean` um. |

Umwandlungsregeln:

In Dezimalwert umwandeln

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Ein Wert vom Typ `Decimal` ohne Dezimaltrennzeichen |
| `Decimal` | Der Quellwert<br><br>**Note**<br>Bei SQL V2 (23.03.2016) geben numerische Werte, bei denen es |

| Argumenttyp | Ergebnis |
| --- | --- |
| | sich um ganze Zahlen handelt, z. B. `10.0` einen `Int` Wert (`10`) anstelle des erwarteten `Decimal` Werts (`10.0`) zurück. Um ganzzahlige numerische Werte zuverlässig in `Decimal`-Werte umzuwandeln, verwenden Sie SQL V1 (2015-10-08) für die Regelabfrageanweisung. |
| `Boolean` | "true" = 1,0, "false" = 0,0 |
| `String` | Versucht, die Zeichenfolge als `Decimal` aufzulösen. AWS IoT versucht, Zeichenfolgen aufzulösen, die dem regex entsprechen: ^-?\d+(\.\d+)?((?i)E-?\d+)?$. „0“, „-1,2“ und „5E-12“ sind Beispiele für Zeichenfolgen, die automatisch in Dezimal-Werte umgewandelt werden. |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

In Ganzzahl umwandeln

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Der Quellwert |
| `Decimal` | Der Quellwert, auf den nächsten `Int`-Wert abgerundet |

| Argumenttyp | Ergebnis |
| --- | --- |
| `Boolean` | "true" = 1,0, "false" = 0,0 |
| `String` | Versucht, die Zeichenfolge als `Decimal` aufzulösen. AWS IoT versucht, Zeichenfolgen aufzulösen, die dem regex entsprechen: ^-?\d+(\.\d+)?((?i)E-?\d+)?$. „0“, „-1,2“ und „5E-12“ sind Beispiele für Zeichenfolgen, die automatisch in Dezimal-Werte umgewandelt werden. AWS IoT versucht, die Zeichenfolge in einen `Decimal`-Wert zu konvertieren und auf den nächsten `Int`-Wert abzurunden. |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

In **`Boolean`** umwandeln

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | 0 = false, alle Werte außer Null = true |
| `Decimal` | 0 = false, alle Werte außer Null = true |
| `Boolean` | Der Quellwert |
| `String` | "true" = wahr und "false" = falsch (ohne Beachtung der Groß- und Kleinschreibung). Andere Zeichenfolgenwerte sind = `Undefined` . |
| Array | `Undefined` . |

| Argumenttyp | Ergebnis |
| --- | --- |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

In Zeichenfolge umwandeln

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Eine Zeichenfolgendarstellung des `Int`-Werts in Standardnotation |
| `Decimal` | Eine Zeichenfolge, die den `Decimal`-Wert in Standardnotation darstellt |
| `Boolean` | "true" oder "false", in Kleinbuchstaben |
| `String` | Der Quellwert |
| Array | Das in JSON serialisierte Array. Die resultierende Zeichenfolge ist eine durch Kommata getrennte Liste in eckigen Klammern. `String`-Werte werden mit Anführungszeichen angegeben. Dies ist bei `Decimal`-, `Int`-, `Boolean`-Werten nicht der Fall. |
| Object | Das in JSON serialisierte Objekt. Die JSON-Zeichenfolge ist eine durch Kommata getrennte Liste von Schlüssel-Wert-Paa ren, die mit geschweiften Klammern beginnt und endet. `String`-Werte werden mit Anführungszeichen angegeben. Dies ist bei `Decimal`-, `Int`-, – `Boolean`und `Null`-Werten nicht der Fall. |

| Argumenttyp | Ergebnis |
| --- | --- |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## ceil(Decimal)

Rundet den angegebenen `Decimal`-Wert auf den nächsten `Int`-Wert auf. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`ceil(1.2)` = 2

`ceil(-1.2)` = -1

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Int`, der Argumentwert |
| `Decimal` | `Int`, der `Decimal`-Wert, auf den nächsten `Int`-Wert gerundet |
| `String` | `Int`. Die Zeichenfolge wird in `Decimal` konvertiert und auf den nächsten `Int` aufgerundet. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . |
| Anderer Wert | `Undefined` . |

## chr(String)

Gibt das ASCII-Zeichen zurück, das dem angegebenen `Int`-Argument entspricht. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`chr(65)` = "A".

`chr(49)` = "1".

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Das Zeichen, das dem angegebenen ASCII-Wert entspricht. Wenn das Argument kein gültiger ASCII-Wert ist, ist das Ergebnis `Undefined` . |
| `Decimal` | Das Zeichen, das dem angegebenen ASCII-Wert entspricht. Das `Decimal`-Argument wird auf den nächsten `Int`-Wert abgerundet. Wenn das Argument kein gültiger ASCII-Wert ist, ist das Ergebnis `Undefined` . |
| `Boolean` | `Undefined` . |
| `String` | Wenn der `String`-Wert nicht in einen `Decimal`-Wert konvertiert werden kann, wird er auf den nächsten `Int`-Wert abgerundet. Wenn das Argument kein gültiger ASCII-Wert ist, ist das Ergebnis `Undefined` . |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Anderer Wert | `Undefined` . |

## clientid()

Gibt die ID des MQTT-Clients zurück, der die Nachricht sendet, oder `n/a`, wenn die Nachricht nicht über MQTT gesendet wurde. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`clientid()` = "123456789012"

## concat()

Hängt Arrays oder Zeichenfolgen aneinander an. Diese Funktion akzeptiert eine beliebige Anzahl von Argumenten und gibt einen – `String`oder `Array`-Wert zurück. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`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]

| Anzahl der Argumente | Ergebnis |
|---|---|
| 0 | `Undefined` . |
| 1 | Das Argument wird unverändert zurückgeg eben. |
| 2+ | Wenn ein Argument ein `Array` ist, ist das Ergebnis ein einzelnes Array, das alle Argumente enthält. Wenn kein Argument den Typ Array hat, und mindestens ein Argument den Typ `String` hat, ist das Ergebnis eine Verkettung der `String`- |

| Anzahl der Argumente | Ergebnis |
| --- | --- |
| | Darstellungen aller Argumente. Argumente werden mithilfe von oben genannten Standardkonvertierungen in Zeichenfolgen konvertiert. |

## cos(Decimal)

Gibt den Kosinus einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`cos(0)` = 1.

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), der Kosinus des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), der Kosinus des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |
| `Boolean` | `Undefined` . |
| `String` | `Decimal` (mit doppelter Genauigkeit), der Kosinus des Arguments. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |
| Array | `Undefined` . |

| Argumenttyp | Ergebnis |
| --- | --- |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## cosh(Decimal)

Gibt den hyperbolischen Kosinus einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `cosh(2.3)` = 5,037220649268761.

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), der hyperbolische Kosinus des Arguments . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), der hyperbolische Kosinus des Arguments . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |
| `Boolean` | `Undefined` . |
| `String` | `Decimal` (mit doppelter Genauigkeit), der hyperbolische Kosinus des Arguments . Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben. |

| Argumenttyp | Ergebnis |
| --- | --- |
| Array | `Undefined .` |
| Object | `Undefined .` |
| Null | `Undefined .` |
| Undefined | `Undefined .` |

## decode(value, decodingScheme)

Verwenden Sie die `decode` Funktion, um einen kodierten Wert zu dekodieren. Wenn es sich bei der dekodierten Zeichenfolge um ein JSON-Dokument handelt, wird ein adressierbares Objekt zurückgegeben. Andernfalls wird die dekodierte Zeichenfolge als Zeichenfolge zurückgegeben. Die Funktion gibt NULL zurück, wenn die Zeichenfolge nicht dekodiert werden kann. Diese Funktion unterstützt die Dekodierung von Base64-kodierten Zeichenketten und das Nachrichtenformat Protocol Buffer (protobuf).

Unterstützt von der SQL Version vom 23.03.2016 und höher.

Wert

Ein Zeichenkettenwert oder einer der gültigen Ausdrücke, wie unter AWS IoT SQL-Referenz definiert, die eine Zeichenfolge zurückgeben.

decodingScheme

Eine Literalzeichenfolge, die das Schema darstellt, das zur Dekodierung des Wertes verwendet wurde. Aktuell werden nur `'base64'` und `'proto'` unterstützt.

### Dekodierung von base64-verschlüsselten Strings

In diesem Beispiel enthält die Nachrichtennutzlast einen kodierten Wert.

```
{
    encoded_temp: "eyAidGVtcGVyYXR1cmUiOiAzMyB9Cg=="
}
```

Die `decode`-Funktion in dieser SQL-Anweisung dekodiert den Wert in der Nachrichtennutzlast.

```
SELECT decode(encoded_temp,"base64").temperature AS temp from 'topic/subtopic'
```

Die Dekodierung des `encoded_temp`-Wertes führt zu dem folgenden gültigen JSON-Dokument, das es der SELECT-Anweisung ermöglicht, den Temperaturwert zu lesen.

```
{ "temperature": 33 }
```

Das Ergebnis der SELECT-Anweisung in diesem Beispiel wird hier gezeigt.

```
{ "temp": 33 }
```

Ist der dekodierte Wert kein gültiges JSON-Dokument, wird der dekodierte Wert als Zeichenfolge zurückgegeben.

Payloads der protobuf-Nachrichten entschlüsseln

Sie können SQL-Funktion dekodieren, um eine Regel zu konfigurieren, die die protobuf-Nachrichtennutzlast dekodieren kann. Weitere Informationen finden Sie unter Payloads von protobuf-Nachrichten dekodieren.

> **Important**
>
> Wenn Sie `source-account` bei der Festlegung von Berechtigungen für einen AWS IoT Prinzipal das `source-arn` oder weglassen, AWS-Konto kann jeder Ihre Decode-Funktion über andere Regeln aufrufen. AWS IoT Informationen zur Sicherung Ihrer Funktion finden Sie unter Bucket-Richtlinien im Amazon Simple Storage Service-Benutzerhandbuch.

Die Signatur der Funktion sieht wie folgt aus:

```
decode(<ENCODED DATA>, 'proto', '<S3 BUCKET NAME>', '<S3 OBJECT KEY>', '<PROTO NAME>',
 '<MESSAGE TYPE>')
```

`ENCODED DATA`

Gibt die protobuf-kodierten Daten an, die dekodiert werden sollen. Wenn es sich bei der gesamten an die Regel gesendeten Nachricht um protobuf-kodierte Daten handelt, können Sie die eingehende rohe binäre Nutzlast mit * referenzieren. Andernfalls muss es sich bei diesem Feld

um eine Base-64-kodierte JSON-Zeichenfolge handeln, und ein Verweis auf die Zeichenfolge kann direkt übergeben werden.

1) Um eine eingehende rohe binäre protobuf-Nutzlast zu dekodieren:

```
decode(*, 'proto', ...)
```

2) Um eine protobuf-kodierte Nachricht zu dekodieren, die durch eine Base64-kodierte Zeichenfolge 'a.b' dargestellt wird:

```
decode(a.b, 'proto', ...)
```

`proto`

Spezifiziert die zu dekodierenden Daten in einem protobuf-Nachrichtenformat. Wenn Sie `base64` statt `proto` angeben, dekodiert diese Funktion Base64-kodierte Zeichenketten als JSON.

`S3 BUCKET NAME`

Der Name des Amazon S3 Buckets, in den Sie die `FileDescriptorSet`-Datei hochgeladen haben.

`S3 OBJECT KEY`

Der Objektschlüssel, das die `FileDescriptorSet`-Datei im Amazon S3 S3-Bucket spezifiziert.

`PROTO NAME`

Der Name der `.proto`-Datei (ohne Erweiterung), aus der die `FileDescriptorSet`-Datei generiert wurde.

`MESSAGE TYPE`

Der Name der protobuf-Nachrichtenstruktur innerhalb der `FileDescriptorSet`-Datei, der die zu dekodierenden Daten entsprechen sollen.

Ein Beispiel für einen SQL-Ausdruck, der die SQL-Funktion decode verwendet, kann wie folgt aussehen:

```
SELECT VALUE decode(*, 'proto', 's3-bucket', 'messageformat.desc', 'myproto',
 'messagetype') FROM 'some/topic'
```

- *

Stellt eine binäre eingehende Nutzlast dar, die dem aufgerufenen protobuf-Nachrichtentyp mit dem Namen `mymessagetypeentspricht`.

- `messageformat.desc`

  Die in einem Amazon S3 S3-Bucket gespeicherte `FileDescriptorSet`-Datei mit dem Namen `s3-bucket`.

- `myproto`

  Die `.proto`-Originaldatei, die zur Generierung der `FileDescriptorSet`-Datei mit dem Namen `myproto.proto` verwendet wurde.

- `messagetype`

  Der aufgerufene Nachrichtentyp `messagetype` (zusammen mit allen importierten Abhängigkeiten), wie in definiert`myproto.proto`.

## encode(value, encodingScheme)

Verwenden Sie die Funktion `encode`, um die Nutzlast, bei der es sich möglicherweise um Nicht-JSON-Daten handelt, auf der Grundlage des Kodierungsschemas in ihre String-Darstellung zu kodieren. Unterstützt von der SQL Version vom 23.03.2016 und höher.

Wert

Einer der gültigen Ausdrücke, wie in AWS IoT SQL-Referenz definiert. Sie können „*“ angeben, um die gesamte Nutzlast zu verschlüsseln, unabhängig davon, ob sie das JSON-Format oder ein anderes Format aufweist. Wenn Sie einen Ausdruck angeben, wird das Ergebnis der Auswertung vor dem Verschlüsseln in eine Zeichenfolge umgewandelt.

encodingScheme

Eine Literalzeichenfolge, die das zu verwendende Verschlüsselungsschema darstellt. Derzeit wird nur `'base64'` unterstützt.

## endswith(String, String)

Gibt einen Wert vom Typ `Boolean` zurück, der angibt, ob das erste `String`-Argument mit dem zweiten `String`-Argument endet. Wenn ein Argument `Null` oder `Undefined` ist, ist das Ergebnis `Undefined`. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `endswith("cat","at")` = true.

| Argumenttyp 1 | Argumenttyp 2 | Ergebnis |
| --- | --- | --- |
| `String` | `String` | "True", wenn das erste Argumer zweite Argument endet. Ansons |
| Anderer Wert | Anderer Wert | Beide Argumente werden mithilf Standardkonvertierungsregeln z lgen konvertiert. "True", wenn da Argument auf das zweite Argum Ansonsten „false“. Wenn ein Arg `Null` oder `Undefined` ist, ist Ergebnis `Undefined` . |

## exp(Decimal)

Gibt "e" zurück, potenziert mit dem `Decimal`-Argument. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `exp(1)` = e.

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), e ^ Argument. |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), e ^ Argument. |
| `String` | `Decimal` (mit doppelter Genauigkeit), e ^ Argument. Wenn der `String`-Wert nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . |
| Anderer Wert | `Undefined` . |

## floor(Decimal)

Rundet den angegebenen `Decimal`-Wert auf den nächsten `Int`-Wert ab. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`floor(1.2)` = 1

`floor(-1.2)` = -2

| Argumenttyp | Ergebnis |
|---|---|
| `Int` | `Int`, der Argumentwert |
| `Decimal` | `Int`, der auf den nächsten `Int` abgerundete `Decimal`-Wert. |
| `String` | `Int`. Die Zeichenfolge wird konvertiert in `Decimal` und auf den nächsten `Int`-Wert abgerundet. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . |
| Anderer Wert | `Undefined` . |

## get

Extrahiert einen Wert aus einem sammlungsartigen Typ (Array, Zeichenfolge, Objekt). Auf das erste Argument wird keine Konvertierung angewendet. Die Konvertierung wird wie in der Tabelle dokumentiert auf das zweite Argument angewendet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`get(["a", "b", "c"], 1)` = "b"

`get({"a":"b"}, "a")` = "b"

`get("abc", 0)` = „a“.

| Argumenttyp 1 | Argumenttyp 2 | Ergebnis |
|---|---|---|
| Array | Beliebiger Typ (konvertiert in `Int`) | Das Element am 0-basierten Ind `Array`-Werts, der vom zweiten angegeben wird (konvertiert in I Wenn die Konvertierung fehlsch das Ergebnis `Undefined` . We der Index außerhalb von `Array` (negativ oder >= array.length), is Ergebnis `Undefined` . |
| String | Beliebiger Typ (konvertiert in `Int`) | Das Zeichen am 0-basierten Ind Zeichenfolge, der vom zweiten A angegeben wird (konvertiert in I die Konvertierung fehlschlägt, is Ergebnis `Undefined` . Wenn s Index außerhalb der Zeichenfolg (negativ oder >= string.length), i Ergebnis `Undefined` . |
| Object | `String` (keine Konvertierung wird angewendet) | Der im ersten Argumentobjekt g rte Wert, der dem Zeichenfolger ssel entspricht, der als zweites A angegeben wurde. |
| Anderer Wert | Beliebiger Wert | `Undefined` . |

## get_dynamodb (tableName,,, partitionKeyName, partitionKeyValue roleArn) sortKeyName sortKeyValue

Ruft Daten aus einer DynamoDB-Tabelle ab. `get_dynamodb()` ermöglicht es Ihnen, eine DynamoDB-Tabelle abzufragen, während eine Regel evaluiert wird. Sie können den Nachrichten-Payload mit Hilfe von Daten aus DynamoDB filtern oder erweitern. Unterstützt von der SQL Version vom 23.03.2016 und höher.

`get_dynamodb()` verwendet folgenden Parameter:

tableName

Der Name der DynamoDB-Tabelle für die Abfrage.

partitionKeyName

Der Name des Partitionsschlüssels. Weitere Informationen finden Sie unter DynamoDB Keys.

partitionKeyValue

Der Wert des Partitionsschlüssels, der zur Identifizierung eines Datensatzes verwendet wird. Weitere Informationen finden Sie unter DynamoDB Keys.

sortKeyName

(Optional) Der Name des Sortierschlüssels. Dieser Parameter ist nur erforderlich, wenn die abgefragte DynamoDB-Tabelle einen zusammengesetzten Schlüssel verwendet. Weitere Informationen finden Sie unter DynamoDB Keys.

sortKeyValue

Der Wert des Sortierschlüssels. Dieser Parameter ist nur erforderlich, wenn die abgefragte DynamoDB-Tabelle einen zusammengesetzten Schlüssel verwendet. Weitere Informationen finden Sie unter DynamoDB Keys.

roleArn

Der ARN der IAM-Rolle, der den Zugriff auf die DynamoDB-Tabelle gewährt. Die Regel-Engine übernimmt diese Rolle, um in Ihrem Namen auf die DynamoDB-Tabelle zuzugreifen. Vermeiden Sie die Verwendung einer zu großzügigen Rolle. Erteilen Sie der Rolle nur die von der Regel benötigten Berechtigungen. Nachfolgend finden Sie eine Beispielrichtlinie, die Zugriff auf eine DynamoDB-Tabelle gewährt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "dynamodb:GetItem",
            "Resource": "arn:aws:dynamodb:aws-region:account-id:table/table-name"
        }
    ]
}
```

Als Beispiel dafür, wie Sie `get_dynamodb()` verwenden können, nehmen wir an, Sie haben eine DynamoDB-Tabelle, die Geräte-ID- und Standortinformationen für alle mit AWS IoT verbundenen Geräte enthält. Die folgende SELECT-Anweisung verwendet die `get_dynamodb()`-Funktion, um den Standort für die angegebene Geräte-ID abzurufen:

```
SELECT *, get_dynamodb("InServiceDevices", "deviceId", id,
"arn:aws:iam::12345678910:role/getdynamo").location AS location FROM 'some/
topic'
```

> **Note**
>
> - Sie können `get_dynamodb()` maximal einmal pro SQL-Anweisung aufrufen. Der mehrfache Aufruf von `get_dynamodb()` in einer einzigen SQL-Anweisung führt dazu, dass die Regel ohne Aufruf von Aktionen beendet wird.
> - Wenn `get_dynamodb()` mehr als 8 KB an Daten zurückgibt, darf die Regelaktion nicht aufgerufen werden.

## get_mqtt_property(name)

Verweist auf einen der folgenden MQTT5 Header:,, und. `contentType` `payLoadFormatIndicator` `responseTopic` `correlationData` Diese Funktion verwendet eine der folgenden Literalzeichenfolgen als Argument:`content_type`, `format_indicator`. `response_topic` und `correlation_data` Weitere Informationen in der folgenden Tabelle mit Funktionsargumenten.

contentType

Zeichenfolge: Eine UTF-8-kodierte Zeichenfolge, die den Inhalt der Veröffentlichungsnachricht beschreibt.

payLoadFormatIndikator

Zeichenfolge: Ein Enum-Zeichenfolgenwert, der angibt, ob die Nutzlast als UTF-8 formatiert ist. Gültige Werte sind `UNSPECIFIED_BYTES` und `UTF8_DATA`.

responseTopic

Zeichenfolge: Eine UTF-8 kodierte Zeichenfolge, die als Themenname für eine Antwortnachricht verwendet wird. Das Antwortthema wird verwendet, um das Thema zu beschreiben, das der

Empfänger im Rahmen des Ablaufs Anforderung-Antwort veröffentlichen soll. Das Thema darf keine Platzhalterzeichen enthalten.

correlationData

Zeichenfolge: Die base64-kodierten Binärdaten, die vom Absender der Request Message verwendet werden, um zu identifizieren, für welche Anforderung die Response Message bestimmt ist, wenn sie empfangen wird.

Die folgende Tabelle zeigt die zulässigen Funktionsargumente und die zugehörigen Rückgabetypen für die `get_mqtt_property`-Funktion:

Funktionsargumente

| SQL | Zurückgegebener Datentyp (falls vorhanden) | Zurückgegebener Datentyp (falls vorhanden) |
|---|---|---|
| `get_mqtt_property( "format_indicator")` | Zeichenfolge (UNSPECIF IED_BYTES oder _DATA) UTF8 | Zeichenfolge (UNSPECIF IED_BYTES) |
| `get_mqtt_property( "content_type")` | String | Undefined |
| `get_mqtt_property( "response_topic")` | String | Undefined |
| `get_mqtt_property( "correlation_data")` | base64-kodierte Zeichenfo lge | Undefined |
| `get_mqtt_property( "some_invalid_name ")` | Undefined | Undefined |

Das folgende Beispiel für Rules SQL verweist auf einen der folgenden MQTT5 Header:,, und. `contentType` `payLoadFormatIndicator` `responseTopic` `correlationData`

```
SELECT *, get_mqtt_property('content_type') as contentType,
          get_mqtt_property('format_indicator') as payloadFormatIndicator,
          get_mqtt_property('response_topic') as responseTopic,
```

```
          get_mqtt_property('correlation_data') as correlationData
FROM 'some/topic'
```

## get_secret (secretId, geheimer Typ, Schlüssel, roleArn)

Ruft den Wert des verschlüsselten `SecretString` oder `SecretBinary`-Feldes der aktuellen Version eines Secrets in AWS Secrets Manager ab. Weitere Hinweise zum Erstellen und Verwalten von Geheimnissen finden Sie unter CreateSecretUpdateSecret, und PutSecretValue.

`get_secret()` verwendet folgenden Parameter:

secretId

Zeichenfolge: Der Amazon-Ressourcenname (ARN) oder der Anzeigename des Secrets, das abgerufen werden soll.

SecretType

Zeichenfolge: Der Secret-Typ. Zulässige Werte: `SecretString` | `SecretBinary`.

SecretString

- Für Geheimnisse, die Sie mit der APIs, oder der AWS Secrets Manager Konsole als JSON-Objekte erstellen: AWS CLI
  - Wenn Sie einen Wert für den `key`-Parameter angeben, gibt diese Funktion den Wert des angegebenen Schlüssels zurück.
  - Wenn Sie keinen Wert für den `key`-Parameter angeben, gibt diese Funktion das gesamte JSON-Objekt zurück.
- Für Geheimnisse, die Sie als Nicht-JSON-Objekte erstellen, indem Sie das APIs oder das AWS CLI verwenden:
  - Wenn Sie einen Wert für den `key`-Parameter angeben, schlägt diese Funktion mit einer Ausnahme fehl.
  - Wenn Sie keinen Wert für den `key`-Parameter angeben, gibt diese Funktion den Inhalt des Secrets zurück.

SecretBinary

- Wenn Sie einen Wert für den `key`-Parameter angeben, schlägt diese Funktion mit einer Ausnahme fehl.
- Wenn Sie keinen Wert für den `key`-Parameter angeben, gibt diese Funktion den geheimen Wert als Base64-kodierte UTF-8-Zeichenfolge zurück.

Schlüssel

(Optional) Zeichenfolge: Der Schlüsselname in einem JSON-Objekt, das im `SecretString`-Feld eines Geheimnisses gespeichert ist. Verwenden Sie diesen Wert, wenn Sie statt des gesamten JSON-Objekts nur den Wert eines in einem geheimen Schlüssel gespeicherten Schlüssels abrufen möchten.

Wenn Sie einen Wert für diesen Parameter angeben und das Geheimnis kein JSON-Objekt in seinem `SecretString`-Feld enthält, schlägt diese Funktion mit einer Ausnahme fehl.

roleArn

Zeichenfolge: Eine Rollen-ARN mit den Berechtigungen `secretsmanager:GetSecretValue` und `secretsmanager:DescribeSecret`.

> **Note**
>
> Diese Funktion gibt immer die aktuelle Version des Geheimnisses zurück (die Version mit dem `AWSCURRENT` Tag). Die AWS IoT Regel-Engine speichert jedes Geheimnis bis zu 15 Minuten lang im Cache. Daher kann es bis zu 15 Minuten dauern, bis die Regel-Engine ein Geheimnis aktualisiert. Das heißt, wenn Sie ein Geheimnis bis zu 15 Minuten nach einem Update mit abrufen AWS Secrets Manager, gibt diese Funktion möglicherweise die vorherige Version zurück.
> Diese Funktion ist nicht kostenpflichtig, es AWS Secrets Manager fallen jedoch Gebühren an. Aufgrund des geheimen Caching-Mechanismus ruft die Regel-Engine gelegentlich AWS Secrets Manager auf. Da es sich bei der Regel-Engine um einen vollständig verteilten Dienst handelt, können Sie während des 15-minütigen Caching-Fensters mehrere Secrets Manager Manager-API-Aufrufe von der Regel-Engine sehen.

Beispiele:

Sie können die `get_secret`-Funktion in einem Authentifizierungsheader in einer HTTPS-Regelaktion verwenden, wie im folgenden Beispiel für die API-Schlüsselauthentifizierung.

```
"API_KEY": "${get_secret('API_KEY', 'SecretString', 'API_KEY_VALUE',
 'arn:aws:iam::12345678910:role/getsecret')}"
```

Weitere Informationen zu Regelaktionen finden Sie unter the section called “HTTP”.

## get_thing_shadow(thingName, shadowName, roleARN)

Gibt den angegebenen Schatten des angegebenen Geräts zurück. Unterstützt von der SQL Version vom 23.03.2016 und höher.

thingName

Zeichenfolge: Der Name des Geräts, dessen Schatten Sie abrufen möchten.

shadowName

(Optionale) Zeichenfolge: Der Name des Schattens. Dieser Parameter ist nur erforderlich, wenn auf benannte Schatten verwiesen wird.

roleArn

Zeichenfolge: Eine Rollen-ARN mit der Berechtigung `iot:GetThingShadow`.

Beispiele:

Geben Sie bei Verwendung mit einem benannten Schatten den `shadowName`-Parameter an.

```
SELECT * from 'topic/subtopic'
WHERE
    get_thing_shadow("MyThing","MyThingShadow","arn:aws:iam::123456789012:role/
AllowsThingShadowAccess")
    .state.reported.alarm = 'ON'
```

Lassen Sie bei Verwendung mit einem benannten Schatten den `shadowName`-Parameter aus.

```
SELECT * from 'topic/subtopic'
WHERE
    get_thing_shadow("MyThing","arn:aws:iam::123456789012:role/
AllowsThingShadowAccess")
    .state.reported.alarm = 'ON'
```

## get_user_properties () userPropertyKey

Verweist auf Benutzereigenschaften, eine Art von Eigenschaftsheadern, die in unterstützt werden. MQTT5

userProperty

Zeichenfolge: Eine Benutzereigenschaft ist ein Schlüssel-Wert-Paar. Diese Funktion verwendet den Schlüssel als Argument und gibt ein Array mit allen Werten zurück, die dem zugehörigen Schlüssel entsprechen.

Funktionsargumente

Für die folgenden Benutzereigenschaften in den Nachrichtenkopfzeilen:

| Schlüssel | Value (Wert) |
|---|---|
| ein Schlüssel | ein Wert |
| ein anderer Schlüssel | ein anderer Wert |
| ein Schlüssel | Wert mit doppeltem Schlüssel |

Die folgende Tabelle zeigt das erwartete SQL-Verhalten:

| SQL | Ein Rückgabedatentyp | Zurückgegebener Datenwert |
|---|---|---|
| get_user_properties ('irgendein Schlüssel') | Zeichenfolgen-Array | `['some value', 'value with duplicate key']` |
| get_user_properties ('anderer Schlüssel') | Zeichenfolgen-Array | `['a different value']` |
| get_user_properties () | Array von Schlüssel-Wert-Paar-Objekten | `[{'"some key": "some value"'}, {"other key": "a different value"}, {"some key": "value with duplicate key"}]` |
| get_user_properties ('Schlüssel nicht vorhandener Schlüssel') | Undefined | |

Das folgende Beispiel für Rules SQL verweist auf Benutzereigenschaften (eine Art MQTT5 Eigenschaften-Header) in der Payload:

```
SELECT *, get_user_properties('user defined property key') as userProperty
FROM 'some/topic'
```

## Hashfunktionen

AWS IoT stellt die folgenden Hashing-Funktionen bereit:

- md2
- md5
- sha1
- sha224
- sha256
- sha384
- sha512

Alle Hashfunktionen erwarten ein Zeichenfolgenargument. Das Ergebnis ist der Hashwert dieser Zeichenfolge. Standard-Zeichenfolgenkonvertierungen gelten für alle Argumente, die keine Zeichenfolgen sind. Alle Hashfunktionen werden von der SQL Version 2015-10-08 und höher unterstützt.

Beispiele:

`md2("hello")` = "a9046c73e00331af68917d3804f70655"

`md5("hello")` = "5d41402abc4b2a76b9719d911017c592"

## indexof(String, String)

Gibt den ersten Index (0-basiert) des zweiten Arguments als Teilzeichenfolge des ersten Arguments zurück. Beide Argumente werden als Zeichenfolgen erwartet. Argumente, die keine Zeichenfolgen sind, unterliegen den Standardregeln für die Zeichenfolgenkonvertierung. Diese Funktion gilt nicht für Arrays, nur für Zeichenfolgen. Unterstützt von der SQL Version vom 23.03.2016 und höher.

Beispiele:

`indexof("abcd", "bc")` = 1

## isNull()

Gibt „true“ zurück, wenn das Argument der Wert `Null` ist. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`isNull(5)` = false.

`isNull(Null)` = true.

| Argumenttyp | Ergebnis |
|---|---|
| `Int` | false |
| `Decimal` | false |
| `Boolean` | false |
| `String` | false |
| `Array` | false |
| `Object` | false |
| `Null` | true |
| `Undefined` | false |

## isUndefined()

Gibt „true“ zurück, wenn das Argument `Undefined` ist. Unterstützt von der SQL Version vom 23.03.2016 und höher.

Beispiele:

`isUndefined(5)` = false.

`isUndefined(floor([1,2,3]))` = true.

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | false |
| `Decimal` | false |
| `Boolean` | false |
| `String` | false |
| `Array` | false |
| `Object` | false |
| `Null` | false |
| `Undefined` | true |

## length(String)

Gibt die Anzahl der Zeichen in der angegebenen Zeichenfolge zurück. Für andere Argumente als `String` gelten Standardkonvertierungsregeln. Unterstützt von der SQL Version vom 23.03.2016 und höher.

Beispiele:

`length("hi")` = 2

`length(false)` = 5

## ln(Decimal)

Gibt den natürlichen Logarithmus des Arguments zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `ln(e)` = 1.

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), der natürliche Logarithmus des Arguments |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), der natürliche Logarithmus des Arguments |
| `Boolean` | `Undefined` . |
| `String` | `Decimal` (mit doppelter Genauigkeit), der natürliche Logarithmus des Arguments Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## log(Decimal)

Gibt den Logarithmus des Arguments zur Basis 10 zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `log(100)` = 2.0.

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), der Logarithmus des Arguments zur Basis 10 |

| Argumenttyp | Ergebnis |
| --- | --- |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), der Logarithmus des Arguments zur Basis 10 |
| `Boolean` | `Undefined` . |
| `String` | `Decimal` (mit doppelter Genauigkeit), der Logarithmus des Arguments zur Basis 10 Wenn der `String`-Wert nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## lower(String)

Gibt die kleingeschriebene Version des angegebenen `String`-Werts zurück. Andere Argumente als Zeichenfolgen werden mithilfe der Standardkonvertierungsregeln zu Zeichenfolgen konvertiert. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`lower("HELLO")` = „hello“

`lower(["HELLO"])` = "[\"hello\"]"

## lpad(String, Int)

Gibt das Argument `String` zurück, das auf der linken Seite mit der vom zweiten Argument festgelegten Anzahl an Leerzeichen aufgefüllt wurde. Das Argument `Int` muss zwischen 0 und 1000 liegen. Wenn der angegebene Wert außerhalb des gültigen Bereichs liegt, wird das Argument auf den nächsten gültigen Wert (0 oder 1000) festgelegt. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`lpad("hello", 2) = "  hello"`.

`lpad(1, 3) = "   1"`

| Argumenttyp 1 | Argumenttyp 2 | Ergebnis |
| --- | --- | --- |
| `String` | `Int` | `String`, der angegebene `Stri` der auf der linken Seite mit der A an Leerzeichen aufgefüllt wurde angegebenen `Int`-Wert entspri |
| `String` | `Decimal` | Das `Decimal`-Argument wird au nächsten `Int`-Wert abgerundet `String` wird links mit der angeg Anzahl an Leerzeichen aufgefül |
| `String` | `String` | Das zweite Argument wird in ein `Decimal`-Wert konvertiert, der a nächsten `Int`-Wert abgerundet und der `String`-Wert wird links angegebenen Anzahl an Leerze aufgefüllt. Wenn das zweite Arg in einen `Int`-Wert konvertiert w ist das Ergebnis `Undefined` . |
| Anderer Wert | `Int/Decimal/String` | Der erste Wert wird mit der Star onvertierungen in `String` konv anschließend wird die LPAD-Fu diesen `String` angewendet. W konvertiert werden kann, ist das `Undefined` . |
| Beliebiger Wert | Anderer Wert | `Undefined` . |

## ltrim(String)

Entfernt alle führenden Leerzeichen (Tabulatoren und Leerzeichen) aus dem angegebenen `String`-Wert. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`Ltrim(" h i ")` = "hi "

| Argumenttyp | Ergebnis |
|---|---|
| `Int` | Die `String`-Darstellung des `Int`-Werts nach dem Entfernen der führenden Leerzeichen. |
| `Decimal` | Die `String`-Darstellung des `Decimal`-Werts nach dem Entfernen der führenden Leerzeichen. |
| `Boolean` | Die `String`-Darstellung des boolesche n Werts („true“ oder „false“) nach dem Entfernen der führenden Leerzeichen. |
| `String` | Das Argument nach dem Entfernen der führenden Leerzeichen. |
| Array | Die `String`-Darstellung dvon es `Array` (mit Standardkonvertierungsregeln) nach dem Entfernen der führenden Leerzeichen. |
| Object | Die `String`-Darstellung des Objekts (mit Standardkonvertierungsregeln) nach dem Entfernen der führenden Leerzeichen. |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## machinelearning_predict (modelId, roleArn, Datensatz)

Verwenden Sie die `machinelearning_predict` Funktion, um anhand der Daten aus einer MQTT-Nachricht, die auf einem Amazon SageMaker AI-Modell basiert, Vorhersagen zu treffen. Unterstützt von SQL Version 2015-10-08 und höher. Die Argumente für die `machinelearning_predict`-Funktion sind:

modelId

Die ID des Modells, für das die Voraussage ausgeführt werden soll. Der Echtzeitendpunkt des Modells muss aktiviert sein.

roleArn

Die IAM-Rolle, die über eine Richtlinie mit den Berechtigungen `machinelearning:Predict` und `machinelearning:GetMLModel` verfügt und Zugriff auf das Modell erlaubt, für das die Voraussage ausgeführt wird.

record

Die Daten, die an die SageMaker AI Predict API übergeben werden sollen. Dies sollte als JSON-Objekt mit einer einzelnen Ebene dargestellt werden. Wenn der Datensatz ein JSON-Objekt mit mehreren Ebenen ist, wird der Datensatz auf eine Ebene gebracht, indem seine Werte serialisiert werden. Das folgende JSON-Objekt:

```
{ "key1": {"innerKey1": "value1"}, "key2": 0}
```

wird beispielsweise folgendermaßen geändert:

```
{ "key1": "{\"innerKey1\": \"value1\"}", "key2": 0}
```

Die Funktion gibt ein JSON-Objekt mit den folgenden Feldern zurück:

predictedLabel

Die Klassifizierung der Eingabe auf Grundlage des Modells

Details

Enthält die folgenden Attribute:

PredictiveModelType

Der Modelltyp. Gültige Werte sind REGRESSION, BINARY, MULTICLASS.

Algorithmus

Der Algorithmus, der von SageMaker KI verwendet wird, um Vorhersagen zu treffen. Dieser Wert muss SGD sein.

predictedScores

Enthält den Klassifizierungs-Rohwert für jede Bezeichnung.

predictedValue

Der von SageMaker KI vorhergesagte Wert.

## mod(Decimal, Decimal)

Gibt den Rest zurück, der beim Teilen des ersten Arguments durch das zweite Argument entstanden ist. Äquivalent mit remainder(Decimal, Decimal). Sie können auch "%" als infix-Operator für die gleiche Modulfunktionalität verwenden. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `mod(8, 3)` = 2

| Left operator | Right operator | Output |
|---|---|---|
| `Int` | `Int` | `Int`, das erste Argumentmodulo zweiten Arguments |
| `Int/Decimal` | `Int/Decimal` | `Decimal`, das erste Argumentm zweiten Operanden |
| `String/Int/Decimal` | `String/Int/Decimal` | Wenn alle Zeichenfolgen in Dez erte konvertiert werden, ist das das erste Argumentmodulo des Arguments. Andernfalls `Undefi` |
| Anderer Wert | Anderer Wert | `Undefined` . |

## nanvl (AnyValue, AnyValue)

Gibt das erste Argument zurück, wenn es ein gültiger `Decimal`-Wert ist. Andernfalls wird das zweite Argument zurückgegeben. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `Nanvl(8, 3)` = 8.

| Argumenttyp 1 | Argumenttyp 2 | Output |
|---|---|---|
| Undefined | Beliebiger Wert | Das zweite Argument |
| Null | Beliebiger Wert | Das zweite Argument |
| `Decimal` (NaN) | Beliebiger Wert | Das zweite Argument |
| `Decimal` (nicht NaN) | Beliebiger Wert | Das erste Argument |
| Anderer Wert | Beliebiger Wert | Das erste Argument |

## newuuid()

Gibt eine zufällige 16-Byte-UUID zurück. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `newuuid()` = `123a4567-b89c-12d3-e456-789012345000`

## numbytes(String)

Gibt die Anzahl von Bytes in der UTF-8-Codierung der angegebenen Zeichenfolge zurück. Für andere Argumente als `String` gelten Standardkonvertierungsregeln. Unterstützt von der SQL Version vom 23.03.2016 und höher.

Beispiele:

`numbytes("hi")` = 2

`numbytes("€")` = 3

## parse_time(String, Long, [String])

Verwenden Sie die Funktion `parse_time`, um einen Zeitstempel in ein verständliches Datums- und Zeitformat umzuwandeln. Unterstützt von der SQL Version vom 23.03.2016 und höher. Informationen

zur Konvertierung einer Zeitstempelzeichenfolge in Millisekunden finden Sie unter time_to_epoch (Zeichenfolge, Zeichenfolge).

Die `parse_time`-Funktion verwendet folgende Argumente:

pattern

(Zeichenfolge) Ein Datums-/Uhrzeitmuster, das den Joda-Time-Formaten folgt.

Zeitstempel

(Long) Die zu formatierende Zeit in Millisekunden seit dem Startdatum der Unixzeit. Siehe Funktion timestamp().

Zeitzone

(Zeichenfolge) Die Zeitzone des formatierten Datums bzw. der formatierten Uhrzeit. Der Standardwert ist "UTC". Die Funktion unterstützt Joda-Zeitzonen Dieses Argument ist optional.

Beispiele:

Wenn diese Nachricht für das Thema „A/B“ veröffentlicht wird, wird die Nutzlast `{"ts": "1970.01.01 AD at 21:46:40 CST"}` an den S3-Bucket gesendet:

```
{
    "ruleArn": "arn:aws:iot:us-east-2:ACCOUNT_ID:rule/RULE_NAME",
    "topicRulePayload": {
        "sql": "SELECT parse_time(\"yyyy.MM.dd G 'at' HH:mm:ss z\", 100000000,
 'America/Belize' ) as ts FROM 'A/B'",

        "ruleDisabled": false,
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            {
                "s3": {
                    "roleArn": "arn:aws:iam::ACCOUNT_ID:rule:role/ROLE_NAME",
                    "bucketName": "BUCKET_NAME",
                    "key": "KEY_NAME"
                }
            }
        ],
        "ruleName": "RULE_NAME"
    }
```

```
}
```

Wenn diese Nachricht für das Thema „A/B“ veröffentlicht wird, wird eine Nutzlast ähnlich `{"ts": "2017.06.09 AD at 17:19:46 UTC"}` (aber mit aktuellen Datum/Uhrzeit) an den S3-Bucket gesendet:

```
{
    "ruleArn": "arn:aws:iot:us-east-2:ACCOUNT_ID:rule/RULE_NAME",
    "topicRulePayload": {
        "sql": "SELECT parse_time(\"yyyy.MM.dd G 'at' HH:mm:ss z\", timestamp() ) as ts
 FROM 'A/B'",
        "awsIotSqlVersion": "2016-03-23",
        "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()` kann auch als Ersatz-Vorlage verwendet werden. Wenn diese Nachricht beispielsweise für das Thema „A/B“ veröffentlicht wird, wird die Nutzlast an den S3-Bucket mit Schlüssel = „2017“ gesendet:

```
{
    "ruleArn": "arn:aws:iot:us-east-2:ACCOUNT_ID:rule/RULE_NAME",
    "topicRulePayload": {
        "sql": "SELECT * FROM 'A/B'",
        "awsIotSqlVersion": "2016-03-23",
        "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)

Gibt das erste Argument, potenziert mit dem zweiten Argument, zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `power(2, 5)` = 32,0

| Argumenttyp 1 | Argumenttyp 2 | Output |
|---|---|---|
| `Int/Decimal` | `Int/Decimal` | Ein `Decimal`-Wert (mit doppelte Genauigkeit), das erste Argume potenziert mit dem zweiten Argu |
| `Int/Decimal/String` | `Int/Decimal/String` | Ein `Decimal`-Wert (mit doppelte Genauigkeit), das erste Argume potenziert mit dem zweiten Argu Zeichenfolgen werden in Dezim konvertiert. Wenn `String`-Wert in `Decimal`-Werte umgewande können, ist das Ergebnis `Undef` |
| Anderer Wert | Anderer Wert | `Undefined` . |

## Prinzipal()

Gibt den Prinzipal zurück, den das Gerät für die Authentifizierung verwendet, basierend darauf, wie die auslösende Nachricht veröffentlicht wurde. Die folgende Tabelle beschreibt den Prinzipal, der für jede Veröffentlichungsmethode und jedes Protokoll zurückgegeben wird.

| So wird die Nachricht veröffentlicht | Protokoll | Anmeldeinformationstyp |
|---|---|---|
| MQTT-Client | MQTT | X.509-Gerätezertifikat |
| AWS IoT MQTT-Client für die Konsole | MQTT | IAM-Benutzer oder Rolle |
| AWS CLI | HTTP | IAM-Benutzer oder Rolle |
| AWS IoT Geräte-SDK | MQTT | X.509-Gerätezertifikat |
| AWS IoT Geräte-SDK | MQTT vorbei WebSocket | IAM-Benutzer oder Rolle |

Die folgenden Beispiele zeigen die verschiedenen Arten von Werten, die von `principal()` zurückgegeben werden:

- X.509-Zertifikat-Thumbprint: `ba67293af50bf2506f5f93469686da660c7c844e7b3950bfb16813e0d31e9373`
- IAM-Rollen-ID und Sitzungsname: `ABCD1EFG3HIJK2LMNOP5:my-session-name`
- gibt eine Benutzer-ID zurück: `ABCD1EFG3HIJK2LMNOP5`

## rand()

Gibt einen pseudozufälligen, einheitlich verteilten doppelten Wert zwischen 0,0 und 1,0 zurück. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`rand()` = 0.8231909191640703

## regexp_matches(String, String)

Gibt „true“ zurück, wenn die Zeichenfolge (erstes Argument) eine Übereinstimmung für den regulären Ausdruck (zweites Argument) enthält. Wenn Sie `|` den regulären Ausdruck verwenden, verwenden Sie ihn mit `()`.

Beispiele:

`regexp_matches("aaaa", "a{2,}")` = true.

`regexp_matches("aaaa", "b")` = false.

`regexp_matches("aaa", "(aaa|bbb)")` = true.

`regexp_matches("bbb", "(aaa|bbb)")` = true.

`regexp_matches("ccc", "(aaa|bbb)")` = false.

Erstes Argument:

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Die `String`-Darstellung des `Int`-Werts |
| `Decimal` | Die `String`-Darstellung des `Decimal`-Werts |
| `Boolean` | Die `String`-Darstellung des booleschen Werts („true“ oder „false“) |
| `String` | Das Tool `String`. |
| Array | Die `String`-Darstellung des `Array`-Werts (mit Standardkonvertierungsregeln) |
| Object | Die `String`-Darstellung des Objekts (mit Standardkonvertierungsregeln) |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

Zweites Argument:

Muss ein gültiger regulärer Ausdruck sein. Nicht-String-Typen werden mit den Standardkonvertierungsregeln umgewandelt in `String`. Je nach Typ ist die resultierende Zeichenfolge unter Umständen kein gültiger regulärer Ausdruck. Wenn das (konvertierte) Argument kein gültiger regulärer Ausdruck ist, ist das Ergebnis `Undefined`.

## regexp_replace(String, String, String)

Ersetzt alle Vorkommen des zweiten Arguments (regulärer Ausdruck) im ersten Argument durch das dritte Argument. Verweist auf Erfassungsgruppen mit "$". Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`regexp_replace("abcd", "bc", "x")` = "axd"

`regexp_replace("abcd", "b(.*)d", "$1")` = "ac"

Erstes Argument:

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Die `String`-Darstellung des `Int`-Werts |
| `Decimal` | Die `String`-Darstellung des `Decimal`-Werts |
| `Boolean` | Die `String`-Darstellung des booleschen Werts („true“ oder „false“) |
| `String` | Der Quellwert |
| Array | Die `String`-Darstellung des `Array`-Werts (mit Standardkonvertierungsregeln) |
| Object | Die `String`-Darstellung des Objekts (mit Standardkonvertierungsregeln) |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

Zweites Argument:

Muss ein gültiger regulärer Ausdruck sein. Nicht-String-Typen werden mit den Standardkonvertierungsregeln umgewandelt in `String`. Je nach Typ ist die resultierende

Zeichenfolge unter Umständen kein gültiger regulärer Ausdruck. Wenn das (konvertierte) Argument kein gültiger regulärer Ausdruck ist, ist das Ergebnis `Undefined`.

Drittes Argument:

Muss eine gültige RegEx-Ersetzungszeichenfolge sein. (Kann auf Erfassungsgruppen verweisen.) Nicht-String-Typen werden mit den Standardkonvertierungsregeln umgewandelt in `String`. Wenn das (konvertierte) Argument keine gültige RegEx-Ersetzungszeichenfolge ist, ist das Ergebnis `Undefined`.

### regexp_substr(String, String)

Findet die erste Übereinstimmung des zweiten Parameters (regex) im ersten Parameter. Verweist auf Erfassungsgruppen mit "$". Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`regexp_substr("hihihello", "hi")` = "hi"

`regexp_substr("hihihello", "(hi)*")` = "hihi"

Erstes Argument:

| Argumenttyp | Ergebnis |
|---|---|
| `Int` | Die `String`-Darstellung des `Int`-Werts |
| `Decimal` | Die `String`-Darstellung des `Decimal`-Werts |
| `Boolean` | Die `String`-Darstellung des booleschen Werts („true“ oder „false“) |
| `String` | Das `String`-Argument |
| Array | Die `String`-Darstellung des `Array`-Werts (mit Standardkonvertierungsregeln) |
| Object | Die `String`-Darstellung des Objekts (mit Standardkonvertierungsregeln) |
| Null | `Undefined` . |

| Argumenttyp | Ergebnis |
| --- | --- |
| Undefined | `Undefined` . |

Zweites Argument:

Muss ein gültiger regulärer Ausdruck sein. Nicht-String-Typen werden mit den Standardkonvertierungsregeln umgewandelt in `String`. Je nach Typ ist die resultierende Zeichenfolge unter Umständen kein gültiger regulärer Ausdruck. Wenn das (konvertierte) Argument kein gültiger regulärer Ausdruck ist, ist das Ergebnis `Undefined`.

## remainder(Decimal, Decimal)

Gibt den Rest zurück, der beim Teilen des ersten Arguments durch das zweite Argument entstanden ist. Äquivalent mit mod(Decimal, Decimal). Sie können auch "%" als infix-Operator für die gleiche Modulfunktionalität verwenden. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `remainder(8, 3)` = 2

| Left operator | Right operator | Output |
| --- | --- | --- |
| `Int` | `Int` | `Int`, das erste Argumentmodulo zweiten Arguments |
| `Int/Decimal` | `Int/Decimal` | `Decimal`, das erste Argumentm zweiten Operanden |
| `String/Int/Decimal` | `String/Int/Decimal` | Wenn alle Zeichenfolgen in Dez erte konvertiert werden, ist das das erste Argumentmodulo des Arguments. Andernfalls `Undefi` |
| Anderer Wert | Anderer Wert | `Undefined` . |

## replace(String, String, String)

Ersetzt alle Vorkommen des zweiten Arguments im ersten Argument durch das dritte Argument. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`replace("abcd", "bc", "x")` = `"axd"`.

`replace("abcdabcd", "b", "x")` = `"axcdaxcd"`.

Alle Argumente

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Die `String`-Darstellung des `Int`-Werts |
| `Decimal` | Die `String`-Darstellung des `Decimal`-Werts |
| `Boolean` | Die `String`-Darstellung des booleschen Werts („true“ oder „false“) |
| `String` | Der Quellwert |
| Array | Die `String`-Darstellung des `Array`-Werts (mit Standardkonvertierungsregeln) |
| Object | Die `String`-Darstellung des Objekts (mit Standardkonvertierungsregeln) |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## rpad(String, Int)

Gibt das Zeichenfolgenargument zurück, das auf der rechten Seite mit der im zweiten Argument festgelegten Anzahl an Leerzeichen aufgefüllt wurde. Das Argument `Int` muss zwischen 0 und 1000 liegen. Wenn der angegebene Wert außerhalb des gültigen Bereichs liegt, wird das Argument auf den nächsten gültigen Wert (0 oder 1000) festgelegt. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`rpad("hello", 2)` = `"hello  "`.

`rpad(1, 3)` = `"1  "`.

| Argumenttyp 1 | Argumenttyp 2 | Ergebnis |
| --- | --- | --- |
| `String` | `Int` | Der `String`-Wert, der auf der rechten Seite mit der Anzahl an Leerzeichen aufgefüll t wurde, die dem angegebenen `Int`-Wert entspricht |
| `String` | `Decimal` | Das `Decimal`-Argument wird auf den nächsten `Int`-Wert abgerundet und die Zeichenfolge wird auf der rechten Seite mit der Anzahl an Leerzeichen aufgefüllt, die dem angegebenen `Int`-Wert entspricht. |
| `String` | `String` | Das zweite Argument wird in einen `Decimal`-Wert konvertiert, der auf den nächsten `Int`-Wert abgerundet wird. Der `String`-Wert wird auf der rechten Seite mit der Anzahl an Leerzeichen aufgefüll t, die dem `Int`-Wert entspricht. |
| Anderer Wert | `Int/Decimal/String` | Der erste Wert wird mit der Standardk onvertierungen in |

| Argumenttyp 1 | Argumenttyp 2 | Ergebnis |
| --- | --- | --- |
| | | `String` konvertiert und anschließend wird die rpad-Funktion auf `String` angewendet. Wenn er nicht konvertiert werden kann, ist das Ergebnis `Undefined` . |
| Beliebiger Wert | Anderer Wert | `Undefined` . |

## round(Decimal)

Runden den angegebenen `Decimal`-Wert auf den nächsten `Int`-Wert. Wenn `Decimal` gleich weit von zwei `Int`-Werten entfernt ist (z. B. 0,5), wird `Decimal` aufgerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `Round(1.2)` = 1.

`Round(1.5)` = 2.

`Round(1.7)` = 2.

`Round(-1.1)` = -1.

`Round(-1.5)` = -2.

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Das Argument |
| `Decimal` | `Decimal` wird auf den nächsten `Int`-Wert abgerundet. |
| `String` | `Decimal` wird auf den nächsten `Int`-Wert abgerundet. Wenn die Zeichenfolge nicht |

| Argumenttyp | Ergebnis |
| --- | --- |
| | in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . |
| Anderer Wert | `Undefined` . |

## rtrim(String)

Entfernt alle nachstehenden Leerzeichen (Tabulatoren und Leerzeichen) aus dem angegebenen `String`-Wert. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`rtrim(" h i ") = " h i"`

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Die `String`-Darstellung des `Int`-Werts |
| `Decimal` | Die `String`-Darstellung des `Decimal`-Werts |
| `Boolean` | Die `String`-Darstellung des booleschen Werts („true“ oder „false“) |
| Array | Die `String`-Darstellung des `Array`-Werts (mit Standardkonvertierungsregeln) |
| Object | Die `String`-Darstellung des Objekts (mit Standardkonvertierungsregeln) |
| Null | `Undefined` . |
| Undefined | `Undefined` |

## sign(Decimal)

Gibt das Vorzeichen der angegebenen Zahl zurück. Wenn das Vorzeichen des Arguments positiv ist, wird 1 zurückgegeben. Wenn das Vorzeichen des Arguments negativ ist, wird -1 zurückgegeben. Wenn das Argument 0 ist, wird 0 zurückgegeben. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`sign(-7)` = -1.

`sign(0)` = 0.

`sign(13)` = 1.

| Argumenttyp | Ergebnis |
|---|---|
| `Int` | `Int`, das Vorzeichen des `Int`-Werts |
| `Decimal` | `Int`, das Vorzeichen des `Decimal`-Werts |
| `String` | `Int`, das Vorzeichen des `Decimal`-Werts Die Zeichenfolge wird in einen `Decimal`-Wert konvertiert und das Vorzeichen des `Decimal`-Werts wird zurückgegeben. Wenn der `String`-Wert nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . Unterstützt von SQL Version 2015-10-08 und höher. |
| Anderer Wert | `Undefined` . |

## sin(Decimal)

Gibt den Sinus einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `sin(0)` = 0,0

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), der Sinus des Arguments |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), der Sinus des Arguments |
| `Boolean` | `Undefined` . |
| `String` | `Decimal` (mit doppelter Genauigkeit), der Sinus des Arguments Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| `Undefined` | `Undefined` . |

## sinh(Decimal)

Gibt den hyperbolischen Sinus einer Zahl zurück. `Decimal`-Werte werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Das Ergebnis ist ein `Decimal`-Wert mit doppelter Genauigkeit. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `sinh(2.3)` = 4,936961805545957

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), der hyperbolische Sinus des Arguments. |

| Argumenttyp | Ergebnis |
| --- | --- |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), der hyperbolische Sinus des Arguments. |
| `Boolean` | `Undefined` . |
| `String` | `Decimal` (mit doppelter Genauigkeit), der hyperbolische Sinus des Arguments . Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## SourceIp

Ruft die IP-Adresse eines Geräts oder des Routers ab, der eine Verbindung zu diesem Gerät herstellt. Wenn Ihr Gerät direkt mit dem Internet verbunden ist, gibt die Funktion die Quell-IP-Adresse des Geräts zurück. Wenn Ihr Gerät mit einem Router verbunden ist, der eine Verbindung zum Internet herstellt, gibt die Funktion die Quell-IP-Adresse des Routers zurück. Unterstützt von der SQL-Version 2016-03-23. `sourceip()` benötigt keine Parameter.

> **Important**
>
> Die öffentliche Quell-IP-Adresse eines Geräts ist häufig die IP-Adresse des letzten Network Address Translation (NAT)-Gateways, z. B. des Routers oder des Kabelmodems Ihres Internetdienstanbieters.

Beispiele:

```
sourceip()="192.158.1.38"
```

```
sourceip()="1.102.103.104"

sourceip()="2001:db8:ff00::12ab:34cd"
```

SQL-Beispiel

```
SELECT *, sourceip() as deviceIp FROM 'some/topic'
```

Beispiele für die Verwendung der Funktion sourceip () in AWS IoT Core Regelaktionen:

Beispiel 1

Das folgende Beispiel zeigt, wie die Funktion () als Ersatzvorlage in einer DynamoDB-Maßnahme aufgerufen wird.

```
{
 "topicRulePayload": {
  "sql": "SELECT * AS message FROM 'some/topic'",
  "ruleDisabled": false,
  "awsIotSqlVersion": "2016-03-23",
  "actions": [
   {
    "dynamoDB": {
     "tableName": "my_ddb_table",
     "hashKeyField": "key",
     "hashKeyValue": "${sourceip()}",
     "rangeKeyField": "timestamp",
     "rangeKeyValue": "${timestamp()}",
     "roleArn": "arn:aws:iam::123456789012:role/aws_iot_dynamoDB"
    }
   }
  ]
 }
}
```

Beispiel 2

Das folgende Beispiel zeigt, wie die Funktion sourceip() als MQTT-Benutzereigenschaft mithilfe von Ersetzungsvorlagen hinzugefügt wird.

```
{
 "topicRulePayload": {
```

```
  "sql": "SELECT * FROM 'some/topic'",
  "ruleDisabled": false,
  "awsIotSqlVersion": "2016-03-23",
  "actions": [
   {
    "republish": {
     "topic": "${topic()}/republish",
     "roleArn": "arn:aws:iam::123456789012:role/aws_iot_republish",
     "headers": {
      "payloadFormatIndicator": "UTF8_DATA",
      "contentType": "rule/contentType",
      "correlationData": "cnVsZSBjb3JyZWxhdGlvbiBkYXRh",
      "userProperties": [
       {
        "key": "ruleKey1",
        "value": "ruleValue1"
       },
       {
        "key": "sourceip",
        "value": "${sourceip()}"
       }
      ]
     }
    }
   }
  ]
 }
}
```

Sie können die Quell-IP-Adresse aus Nachrichten abrufen, die sowohl über den Message Broker- als auch über den Basic-Ingest-Pfad an AWS IoT Core Regeln weitergeleitet werden. Sie können auch die Quell-IP für beide IPv4 IPv6 Nachrichten abrufen. Die Quell-IP wird wie folgt angezeigt:

IPv6: `yyyy:yyyy:yyyy::yyyy:yyyy`

IPv4: `xxx.xxx.xxx.xxx`

> **Note**
>
> Die ursprüngliche Quell-IP wird bei der Maßnahme Erneut veröffentlichen nicht weitergegeben.

## substring(String, Int[, Int])

Erwartet einen `String`-Wert, gefolgt von einem oder zwei `Int`-Werten. Für einen `String`-Wert und ein einzelnes `Int`-Argument gibt diese Funktion die Teilzeichenfolge des angegebenen `String`-Werts vom angegebenen `Int`-Index (0-basiert, inklusive) am Ende des `String`-Werts zurück. Für einen `String`-Wert und ein zwei `Int`-Argumente gibt diese Funktion die Teilzeichenfolge des angegebenen `String`-Werts vom ersten `Int`-Indexargument (0-basiert, inklusive) an das zweite`Int`-Indexargument (0-basiert, exklusive) zurück. Indizes, die kleiner als Null sind, werden auf Null festgelegt. Indizes, die größer sind als die `String`-Länge, werden auf die `String`-Länge festgelegt. Wenn bei drei Argumenten der erste Index mindestens genauso groß ist wie der zweite Index, ist das Ergebnis der leere `String`-Wert.

Wenn die angegebenen Argumente nicht (*`String`*,*`Int`*) oder (,,) sind *`StringInt`*, *`Int`* werden die Standardkonvertierungen auf die Argumente angewendet, um zu versuchen, sie in die richtigen Typen zu konvertieren. Wenn die Typen nicht konvertiert werden können, ist das Ergebnis der Funktion `Undefined`. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`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)` = "true".

`substring(false, -2.411E247)` = "false".

`substring("012345", 1, 3)` = "12".

`substring("012345", -50, 50)` = "012345".

`substring("012345", 3, 1)` = "".

## sql_version()

Gibt die in dieser Regel angegebene SQL Version zurück. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`sql_version()` = "2016-03-23"

## sqrt(Decimal)

Gibt die Quadratwurzel einer Zahl zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `sqrt(9)` = 3.0.

| Argumenttyp | Ergebnis |
|---|---|
| `Int` | Die Quadratwurzel des Arguments. |
| `Decimal` | Die Quadratwurzel des Arguments. |
| `Boolean` | `Undefined` . |
| `String` | Die Quadratwurzel des Arguments. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . |
| Array | `Undefined` . |
| Object | `Undefined` . |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## startswith(String, String)

Gibt einen Wert vom Typ `Boolean` zurück, der angibt, ob das erste Zeichenfolgenargument mit dem zweiten Zeichenfolgenargument beginnt. Wenn ein Argument `Null` oder `Undefined` ist, ist das Ergebnis `Undefined`. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`startswith("ranger","ran")` = true

| Argumenttyp 1 | Argumenttyp 2 | Ergebnis |
| --- | --- | --- |
| `String` | `String` | Ob die erste Zeichenfolge mit d Zeichenfolge beginnt |
| Anderer Wert | Anderer Wert | Beide Argumente werden mithilf Standardkonvertierungsregeln z lgen konvertiert. Gibt „true“ zurü die erste Zeichenfolge mit der z Zeichenfolge beginnt. Wenn ein `Null` oder `Undefined` ist, ist Ergebnis `Undefined` . |

## tan(Decimal)

Gibt den Tangens einer Zahl im Bogenmaß zurück. `Decimal`-Werte werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `tan(3)` = -0,1425465430742778

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), der Tangens des Arguments. |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), der Tangens des Arguments. |
| `Boolean` | `Undefined` . |
| `String` | `Decimal` (mit doppelter Genauigkeit), der Tangens des Arguments. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . |
| Array | `Undefined` . |

| Argumenttyp | Ergebnis |
| --- | --- |
| Object | `Undefined .` |
| Null | `Undefined .` |
| Undefined | `Undefined .` |

## tanh(Decimal)

Gibt den hyperbolischen Tangens einer Zahl im Bogenmaß zurück. `Decimal`-Werte werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `tanh(2.3)` = 0,9800963962661914

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | `Decimal` (mit doppelter Genauigkeit), der hyperbolische Tangens des Arguments |
| `Decimal` | `Decimal` (mit doppelter Genauigkeit), der hyperbolische Tangens des Arguments |
| `Boolean` | `Undefined .` |
| `String` | `Decimal` (mit doppelter Genauigkeit), der hyperbolische Tangens des Arguments Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined .` |
| Array | `Undefined .` |
| Object | `Undefined .` |
| Null | `Undefined .` |
| Undefined | `Undefined .` |

## time_to_epoch (Zeichenfolge, Zeichenfolge)

Verwenden Sie die `time_to_epoch`-Funktion, um eine Zeitstempelzeichenfolge in eine Anzahl von Millisekunden in der Unix-Zeit umzuwandeln. Unterstützt von der SQL Version vom 23.03.2016 und höher. Informationen zur Konvertierung von Millisekunden in eine formatierte Zeitstempelzeichenfolge finden Sie unter parse_time(String, Long, [String]).

Die `time_to_epoch`-Funktion verwendet folgende Argumente:

Zeitstempel

(Zeichenfolge) Die Zeitstempelzeichenfolge, die seit der Unix-Epoche in Millisekunden konvertiert werden soll. Wenn die Zeitstempelzeichenfolge keine Zeitzone angibt, verwendet die Funktion die UTC-Zeitzone.

pattern

(Zeichenfolge) Ein Datums-/Uhrzeitmuster, das den JDK11 Zeitformaten folgt.

Beispiele:

`time_to_epoch("2020-04-03 09:45:18 UTC+01:00", "yyyy-MM-dd HH:mm:ss VV")` = 1585903518000

`time_to_epoch("18 December 2015", "dd MMMM yyyy")` = 1450396800000

`time_to_epoch("2007-12-03 10:15:30.592 America/Los_Angeles", "yyyy-MM-dd HH:mm:ss.SSS z")` = 1196705730592

## timestamp()

Gibt den aktuellen Zeitstempel in Millisekunden ab 00:00:00 Uhr Coordinated Universal Time (UTC), Donnerstag, 1. Januar 1970, zurück, wie er von der Regel-Engine beobachtet wurde. AWS IoT Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel: `timestamp()` = `1481825251155`

## topic(Decimal)

Gibt das Topic zurück, an das die Nachricht gesendet wurde, welche die Regel ausgelöst hat. Wenn kein Parameter angegeben ist, wird das gesamte Topic zurückgegeben. Der Parameter `Decimal`

wird verwendet, um ein bestimmtes Themensegment anzugeben, wobei 1 das erste Segment bezeichnet. Für das Thema `foo/bar/baz` gibt topic(1) `foo` zurück, topic(2) gibt `bar` zurück usw. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`topic()` = "things/myThings/thingOne"

`topic(1)` = "things"

Wenn Basic Ingest verwendet wird, ist das anfängliche Präfix des Themas (`$aws/rules/`*`rule-name`*) nicht für die Thema()-Funktion verfügbar. Angenommen, das Thema ist:

`$aws/rules/BuildingManager/Buildings/Building5/Floor2/Room201/Lights`

`topic()` = "Buildings/Building5/Floor2/Room201/Lights"

`topic(3)` = "Floor2" („Etage2”)

## traceid()

Gibt die Ablaufverfolgungs-ID (UUID) der MQTT-Nachricht zurück oder `Undefined`, wenn die Nachricht nicht über MQTT gesendet wurde. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`traceid()` = "12345678-1234-1234-1234-123456789012"

## transformieren (Zeichenfolge, Objekt, Array)

Gibt ein Array von Objekten zurück, das das Ergebnis der angegebenen Transformation des `Object` Parameters für den `Array`-Parameter enthält.

Unterstützt von der SQL Version vom 23.03.2016 und höher.

String

> Der zu verwendende Transformationsmodus. In der folgenden Tabelle finden Sie Informationen zu den unterstützten Transformationsmodi und dazu, wie sie die `Array`-Parameter `Result` aus den `Object` und erstellen.

Object

Ein Objekt, das die Attribute enthält, die auf jedes Element von `Array` angewendet werden sollen.

Array

Eine Reihe von Objekten, auf die die Attribute von `Object` angewendet werden.

Jedes Objekt in diesem Array entspricht einem Objekt in der Antwort der Funktion. Jedes Objekt in der Antwort der Funktion enthält die Attribute, die im ursprünglichen Objekt vorhanden sind, und die Attribute, die von `Object` bereitgestellt werden, wie durch den in `String` angegebenen Transformationsmodus bestimmt.

| **`String`** Parameter | **`Object`** Parameter | **`Array`** Parameter | Ergebnis |
|---|---|---|---|
| `enrichArray` | Object | Array von -Objekten. | Ein Array von Objekten, in dem jedes Objekt die Attribute eines Elements aus dem `Array`-Parameter und die Attribute des `Object`-Parameters enthält. |
| Jeder andere Wert | Beliebiger Wert | Beliebiger Wert | Undefined |

> **Note**
>
> Das von dieser Funktion zurückgegebene Array ist auf 128 KiB begrenzt.

Beispiel 1 für die Transformationsfunktion

Dieses Beispiel zeigt, wie die transform()-Funktion aus einem Datenobjekt und einem Array ein einzelnes Array von Objekten erzeugt.

In diesem Beispiel wird folgende Nachricht im MQTT-Thema `A/B` veröffentlicht.

```
{
    "attributes": {
        "data1": 1,
        "data2": 2
    },
    "values": [
        {
            "a": 3
        },
        {
            "b": 4
        },
        {
            "c": 5
        }
    ]
}
```

Diese SQL-Anweisung für eine Themenregelaktion verwendet die transform()-Funktion mit dem Wert `String` von `enrichArray`. In diesem Beispiel `Object` handelt es sich um die `attributes`-Eigenschaft aus der Nachrichtennutzlast und um `Array` das `values` Array, das drei Objekte enthält.

```
select value transform("enrichArray", attributes, values) from 'A/B'
```

Nach dem Empfang der Nachrichtennutzdaten wird die SQL-Anweisung zu der folgenden Antwort ausgewertet.

```
[
  {
    "a": 3,
    "data1": 1,
    "data2": 2
  },
  {
    "b": 4,
    "data1": 1,
    "data2": 2
  },
  {
    "c": 5,
    "data1": 1,
    "data2": 2
```

```
  }
]
```

Beispiel 2 für die Transformationsfunktion

Dieses Beispiel zeigt, wie die transform()-Funktion Literalwerte verwenden kann, um einzelne Attribute aus der Nachrichtennutzlast einzubeziehen und umzubenennen.

In diesem Beispiel wird folgende Nachricht im MQTT-Thema `A/B` veröffentlicht. Dies ist dieselbe Nachricht, die in the section called “Beispiel 1 für die Transformationsfunktion” verwendet wurde.

```
{
    "attributes": {
        "data1": 1,
        "data2": 2
    },
    "values": [
        {
            "a": 3
        },
        {
            "b": 4
        },
        {
            "c": 5
        }
    ]
}
```

Diese SQL-Anweisung für eine Themenregelaktion verwendet die transform()-Funktion mit dem Wert `String` von `enrichArray`. Die `Object` in der transform()-Funktion hat ein einzelnes Attribut, das `key` mit dem Wert von `attributes.data1` in der Nachrichtennutzlast benannt ist, und `Array` ist das `values` Array, das dieselben drei Objekte enthält, die im vorherigen Beispiel verwendet wurden.

```
select value transform("enrichArray", {"key": attributes.data1}, values) from 'A/B'
```

Nach dem Empfang der Nachrichtennutzdaten wird diese SQL-Anweisung zu der folgenden Antwort ausgewertet. Beachten Sie, wie die `data1`-Eigenschaft `key` in der Antwort benannt ist.

```
[
  {
    "a": 3,
```

```
    "key": 1
  },
  {
    "b": 4,
    "key": 1
  },
  {
    "c": 5,
    "key": 1
  }
]
```

Beispiel 3 für die Transformationsfunktion

Dieses Beispiel zeigt, wie die transform()-Funktion in verschachtelten SELECT-Klauseln verwendet werden kann, um mehrere Attribute auszuwählen und neue Objekte für die nachfolgende Verarbeitung zu erstellen.

In diesem Beispiel wird folgende Nachricht im MQTT-Thema `A/B` veröffentlicht.

```
{
  "data1": "example",
  "data2": {
    "a": "first attribute",
    "b": "second attribute",
    "c": [
      {
        "x": {
          "someInt": 5,
          "someString": "hello"
        },
        "y": true
      },
      {
        "x": {
          "someInt": 10,
          "someString": "world"
        },
        "y": false
      }
    ]
  }
}
```

Das `Object` für diese Transformationsfunktion ist das Objekt, das von der SELECT-Anweisung zurückgegeben wurde, die die Elemente a und b des `data2`-Objekts der Nachricht enthält. Der `Array`-Parameter besteht aus den beiden Objekten aus dem `data2.c` Array in der ursprünglichen Nachricht.

```
select value transform('enrichArray', (select a, b from data2), (select value c from
 data2)) from 'A/B'
```

Bei der vorherigen Nachricht ergibt die SQL-Anweisung die folgende Antwort.

```
[
  {
    "x": {
      "someInt": 5,
      "someString": "hello"
    },
    "y": true,
    "a": "first attribute",
    "b": "second attribute"
  },
  {
    "x": {
      "someInt": 10,
      "someString": "world"
    },
    "y": false,
    "a": "first attribute",
    "b": "second attribute"
  }
]
```

Das in dieser Antwort zurückgegebene Array könnte mit Themenregelaktionen verwendet werden, die `batchMode` unterstützen.

## trim(String)

Entfernt alle führenden und nachfolgenden Leerzeichen aus dem angegebenen `String`-Wert. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiel:

`Trim(" hi ")` = "hi"

| Argumenttyp | Ergebnis |
| --- | --- |
| `Int` | Die `String`-Darstellung des `Int`-Werts nach dem Entfernen der führenden und nachfolgenden Leerzeichen. |
| `Decimal` | Die `String`-Darstellung des `Decimal`-Werts nach dem Entfernen der führenden und nachfolgenden Leerzeichen. |
| `Boolean` | Die `String`-Darstellung des `Boolean`-Werts ("true" oder "false") nach dem Entfernen der führenden und nachfolge nden Leerzeichen. |
| `String` | Der `String`-Wert nach dem Entfernen der führenden und nachfolgenden Leerzeichen. |
| Array | Die `String`-Darstellung des `Array`-Werts mit Standardkonvertierungsregeln |
| Object | Die `String`-Darstellung des Objekts mit Standardkonvertierungsregeln |
| Null | `Undefined` . |
| Undefined | `Undefined` . |

## trunc(Decimal, Int)

Schneidet das erste Argument auf die Anzahl von `Decimal`-Stellen ab, die vom zweiten Argument festgelegt wurden. Wenn das zweite Argument kleiner ist als Null, wird es auf Null festgelegt. Wenn das zweite Argument größer ist als 34, wird es auf 34 festgelegt. Nachfolgende Nullen werden aus dem Ergebnis entfernt. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`trunc(2.3, 0)` = 2.

`trunc(2.3123, 2)` = 2,31.

`trunc(2.888, 2)` = 2,88.

`trunc(2.00, 5)` = 2.

| Argumenttyp 1 | Argumenttyp 2 | Ergebnis |
| --- | --- | --- |
| `Int` | `Int` | Der Quellwert |
| `Int/Decimal` | `Int/Decimal` | Das erste Argument wird auf die abgeschnitten, die vom zweiten beschrieben wird. Wenn das zw Argument kein `Int`-Wert ist, wir den nächsten `Int`-Wert abgeru |
| `Int/Decimal/String` | `Int/Decimal` | Das erste Argument wird auf die abgeschnitten, die vom zweiten beschrieben wird. Wenn das zw Argument kein `Int`-Wert ist, wir den nächsten `Int`-Wert abgeru `String`-Wert wird zu einem De konvertiert. Wenn die Konvertie Zeichenfolge fehlschlägt, ist das `Undefined` . |
| Anderer Wert | | `Undefined` . |

## upper(String)

Gibt die großgeschriebene Version des angegebenen `String`-Werts zurück. Andere Argumente als `String` werden mit der Standardkonvertierungsregeln in ,`String` konvertiert. Unterstützt von SQL Version 2015-10-08 und höher.

Beispiele:

`upper("hello")` = "HELLO"

`upper(["hello"])` = "[\"HELLO\"]"

## Literale

Sie können Literalobjekte in den SELECT- und WHERE-Klauseln Ihrer Regel-SQL direkt angeben, was zum Weitergeben von Informationen praktisch ist.

> **Note**
>
> Literale sind nur verfügbar, wenn Sie die SQL-Version vom 23.03.2016 oder höher verwenden.

Die JSON-Objektsyntax wird verwendet (Schlüssel-Wert-Paare, durch Trennzeichen getrennt, wobei Schlüssel Zeichenfolgen und Wert JSON-Werte sind, eingeschlossen in geschweifte Klammern: {}). Zum Beispiel:

Eingehende Nutzlast veröffentlicht für Topic `topic/subtopic`: `{"lat_long": [47.606,-122.332]}`

SQL-Anweisung: `SELECT {'latitude': get(lat_long, 0),'longitude':get(lat_long, 1)} as lat_long FROM 'topic/subtopic'`

Die resultierende ausgehende Nutzlast ist: `{"lat_long": {"latitude":47.606,"longitude":-122.332}}`.

Sie können auch Arrays in den SELECT- und WHERE-Klauseln Ihrer Regel-SQL direkt angeben, was Ihnen das Gruppieren von Informationen ermöglicht. Die JSON-Syntax wird verwendet (setzen Sie durch Trennzeichen getrennte Elemente zwischen eckige Klammern, [], um ein Arrayliteral zu erstellen). Zum Beispiel:

Eingehende Nutzlast veröffentlicht für Topic `topic/subtopic`: `{"lat": 47.696, "long": -122.332}`

SQL-Anweisung: `SELECT [lat,long] as lat_long FROM 'topic/subtopic'`

Verwenden Sie eine Austausch-Vorlage, um die JSON-Daten zu erhöhen, die zurückgegeben werden, wenn eine Regel ausgelöst wird und `{"lat_long": [47.606,-122.332]}` eine Maßnahme durchführt.

## Case-Anweisungen

Case-Anweisungen können zum Branchen verwendet werden, wie etwa eine switch-Anweisung.

Syntax:

```
CASE v WHEN t[1] THEN r[1]
  WHEN t[2] THEN r[2] ...
  WHEN t[n] THEN r[n]
  ELSE r[e] END
```

Der Ausdruck *v* wird ausgewertet und die Übereinstimmung mit dem Wert jeder *t[i]*-Klausel abgeglichen. `WHEN` Bei einer Übereinstimmung wird der entsprechende *r[i]*-Ausdruck zum Ergebnis der `CASE`-Anweisung. Die `WHEN`-Klauseln werden der Reihe nach ausgewertet, sodass, wenn es mehr als eine übereinstimmende Klausel gibt, das Ergebnis der ersten übereinstimmenden Klausel zum Ergebnis der `CASE`-Anweisung wird. Wenn es keine Treffer gibt, ist *r[e]* der`ELSE` Klausel das Ergebnis. Wenn es keine Übereinstimmung und keine `ELSE`-Klausel gibt, ist das Ergebnis `Undefined`.

Für `CASE`-Anweisungen ist mindestens eine `WHEN`-Klausel erforderlich. Eine `ELSE`-Klausel ist optional.

Zum Beispiel:

Eingehende Nutzlast veröffentlicht für Topic `topic/subtopic`:

```
{
    "color":"yellow"
}
```

SQL-Anweisung:

```
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 'topic/subtopic'
```

Die resultierende Ausgabenutzlast ist:

```
{
    "instructions":"caution"
```

```
}
```

> **Note**
>
> Wenn *v* `Undefined` ist, ist das Ergebnis der Case-Anweisung `Undefined`.

## JSON-Erweiterungen

Sie können die folgenden Erweiterungen für die ANSI SQL-Syntax verwenden, um die Arbeit mit verschachtelten JSON-Objekten zu vereinfachen.

"." Operator

Dieser Operator greift auf Elemente in eingebetteten JSON-Objekten zu und funktioniert genauso wie ANSI SQL und. JavaScript Zum Beispiel:

```
SELECT foo.bar AS bar.baz FROM 'topic/subtopic'
```

wählt den Wert der `bar`-Eigenschaft im `foo`-Objekt aus der folgenden Nachrichten-Payload aus, die an das `topic/subtopic`-Thema gesendet wurde.

```
{
  "foo": {
    "bar": "RED",
    "bar1": "GREEN",
    "bar2": "BLUE"
  }
}
```

Wenn ein JSON-Eigenschaftsname einen Bindestrich oder numerische Zeichen enthält, funktioniert die Notation „Punkt“ nicht. Stattdessen müssen Sie die Funktion get verwenden, um den Wert der Eigenschaft zu extrahieren.

In diesem Beispiel wird die folgende Nachricht an das `iot/rules`-Thema gesendet.

```
{
  "mydata": {
    "item2": {
```

```
      "0": {
        "my-key": "myValue"
      }
    }
  }
}
```

Normalerweise wird der Wert von `my-key` wie in dieser Abfrage identifiziert.

```
SELECT * from iot/rules WHERE mydata.item2.0.my-key= "myValue"
```

Da der Eigenschaftsname `my-key` jedoch einen Bindestrich und ein numerisches Zeichen `item2` enthält, muss die Funktion get verwendet werden, wie die folgende Abfrage zeigt.

```
SELECT * from 'iot/rules' WHERE get(get(get(mydata,"item2"),"0"),"my-key") = "myValue"
```

*-Operator

Dieser funktioniert genauso wie der Platzhalter * in ANSI SQL. Er wird nur in der SELECT-Klausel verwendet und erstellt ein neues JSON-Objekt, das die Nachrichtdaten enthält. Wenn die Nachrichtnutzlast nicht im JSON-Format vorliegt, gibt * die gesamte Nachrichtnutzlast als Rohbytes zurück. Zum Beispiel:

```
SELECT * FROM 'topic/subtopic'
```

Anwenden einer Funktion auf einen Attributwert

Im Folgenden finden Sie ein Beispiel für eine JSON-Nutzlast, die von einem Gerät veröffentlicht werden kann:

```
{
    "deviceid" : "iot123",
    "temp" : 54.98,
    "humidity" : 32.43,
    "coords" : {
        "latitude" : 47.615694,
        "longitude" : -122.3359976
    }
}
```

Das folgende Beispiel wendet eine Funktion auf einen Attributwert in einer JSON-Nutzlast an:

```
SELECT temp, md5(deviceid) AS hashed_id FROM topic/#
```

Das Ergebnis dieser Abfrage ist das folgende JSON-Objekt:

```
{
   "temp": 54.98,
   "hashed_id": "e37f81fb397e595c4aeb5645b8cbbbd1"
}
```

## Ersetzungsvorlagen

Sie können eine Ersatzvorlage verwenden, um die JSON-Daten zu erweitern, die zurückgegeben werden, wenn eine Regel ausgelöst wird und AWS IoT eine Aktion ausführt. Die Syntax für eine Substitutionsvorlage lautet *${* Ausdruck*}*, wobei Ausdruck ein beliebiger Ausdruck sein kann, der von INSELECT-Klauseln, AWS IoT WHERE-Klauseln und unterstützt wird. AWS IoT Regelaktionen Dieser Ausdruck kann in ein Aktionsfeld für eine Regel eingefügt werden, sodass Sie eine Aktion dynamisch konfigurieren können. Tatsächlich ersetzt diese Funktion eine Information in einer Aktion. Dazu gehören Funktionen, Operatoren und Informationen aus der ursprünglichen Nachrichtennutzlast.

> **Important**
>
> Da ein Ausdruck in einer Ersatzvorlage separat von dem „SELECT...“-Ausdruck evaluiert wird, können Sie nicht auf ein mit der AS-Klausel erstelltes Alias verweisen. Sie können zu den unterstützten Funktionen und Operatoren nur in der ursprünglichen Nutzlast vorhandene Informationen referenzieren.

Weitere Informationen zu unterstützten Ausdrücken unter AWS IoT SQL-Referenz.

Die folgenden Regelaktionen unterstützen Ersetzungsvorlagen. Jede Aktion unterstützt verschiedene Felder, die ersetzt werden können.

- Apache Kafka
- CloudWatch Alarme
- CloudWatch Logs

- CloudWatch Metriken
- DynamoDB
- Dynamo DBv2
- Elasticsearch
- HTTP
- IoT Analytics
- AWS IoT Events
- AWS IoT SiteWise
- Kinesis Data Streams
- Firehose
- Lambda
- Ort
- OpenSearch
- Wiederveröffentlichen
- S3
- SNS
- SQS
- Step Functions
- Timestream

Ersetzungsvorlagen werden in den Aktionsparametern innerhalb einer Regel angezeigt:

```
{
    "sql": "SELECT *, timestamp() AS timestamp FROM 'my/iot/topic'",
    "ruleDisabled": false,
    "actions": [{
        "republish": {
            "topic": "${topic()}/republish",
            "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"
        }
    }]
}
```

Wenn diese Regel vom folgenden in `my/iot/topic` veröffentlichten JSON ausgelöst wird:

```
{
    "deviceid": "iot123",
    "temp": 54.98,
    "humidity": 32.43,
    "coords": {
        "latitude": 47.615694,
        "longitude": -122.3359976
    }
}
```

Anschließend veröffentlicht diese Regel das folgende JSON-Format`my/iot/topic/republish`, das AWS IoT durch Folgendes ersetzt wird: `${topic()}/republish`

```
{
    "deviceid": "iot123",
    "temp": 54.98,
    "humidity": 32.43,
    "coords": {
        "latitude": 47.615694,
        "longitude": -122.3359976
    },
    "timestamp": 1579637878451
}
```

## Verschachtelte Objektabfragen

Sie können verschachtelte SELECT-Klauseln verwenden, um Attribute in Arrays und inneren JSON-Objekten abzufragen. Unterstützt von der SQL Version vom 23.03.2016 und höher.

Betrachten Sie die folgende MQTT-Meldung:

```
{
    "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 }
    ]
}
```

Example

Sie können Werte in ein neues Array mit der folgenden Regel konvertieren.

```
SELECT (SELECT VALUE n FROM e) as sensors FROM 'my/topic'
```

Die Regel generiert folgenden Output:

```
{
    "sensors": [
        "temperature",
        "light",
        "acidity"
    ]
}
```

Example

Mit derselben MQTT-Meldung können Sie auch einen bestimmten Wert innerhalb eines verschachtelten Objekts mit der folgenden Regel abfragen.

```
SELECT (SELECT v FROM e WHERE n = 'temperature') as temperature FROM 'my/topic'
```

Die Regel generiert folgenden Output:

```
{
    "temperature": [
        {
            "v": 22.5
        }
    ]
}
```

Example

Sie können die Ausgabe auch mit einer komplizierteren Regel glätten.

```
SELECT get((SELECT v FROM e WHERE n = 'temperature'), 0).v as temperature FROM 'topic'
```

Die Regel generiert folgenden Output:

```
{
    "temperature": 22.5
}
```

# Arbeiten mit binären Nutzlasten

Wenn Nachrichtennutzlasten als unformatierte binäre Daten behandelt werden sollen (und nicht als JSON-Objekt), können Sie den Operator * verwenden, um darauf in einer SELECT-Klausel zu verweisen.

In diesem Thema:


- Beispiele für binäre Nutzlasten
- Payloads von protobuf-Nachrichten entschlüsseln


## Beispiele für binäre Nutzlasten

Wenn Sie * verwenden, um die Nachrichtennutzlast als unformatierte Binärdaten zu bezeichnen, können Sie der Regel Daten hinzufügen. Wenn Sie eine leere oder eine JSON-Nutzlast haben, können der resultierenden Nutzlast mithilfe der Regel Daten hinzugefügt werden. Es folgen Beispiele unterstützter `SELECT`-Klauseln.

- Sie können die folgenden `SELECT`-Klauseln nur mit einem Sternchen (*) für binäre Payloads verwenden.
  - ```
    SELECT * FROM 'topic/subtopic'
    ```
  - ```
    SELECT * FROM 'topic/subtopic' WHERE timestamp() % 12 = 0
    ```
- Sie können auch Daten hinzufügen und die folgenden `SELECT`-Klauseln verwenden.
  - ```
    SELECT *, principal() as principal, timestamp() as time FROM 'topic/subtopic'
    ```
  - ```
    SELECT encode(*, 'base64') AS data, timestamp() AS ts FROM 'topic/subtopic'
    ```
- Sie können diese `SELECT`-Klauseln auch mit binären Payloads verwenden.
  - Das Folgende bezieht sich auf `device_type` in der WHERE-Klausel.

    ```
    SELECT * FROM 'topic/subtopic' WHERE device_type = 'thermostat'
    ```

- Folgendes wird ebenfalls unterstützt.

```
{
 "sql": "SELECT * FROM 'topic/subtopic'",
 "actions": [
  {
   "republish": {
    "topic": "device/${device_id}"
   }
  }
 ]
}
```

Die folgenden Regelaktionen unterstützen keine binären Payloads, sodass Sie sie dekodieren müssen.

- Für Regelaktionen, die die Eingabe binärer Nutzlast nicht unterstützen, wie z. B. die -Maßnahme, müssen Sie binäre Nutzlasten dekodieren. Die Lambda-Regelaktion kann binäre Daten empfangen, wenn sie base64-kodiert und in einer JSON-Nutzlast enthalten sind. Dazu müssen Sie die Regel folgendermaßen ändern:

```
SELECT encode(*, 'base64') AS data FROM 'my_topic'
```

- Die SQL-Anweisung unterstützt keine Zeichenfolge als Eingabe. Um eine String-Eingabe in JSON zu konvertieren, können Sie den folgenden Befehl ausführen.

```
SELECT decode(encode(*, 'base64'), 'base64') AS payload FROM 'topic'
```

## Payloads von protobuf-Nachrichten entschlüsseln

Protocol Buffers (protobuf) ist ein Open-Source-Datenformat, das zur Serialisierung strukturierter Daten in kompakter, binärer Form verwendet wird. Es wird verwendet, um Daten über Netzwerke zu übertragen oder in Dateien zu speichern. Mit Protobuf können Sie Daten in kleinen Paketgrößen und mit einer schnelleren Geschwindigkeit als mit anderen Nachrichtenformaten senden. AWS IoT Core Regeln unterstützen Protobuf, indem sie die SQL-Funktion decode (value, decodingScheme) bereitstellen, mit der Sie Protobuf-kodierte Nachrichtennutzdaten in das JSON-Format dekodieren und an nachgeschaltete Dienste weiterleiten können. In diesem Abschnitt wird der Prozess zur Konfiguration der Protobuf-Decodierung in Regeln beschrieben. step-by-step AWS IoT Core

In diesem Abschnitt:


- Voraussetzungen
- Deskriptordateien erstellen
- So laden Sie die Dateien zu einem S3-Bucket hoch
- Konfigurieren Sie die protobuf-Dekodierung in Regeln.
- Einschränkungen
- Bewährte Methoden


### Voraussetzungen

- Ein grundlegendes Verständnis von Protocol Buffers (protobuf)
- Die `.proto`-Dateien, die Nachrichtentypen und zugehörige Abhängigkeiten definieren
- Installieren Sie den protobuf Compiler (protoc) auf Ihrem System.

### Deskriptordateien erstellen

Wenn Sie bereits über die Deskriptordateien verfügen, können Sie diesen Schritt überspringen. Eine Deskriptordatei (`.desc`) ist eine kompilierte Version einer `.proto`-Datei, bei der es sich um eine Textdatei handelt, die die Datenstrukturen und Nachrichtentypen definiert, die bei einer protobuf-Serialisierung verwendet werden sollen. Um eine Deskriptordatei zu generieren, müssen Sie eine `.proto`-Datei definieren und sie mit dem protoc-Compiler kompilieren.

1. Erstellen Sie `.proto`-Dateien, die die Nachrichtentypen definieren. Ein Beispiel `.proto` könnte folgendermaßen aussehen:

   ```
   syntax = "proto3";

   message Person {
     optional string name = 1;
     optional int32 id = 2;
     optional string email = 3;
   }
   ```

   In dieser `.proto`-Beispieldatei verwenden Sie die Proto3-Syntax und definieren den Nachrichtentyp `Person`. Die `Person`-Nachrichtendefinition spezifiziert drei Felder (Name, ID und E-Mail). Weitere Informationen zu `.proto`-Dateiformaten im Language Guide (proto3).

2. Verwenden Sie den Protoc-Compiler, um die `.proto` Dateien zu kompilieren und eine Deskriptordatei zu generieren. Ein Beispielbefehl zum Erstellen einer Deskriptordatei (`.desc`) kann der folgende sein:

```
protoc --descriptor_set_out=<FILENAME>.desc \
    --proto_path=<PATH_TO_IMPORTS_DIRECTORY> \
    --include_imports \
    <PROTO_FILENAME>.proto
```

Dieser Beispielbefehl generiert eine Deskriptordatei`<FILENAME>.desc`, mit der AWS IoT Core Rules Protobuf-Payloads dekodieren kann, die der in definierten Datenstruktur entsprechen. `<PROTO_FILENAME>.proto`

- `--descriptor_set_out`

  Gibt den Namen der Deskriptordatei (`<FILENAME>.desc`) an, die generiert werden soll.

- `--proto_path`

  Gibt die Speicherorte aller importierten `.proto`-Dateien an, auf die in der kompilierten Datei verwiesen wird. Sie können das Kennzeichen mehrfach angeben, wenn Sie mehrere importierte `.proto`-Dateien mit unterschiedlichen Speicherorten haben.

- `--include_imports`

  Gibt an, dass alle importierten `.proto`-Dateien ebenfalls kompiliert und in die `<FILENAME>.desc`-Deskriptordatei aufgenommen werden sollen.

- `<PROTO_FILENAME>.proto`

  Gibt den Namen der `.proto`-Datei an, die Sie kompilieren möchten.

Weitere Informationen über die Protoc-Referenz finden Sie unter API-Referenz.

So laden Sie die Dateien zu einem S3-Bucket hoch

Nachdem Sie Ihre Deskriptordateien erstellt haben`<FILENAME>.desc`, laden Sie die Deskriptordateien `<FILENAME>.desc` mithilfe der AWS API, des AWS SDK oder der in einen Amazon S3 S3-Bucket hoch. AWS Management Console

Wichtige Überlegungen

- Stellen Sie sicher, dass Sie die Deskriptordateien in einen Amazon S3 S3-Bucket AWS-Konto in derselben Umgebung hochladen AWS-Region , in der Sie Ihre Regeln konfigurieren möchten.
- Stellen Sie sicher, dass Sie AWS IoT Core Zugriff auf das Lesen `FileDescriptorSet` von S3 gewähren. Wenn im S3-Bucket die serverseitige Verschlüsselung (SSE) deaktiviert ist oder wenn Ihr S3-Bucket mit von Amazon S3-verwalteten Schlüsseln (SSE-S3) verschlüsselt ist, sind keine zusätzlichen Richtlinienkonfigurationen erforderlich. Dies kann mit der Beispiel-Bucket-Richtlinie erreicht werden:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "Statement1",
   "Effect": "Allow",
   "Principal": {
    "Service": "iot.amazonaws.com"
   },
   "Action": "s3:Get*",
                    "Resource": "arn:aws:s3:::<BUCKET NAME>/<FILENAME>.desc"
  }
 ]
}
```

- Wenn Ihr S3-Bucket mit einem AWS Key Management Service Schlüssel (SSE-KMS) verschlüsselt ist, stellen Sie sicher, dass Sie beim Zugriff auf Ihren S3-Bucket die AWS IoT Core Erlaubnis zur Verwendung des Schlüssels erteilen. Dazu müssen Sie diese Erklärung zu Ihrer Schlüsselrichtlinie hinzufügen:

```
{
 "Sid": "Statement1",
 "Effect": "Allow",
 "Principal": {
  "Service": "iot.amazonaws.com"
 },
 "Action": [
  "kms:Decrypt",
  "kms:GenerateDataKey*",
  "kms:DescribeKey"
 ],
        "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
```

```
}
```

Konfigurieren Sie die protobuf-Dekodierung in Regeln.

Nachdem Sie die Deskriptordateien in Ihren Amazon S3 S3-Bucket hochgeladen haben, konfigurieren Sie eine Regel, die Ihr protobuf-Nachrichtennutzdatenformat mit der SQL-Funktion decode (value, decodingScheme) dekodieren kann. Eine ausführliche Funktionssignatur und ein Beispiel finden Sie in der SQL-Funktion decode (value, decodingScheme) der SQL-Referenz.AWS IoT

Im Folgenden finden Sie ein Beispiel für einen SQL-Ausdruck, der die Funktion decode (value, decodingScheme) verwendet:

```
SELECT VALUE decode(*, 'proto', '<BUCKET NAME>', '<FILENAME>.desc', '<PROTO_FILENAME>',
 '<PROTO_MESSAGE_TYPE>') FROM '<MY_TOPIC>'
```

In diesem Beispielausdruck:

- Sie verwenden die SQL-Funktion decode (value, DecodingScheme), um die Nutzdaten der binären Nachricht zu dekodieren, auf die von * verwiesen wird. Dies kann eine binäre protobuf-kodierte Nutzlast oder eine JSON-Zeichenfolge sein, die eine Base64-kodierte protobuf-Nutzlast darstellt.
- Die bereitgestellte Nachrichtennutzlast ist mit dem Nachrichtentyp `Person` definierten in `PROTO_FILENAME.proto` kodiert.
- Der benannte Amazon S3 S3-Bucket `BUCKET NAME` enthält das `FILENAME.desc` generierte von `PROTO_FILENAME.proto`.

Nachdem Sie die Konfiguration abgeschlossen haben, veröffentlichen Sie eine Nachricht zu AWS IoT Core dem Thema, das die Regel abonniert hat.

Einschränkungen

AWS IoT Core Regeln unterstützen Protobuf mit den folgenden Einschränkungen:

- Die Dekodierung von protobuf-Nachrichtennutzlasten innerhalb von Ersatzvorlagen wird nicht unterstützt.
- Beim Dekodieren von protobuf-Nachrichtennutzlasten können Sie die Funktion „SQL dekodieren“ innerhalb eines einzelnen SQL-Ausdrucks bis zu zweimal verwenden.

- Die maximale Größe der eingehenden Nutzlast beträgt 128 KiB (1 = 1024 Byte), die maximale Größe der ausgehenden Nutzlast beträgt 128 KiB und die maximale Größe für ein `FileDescriptorSet`-Objekt, das in einem Amazon S3-Bucket gespeichert ist, beträgt 32 KiB.
- Mit SSE-C-Verschlüsselung verschlüsselte Amazon S3 Buckets werden nicht unterstützt.

Bewährte Methoden

Nachfolgend Best Practices und Tipps zur Fehlerbehebung.

- Laden Sie die proto-Dateien in den Amazon S3 Bucket hoch.

  Es empfiehlt sich, die proto-Dateien zu sichern, falls etwas schief geht. Wenn Sie z. B. bei der Ausführung von protoc die proto-Dateien fälschlicherweise ohne Sicherungen ändern, kann dies zu Problemen in Ihrem Produktionsstapel führen. Es gibt mehrere Möglichkeiten, Dateien in einem Amazon S3-Bucket zu sichern. Sie können beispielsweise die Versionierung in S3-Buckets verwenden. Weitere Informationen zum Sichern von Dateien in Amazon S3-Buckets im Amazon S3 Developer Guide.
- Konfigurieren Sie die AWS IoT Protokollierung, um Protokolleinträge anzuzeigen.

  Es empfiehlt sich, die AWS IoT Protokollierung so zu konfigurieren, dass Sie die AWS IoT Protokolle für Ihr Konto überprüfen können CloudWatch. Wenn die SQL-Abfrage einer Regel eine externe Funktion aufruft, generiert AWS IoT Core Rules einen Protokolleintrag mit dem Wert `eventType` of`FunctionExecution`, der das Feld „Grund“ enthält, das Ihnen bei der Behebung von Fehlern hilft. Zu den möglichen Fehlern gehören ein Amazon S3 S3-Objekt, das nicht gefunden wurde, oder ein ungültiger protobuf-Dateideskriptor. Weitere Informationen zur Konfiguration der AWS IoT -Protokollierung und zum Anzeigen der Protokolleinträge unter AWS IoT Protokollierung konfigurieren und Protokolleinträge der Rules Engine.
- Aktualisieren Sie `FileDescriptorSet` mit einem neuen Objektschlüssel und aktualisieren Sie den Objektschlüssel in der Regel.

  Zum Aktualisieren von `FileDescriptorSet` laden Sie eine aktualisierte Deskriptordatei in den Amazon S3 S3-Bucket hoch. Es kann bis zu 15 Minuten dauern, bis `FileDescriptorSet`-Aktualisierungen angezeigt werden. Es empfiehlt sich, die aktualisierte `FileDescriptorSet` mit einem neuen Objektschlüssel hochzuladen und den Objektschlüssel in der Regel zu aktualisieren.

# SQL-Versionen

Die AWS IoT Regel-Engine verwendet eine SQL-ähnliche Syntax, um Daten aus MQTT-Nachrichten auszuwählen. Die SQL-Anweisungen werden auf Grundlage einer SQL-Version interpretiert, die mit der Eigenschaft `awsIotSqlVersion` in einem JSON-Dokument angegeben ist, welches die Regel beschreibt. Weitere Informationen zur Struktur von JSON-Regeldokumenten unter Erstellen einer Regel. Mit der `awsIotSqlVersion` Eigenschaft können Sie angeben, welche Version der AWS IoT SQL-Regel-Engine Sie verwenden möchten. Wenn eine neue Version bereitgestellt wird, können Sie weiterhin eine frühere Version verwenden oder die Regel ändern, damit sie die neue Version nutzt. Die aktuellen Regeln verwenden weiterhin die Version, mit der sie erstellt wurden.

Das folgende JSON-Beispiel zeigt, wie die SQL-Version mit der Eigenschaft `awsIotSqlVersion` angegeben wird:

```
{
    "sql": "expression",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
        "republish": {
            "topic": "my-mqtt-topic",
            "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"
        }
    }]
}
```

AWS IoT unterstützt derzeit die folgenden SQL-Versionen:

- `2016-03-23` – Die SQL-Version von 23.03.2016 (empfohlen).
- `2015-10-08` – Die ursprüngliche SQL-Version von 08.10.2015.
- `beta` – Die neueste Beta-SQL-Version. Mit dieser Version können Sie die Regeln grundlegend ändern.

## Neuerungen in der Version der SQL-Regel-Engine vom 23.03.2016

- Lösungen für das Auswählen verschachtelter JSON-Objekte
- Lösungen für Array-Abfragen

- Unterstützung von Intra-Objektabfragen. Weitere Informationen finden Sie unter Verschachtelte Objektabfragen.
- Unterstützung zum Ausgeben eines Arrays als oberstes Objekt
- Hinzufügen der `encode(value, encodingScheme)`-Funktion, die auf JSON- und Nicht-JSON-Formatdaten angewendet werden kann. Weitere Informationen finden Sie unter Encode-Funktion.

### Ausgeben von **`Array`** als oberstes Objekt

Diese Funktion ermöglicht eine Regel, mit der ein Array als oberstes Objekt zurückgegeben wird. Als Beispiel dient etwa die folgende MQTT-Nachricht:

```
{
    "a": {"b":"c"},
    "arr":[1,2,3,4]
}
```

Und die folgende Regel:

```
SELECT VALUE arr FROM 'topic'
```

Die Regel generiert folgenden Output:

```
[1,2,3,4]
```

# AWS IoT Device Shadow-Dienst

Der AWS IoT Device Shadow-Dienst fügt AWS IoT Dingobjekten Schatten hinzu. Durch Schatten kann der Status eines Geräts Apps und anderen Diensten zur Verfügung gestellt werden, unabhängig davon, ob das Gerät mit dem Gerät verbunden ist AWS IoT oder nicht. AWS IoT Dingobjekte können mehrere benannte Schatten haben, sodass Ihre IoT-Lösung mehr Optionen für die Verbindung Ihrer Geräte mit anderen Apps und Diensten bietet.

AWS IoT Ding-Objekte haben keine Schatten, bis sie explizit erstellt werden. Schatten können mithilfe der AWS IoT Konsole erstellt, aktualisiert und gelöscht werden. Geräte, andere Webclients und Services können Schatten erstellen, aktualisieren und löschen mithilfe von MQTT und den reservierten MQTT-Themen; HTTP mithilfe der Geräteschatten-REST-API; und der AWS CLI für AWS IoT Da Schatten AWS in der Cloud gespeichert werden, können sie Gerätestatusdaten von Apps und anderen Cloud-Diensten sammeln und melden, unabhängig davon, ob das Gerät verbunden ist oder nicht.

## Verwendung von Schatten

Schatten bieten einen zuverlässigen Datenspeicher für Geräte, Anwendungen und andere Cloud-Services, um Daten gemeinsam zu nutzen. Sie ermöglichen es Geräten, Anwendungen und anderen Cloud-Services, eine Verbindung herzustellen und zu trennen, ohne den Status eines Geräts zu verlieren.

Geräte, Apps und andere Cloud-Dienste sind zwar mit ihnen verbunden AWS IoT, können aber über deren Schatten auf den aktuellen Status eines Geräts zugreifen und diesen kontrollieren. Eine App kann beispielsweise eine Änderung des Gerätestatus anfordern, indem sie einen Schatten aktualisiert. AWS IoT veröffentlicht eine Nachricht, die auf die Änderung des Geräts hinweist. Das Gerät empfängt diese Nachricht, aktualisiert seinen Status so, dass er übereinstimmt, und veröffentlicht eine Nachricht mit dem aktualisierten Status. Der Geräteschatten-Service spiegelt diesen aktualisierten Status im entsprechenden Schatten wider. Die Anwendung kann das Update des Schattens abonnieren oder den Schatten nach seinem aktuellen Status abfragen.

Wenn ein Gerät offline geht, kann eine App immer noch mit AWS IoT den Schatten des Geräts kommunizieren. Wenn das Gerät erneut eine Verbindung herstellt, erhält es den aktuellen Status seiner Schatten. Das Gerät kann seinen Status so aktualisieren, dass er mit dem seiner Schatten übereinstimmt, und dann eine Nachricht mit dem aktualisierten Status veröffentlichen. Wenn eine Anwendung offline ist und sich der Gerätestatus ändert, während sie offline ist, hält das Gerät den

Schatten aktualisiert, damit die Anwendung die Schatten nach seinem aktuellen Status abfragen kann, wenn sie erneut eine Verbindung herstellt.

Wenn die Geräte häufig offline sind und Sie die Geräte so konfigurieren möchten, dass sie Deltameldungen empfangen, nachdem sie wieder eine Verbindung hergestellt haben, können Sie die Funktion für persistente Sitzungen verwenden. Weitere Informationen zum Ablauf der persistenten Sitzung finden Sie unter Ablauffrist für persistente Sitzungen.

## Auswählen der Verwendung benannter oder unbenannter Schatten

Der Geräteschatten-Service unterstützt benannte und unbenannte (klassische) Schatten. Ein Objekt kann mehrere benannte Schatten und nicht mehr als einen unbenannten, klassischen Schatten haben. Das Objekt kann auch einen reservierten benannten Schatten haben, der ähnlich wie ein benannter Schatten funktioniert, außer dass Sie seinen Namen nicht aktualisieren können. Weitere Informationen finden Sie unter Reservierter benannter Schatten.

Ein Objekt kann sowohl benannte als auch unbenannte Schatten gleichzeitig haben. Die API, die für den jeweiligen Zugriff verwendet wird, unterscheidet sich jedoch leicht. Daher ist es möglicherweise effizienter, zu entscheiden, welcher Schattentyp für Ihre Lösung am besten geeignet ist, und nur diesen Typ zu verwenden. Weitere Informationen zur API für den Zugriff auf die Schatten finden Sie unter Schatten-Themen.

Mit benannten Schatten können Sie verschiedene Ansichten des Status eines Objekts erstellen. Beispielsweise könnten Sie ein Objekt mit vielen Eigenschaften in Schatten mit logischen Eigenschaftengruppen unterteilen, die jeweils durch einen Schattennamen gekennzeichnet sind. Sie können den Zugriff auf Eigenschaften auch einschränken, indem Sie sie in verschiedene Schatten gruppieren und Richtlinien verwenden, um den Zugriff zu steuern. Weitere Informationen zu Richtlinien, die mit Geräteschatten verwendet werden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT und AWS IoT Core Richtlinien.

Die klassischen, unbenannten Schatten sind einfacher, aber etwas stärker eingeschränkt als die benannten Schatten. Jedes AWS IoT Objekt kann nur einen unbenannten Schatten haben. Wenn Sie erwarten, dass Ihre IoT-Lösung nur einen begrenzten Bedarf an Schattendaten hat, sollten Sie auf diese Weise mit der Verwendung von Schatten beginnen. Wenn Sie jedoch der Meinung sind, dass Sie in Zukunft weitere Schatten hinzufügen möchten, sollten Sie von Anfang an benannte Schatten verwenden.

Die Flottenindizierung unterstützt unbenannte Schatten und benannte Schatten unterschiedlich. Weitere Informationen finden Sie unter Verwalten der Flottenindizierung.

# Zugreifen auf Schatten

Jeder Schatten verfügt über ein reserviertes MQTT-Thema und eine HTTP-URL, die die `get`-, `update`- und `delete`-Aktionen für den Schatten unterstützt.

Schatten verwenden JSON-Schattendokumente zum Speichern und Abrufen von Daten. Das Dokument eines Schattens enthält eine Statuseigenschaft, die die folgenden Aspekte des Gerätezustands beschreibt:

- `desired`

  Apps geben die gewünschten Status der Geräteeigenschaften an, indem sie das `desired`-Objekt aktualisieren.
- `reported`

  Geräte melden ihren aktuellen Status im `reported`-Objekt.
- `delta`

  AWS IoT meldet Unterschiede zwischen dem gewünschten und dem gemeldeten Zustand des `delta` Objekts.

Die in einem Schatten gespeicherten Daten werden durch die Statuseigenschaft des Nachrichtentexts der Aktualisierungsaktion bestimmt. Nachfolgende Aktualisierungsaktionen können die Werte eines vorhandenen Datenobjekts ändern und Schlüssel und andere Elemente im Zustandsobjekt des Schattens hinzufügen und löschen. Weitere Informationen zum Zugriff auf Schatten finden Sie unter Verwenden von Schatten in Geräten und Verwenden von Schatten in Apps und Services.

> **Important**
>
> Die Berechtigung, Aktualisierungsanforderungen zu stellen, sollte auf vertrauenswürdige Apps und Geräte beschränkt sein. Dadurch wird verhindert, dass die Statuseigenschaft des Schattens unerwartet geändert wird. Andernfalls sollten die Geräte und Apps, die den Schatten verwenden, so konzipiert werden, dass sie erwarten, dass sich die Schlüssel in der Statuseigenschaft ändern.

## Verwenden von Schatten in Geräten, Apps und anderen Cloudservices

Die Verwendung von Schatten in Geräten, Apps und anderen Cloudservices erfordert Konsistenz und Koordination zwischen all diesen Services. Der AWS IoT Device Shadow-Dienst speichert den Shadow-Status, sendet Nachrichten, wenn sich der Shadow-Status ändert, und reagiert auf Nachrichten, die seinen Status ändern. Die Geräte, Apps und anderen Cloud-Services in Ihrer IoT-Lösung müssen ihren Status verwalten und den Status des Geräteschattens konsistent halten.

Die Schattenstatusdaten sind dynamisch und können von Geräten, Apps und anderen Cloud-Services mit Berechtigung zum Zugriff auf den Schatten geändert werden. Aus diesem Grund ist es wichtig zu berücksichtigen, wie jedes Gerät, jede App und jeder andere Cloud-Service mit dem Schatten interagiert. Zum Beispiel:

- Geräte sollten nur in die `reported`-Eigenschaft des Schattenstatus schreiben, wenn Statusdaten an den Schatten übertragen werden.
- Apps und andere Cloud-Services sollten nur in die `desired`-Eigenschaft schreiben, wenn Statusänderungsanforderungen über den Schatten an das Gerät übermittelt werden.

> **Important**
>
> Die in einem Schattendatenobjekt enthaltenen Daten sind unabhängig von anderen Schatten und anderen Objekteigenschaften, z. B. den Attributen eines Objekts und dem Inhalt von MQTT-Nachrichten, die das Gerät eines Objekts veröffentlichen könnte. Ein Gerät kann jedoch bei Bedarf dieselben Daten in verschiedenen MQTT-Themen und -Schatten melden. Ein Gerät, das mehrere Schatten unterstützt, muss die Konsistenz der Daten aufrechterhalten, die es in den verschiedenen Schatten meldet.

## Nachrichtenreihenfolge

Es gibt keine Garantie dafür, dass Nachrichten des AWS IoT Dienstes in einer bestimmten Reihenfolge auf dem Gerät ankommen. Das folgende Szenario zeigt, was in diesem Fall passiert.

Ursprüngliches Statusdokument:

```
{
  "state": {
    "reported": {
```

```
      "color": "blue"
    }
  },
  "version": 9,
  "timestamp": 123456776
}
```

Aktualisierung 1:

```
{
  "state": {
    "desired": {
      "color": "RED"
    }
  },
  "version": 10,
  "timestamp": 123456777
}
```

Aktualisierung 2:

```
{
  "state": {
    "desired": {
      "color": "GREEN"
    }
  },
  "version": 11,
  "timestamp": 123456778
}
```

Endgültiges Statusdokument:

```
{
  "state": {
    "reported": {
      "color": "GREEN"
    }
  },
  "version": 12,
  "timestamp": 123456779
}
```

Dies führt zu zwei Delta-Nachrichten:

```
{
  "state": {
    "color": "RED"
  },
  "version": 11,
  "timestamp": 123456778
}
```

```
{
  "state": {
    "color": "GREEN"
  },
  "version": 12,
  "timestamp": 123456779
}
```

Das Gerät kann diese Nachrichten ohne feste Reihenfolge erhalten. Da der Status in diesen Nachrichten kumulativer Natur ist, kann ein Gerät Nachrichten, die eine Versionsnummer enthalten, die älter ist als die, die es verfolgt, sicher verwerfen. Erhält das Gerät das Delta für die Version 12 vor der Version 11 kann es die Nachricht zur Version 11 sicher verwerfen.

## Kürzen von Shadow-Nachrichten

Um die Größe der Schatten-Nachrichten, die an Ihr Gerät gesendet werden, zu reduzieren, legen Sie eine Regel fest, mit der nur die Felder, die Ihr Gerät benötigt, ausgewählt und die Nachricht in einem MQTT-Thema, das Ihr Gerät überwacht, erneut veröffentlicht werden.

Die Regel wird in der JSON vorgegeben und sollte wie folgt aussehen:

```
{
  "sql": "SELECT state, version FROM '$aws/things/+/shadow/update/delta'",
  "ruleDisabled": false,
  "actions": [
    {
      "republish": {
        "topic": "${topic(3)}/delta",
        "roleArn": "arn:aws:iam:123456789012:role/my-iot-role"
      }
    }
  ]
```

```
}
```

Mit der SELECT-Anweisung wird festgelegt, welche Felder der Nachricht im vorgegebenen Topic erneut veröffentlicht werden. Der Platzhalter "+" wird verwendet, um allen Schattennamen zu entsprechen. Mit der Regel wird festgelegt, dass alle passenden Nachrichten im vorgegebenen Topic erneut veröffentlicht werden sollen. In diesem Fall wird die Funktion `"topic()"` verwendet, um das Thema anzugeben, in dem erneut eine Veröffentlichung erfolgen soll. `topic(3)` ermittelt den Objektnamen im Ursprungs-Thema. Weitere Informationen zum Erstellen von Regeln finden Sie unter Regeln für AWS IoT.

## Verwenden von Schatten in Geräten

In diesem Abschnitt wird die Gerätekommunikation mit Shadows mithilfe von MQTT-Nachrichten beschrieben, der bevorzugten Methode für Geräte zur Kommunikation mit dem AWS IoT Device Shadow-Dienst.

Shadow-Kommunikation emuliert ein request/response model using the publish/subscribe Kommunikationsmodell von MQTT. Jede Schattenaktion besteht aus einem Anforderungsthema, einem Thema für erfolgreiche Antworten (`accepted`) und einem Thema für Fehlerantworten (`rejected`).

Informationen dazu, ob Apps und Services feststellen können, ob ein Gerät verbunden ist, finden Sie unter Erkennen, dass ein Gerät verbunden ist.

> **Important**
>
> Da MQTT ein Veröffentlichen-/Abonnieren-Kommunikationsmodell verwendet, müssen Sie die Antwortthemen abonnieren, bevor Sie ein Anfrage-Thema veröffentlichen. Wenn Sie dies nicht tun, erhalten Sie keine Antwort auf die Anfrage, die Sie veröffentlichen.
> Wenn Sie einen verwenden AWS IoT Device SDK, um den Device Shadow-Dienst aufzurufen APIs, wird dies für Sie erledigt.

Die Beispiele in diesem Abschnitt verwenden eine verkürzte Form des Themas, wobei sich der Begriff entweder auf einen benannten oder einen unbenannten Schatten beziehen *`ShadowTopicPrefix`* kann, wie in dieser Tabelle beschrieben.

Schatten können benannt oder unbenannt sein (klassisch). Die jeweils verwendeten Themen unterscheiden sich nur durch das Themenpräfix. In dieser Tabelle wird das Themenpräfix angezeigt, das von jedem Schattentyp verwendet wird.

| *ShadowTopicPrefix* Wert | Schattentyp |
| --- | --- |
| `$aws/things/ thingName /shadow` | Unbenannter (klassischer) Schatten |
| `$aws/things/ thingName /shadow/name/ shadowName` | Benannter Schatten |

> **Important**
>
> Stellen Sie sicher, dass die Verwendung der Schatten durch Ihre App oder Ihren Service konsistent ist und von den entsprechenden Implementierungen auf Ihren Geräten unterstützt wird. Bedenken Sie beispielsweise, wie Schatten erstellt, aktualisiert und gelöscht werden. Berücksichtigen Sie auch, wie Updates auf dem Gerät und in den Apps oder Services behandelt werden, die über einen Schatten auf das Gerät zugreifen. Ihr Design sollte klar angeben, wie der Zustand des Geräts aktualisiert und gemeldet wird und wie Ihre Apps und Services mit dem Gerät und seinen Schatten interagieren.

Um ein vollständiges Thema zu erstellen, wählen Sie *ShadowTopicPrefix* als Schattentyp aus, auf den Sie verweisen möchten. Ersetzen Sie *thingName* und *shadowName* mit den entsprechenden Werten, wenn zutreffend. Fügen Sie anschließend den Themen-Stub an wie in der folgenden Tabelle dargestellt. Denken Sie daran, dass bei Themen zwischen Groß- und Kleinschreibung unterschieden wird.

Weitere Informationen zu den reservierten Themen für Schatten finden Sie unter Schatten-Themen.

## Initialisierung des Geräts bei der ersten Verbindung zu AWS IoT

Nachdem sich ein Gerät bei registriert hat AWS IoT, sollte es diese MQTT-Nachrichten für die Shadows abonnieren, die es unterstützt.

| Thema | Bedeutung | Aktion, die ein Gerät ausführen sollte, wenn dieses Thema empfangen wird |
|---|---|---|
| *ShadowTopicPrefix* / delete/accepted | Die delete Anfrage wurde akzeptiert und der Shadow wurde AWS IoT gelöscht. | Die Aktionen, die für den gelöschten Schatten erforderl ich sind, z. B. das Beenden der Veröffentlichung von Aktualisierungen. |
| *ShadowTopicPrefix* / delete/rejected | Die delete Anfrage wurde von abgelehnt AWS IoT und der Shadow wurde nicht gelöscht. Der Nachrichtentext enthält die Fehlerinformatione n. | Reagieren Sie auf die Fehlermeldung im Nachricht entext. |
| *ShadowTopicPrefix* / get/accepted | Die get Anfrage wurde von akzeptiert AWS IoT, und der Nachrichtentext enthält das aktuelle Shadow-Dokument. | Die Aktionen, die erforderl ich sind, um das Statusdok ument im Nachrichtentext zu verarbeiten. |
| *ShadowTopicPrefix* / get/rejected | Die get Anfrage wurde von abgelehnt AWS IoT, und der Nachrichtentext enthält die Fehlerinformationen. | Reagieren Sie auf die Fehlermeldung im Nachricht entext. |
| *ShadowTopicPrefix* / update/accepted | Die update Anfrage wurde von akzeptiert AWS IoT, und der Nachrichtentext enthält das aktuelle Schattend okument. | Bestätigen Sie, dass die aktualisierten Daten im Nachrichtentext mit dem Gerätestatus übereinstimmen. |
| *ShadowTopicPrefix* / update/rejected | Die update Anfrage wurde von abgelehnt AWS IoT, und der Nachrichtentext enthält die Fehlerinformationen. | Reagieren Sie auf die Fehlermeldung im Nachricht entext. |

| Thema | Bedeutung | Aktion, die ein Gerät ausführen sollte, wenn dieses Thema empfangen wird |
|---|---|---|
| *ShadowTopicPrefix* /update/delta | Das Schattendokument wurde durch eine Anfrage an aktualisiert AWS IoT, und der Nachrichtentext enthält die angeforderten Änderungen. | Aktualisieren Sie den Gerätestatus so, dass er mit dem gewünschten Status im Nachrichtentext übereinst immt. |
| *ShadowTopicPrefix* /update/documents | Eine Aktualisierung des Schattens wurde kürzlich abgeschlossen, und der Nachrichtentext enthält das aktuelle Schattendokument. | Bestätigen Sie, dass der aktualisierte Status im Nachrichtentext mit dem Gerätestatus übereinstimmt. |

Nach dem Abonnieren der Nachrichten in der obigen Tabelle für jeden Schatten sollte das Gerät testen, ob die Schatten, die es unterstützt, bereits erstellt wurden, indem es ein `/get`-Thema in jedem Schatten veröffentlicht. Wenn eine `/get/accepted`-Nachricht empfangen wird, enthält der Nachrichtentext das Schattendokument, mit dem das Gerät seinen Status initialisieren kann. Wenn eine `/get/rejected`-Nachricht empfangen wird, sollte der Schatten erstellt werden, indem eine `/update`-Nachricht mit dem aktuellen Gerätestatus veröffentlicht wird.

Nehmen wir zum Beispiel an, Sie haben ein Objekt `My_IoT_Thing`, das keine klassischen oder benannten Schatten hat. Wenn Sie jetzt eine `/get`-Anfrage zum reservierten Thema `$aws/things/My_IoT_Thing/shadow/get` veröffentlichen, erhält das `$aws/things/My_IoT_Thing/shadow/get/rejected` Thema einen Fehler, da das Objekt keine Schatten hat. Um diesen Fehler zu beheben, veröffentlichen Sie zunächst eine `/update`-Nachricht, indem Sie das `$aws/things/My_IoT_Thing/shadow/update` Thema mit dem aktuellen Gerätestatus verwenden, z. B. die folgende Payload.

```
{
 "state": {
  "reported": {
   "welcome": "aws-iot",
   "color": "yellow"
  }
 }
```

```
}
```

Für das Objekt wird jetzt ein klassischer Schatten erstellt, und die Nachricht wird auf dem `$aws/things/My_IoT_Thing/shadow/update/accepted`-Thema veröffentlicht. Wenn Sie zu dem Thema `$aws/things/My_IoT_Thing/shadow/get` veröffentlichen, wird eine Antwort auf das `$aws/things/My_IoT_Thing/shadow/get/accepted`-Thema mit dem Gerätestatus zurückgegeben.

Bei benannten Schatten müssen Sie zuerst den benannten Schatten erstellen oder ein Update mit dem Schatten-Namen veröffentlichen, bevor Sie die GET-Anfrage verwenden können. Um beispielsweise einen benannten Schatten `namedShadow1` zu erstellen, müssen Sie zunächst die Informationen zum Gerätestatus für das Thema veröffentlichen`$aws/things/My_IoT_Thing/shadow/name/namedShadow1/update`. Um die Statusinformationen abzurufen, verwenden Sie die `/get`-Anfrage für den benannten Schatten, `$aws/things/My_IoT_Thing/shadow/name/namedShadow1/get`.

## Nachrichten werden verarbeitet, während das Gerät angeschlossen ist AWS IoT

Solange ein Gerät verbunden ist AWS IoT, kann es /update/delta-Meldungen empfangen und sollte den Gerätestatus an die Änderungen in seinem Schatten anpassen, indem es:

1. Lesen aller empfangenen /update/delta-Nachrichten und entsprechende Anpassung des Gerätestatus.
2. Veröffentlichen einer /update-Nachricht mit einem `reported`-Nachrichtentext, der den aktuellen Status des Geräts hat, wenn sich der Gerätestatus ändert.

Solange ein Gerät angeschlossen ist, sollte es diese Meldungen veröffentlichen, wenn angezeigt.

| Indikation | Thema | Nutzlast |
| --- | --- | --- |
| Der Zustand des Geräts hat sich geändert. | *ShadowTopicPrefix* `/update` | Ein Schattendokument mit der `reported`-Eigenschaft. |
| Das Gerät wird möglicher weise nicht mit dem Schatten synchronisiert. | *ShadowTopicPrefix* `/get` | (empty) |

| Indikation | Thema | Nutzlast |
| --- | --- | --- |
| Eine Aktion auf dem Gerät zeigt an, dass ein Schatten vom Gerät nicht mehr unterstützt wird, z. B. wenn das Gerät entfernt oder ersetzt wird. | *ShadowTopicPrefix* / delete | (empty) |

## Nachrichten werden verarbeitet, wenn das Gerät wieder eine Verbindung herstellt mit AWS IoT

Wenn ein Gerät mit einem oder mehreren Schatten eine Verbindung herstellt AWS IoT, sollte es seinen Status mit dem aller Schatten synchronisieren, die es unterstützt, und zwar wie folgt:

1. Lesen aller empfangenen /update/delta-Nachrichten und entsprechende Anpassung des Gerätestatus.
2. Veröffentlichen einer /update-Nachricht mit einem `reported`-Nachrichtentext, der den aktuellen Status des Geräts hat.

# Verwenden von Schatten in Apps und Services

In diesem Abschnitt wird beschrieben, wie eine App oder ein Dienst mit dem AWS IoT Device Shadow-Dienst interagiert. In diesem Beispiel wird davon ausgegangen, dass die App oder der Service nur mit dem Schatten und darüber dem Gerät interagiert. In diesem Beispiel sind keine Verwaltungsaktionen enthalten, z. B. das Erstellen oder Löschen von Schatten.

In diesem Beispiel wird die REST-API des AWS IoT Device Shadow-Dienstes verwendet, um mit Schatten zu interagieren. Im Gegensatz zu dem in verwendeten BeispielVerwenden von Schatten in Geräten, das ein publish/subscribe communications model, this example uses the request/response Kommunikationsmodell der REST-API verwendet. Das bedeutet, dass die App oder der Dienst eine Anfrage stellen muss, bevor sie eine Antwort von erhalten kann AWS IoT. Ein Nachteil dieses Modells ist jedoch, dass es keine Benachrichtigungen unterstützt. Wenn Ihre App oder Ihr Service rechtzeitige Benachrichtigungen über Änderungen des Gerätestatus erfordert, sollten Sie die Protokolle MQTT oder MQTT über WSS-Protokolle berücksichtigen, die das für Veröffentlichen/

Abonnieren-Kommunikationsmodell unterstützen, wie unter Verwenden von Schatten in Geräten beschrieben.

> **Important**
>
> Stellen Sie sicher, dass die Verwendung der Schatten Ihrer App oder Ihres Services mit den entsprechenden Implementierungen in Ihren Geräten konsistent ist und von diesen unterstützt wird. Berücksichtigen Sie beispielsweise, wie Schatten erstellt, aktualisiert und gelöscht werden und wie Updates auf dem Gerät und in den Apps oder Services, die auf den Schatten zugreifen, gehandhabt werden. In Ihrem Design sollte klar angegeben werden, wie der Zustand des Geräts aktualisiert und gemeldet wird und wie Ihre Apps und Services mit dem Gerät und seinen Schatten interagieren.

Die URL der REST-API für einen benannten Schatten lautet:

```
https://endpoint/things/thingName/shadow?name=shadowName
```

und für einen unbenannten Schatten:

```
https://endpoint/things/thingName/shadow
```

Wobei:

Endpunkt

Der vom CLI-Befehl zurückgegebene Endpunkt:

```
aws iot describe-endpoint --endpoint-type IOT:Data-ATS
```

thingName

Der Name des Objekts, zu dem der Schatten gehört

shadowName

Der Name des benannten Schattens. Dieser Parameter wird mit unbenannten Schatten nicht verwendet.

## Initialisierung der App oder des Dienstes bei der Verbindung zu AWS IoT

Wenn die App zum ersten Mal eine Verbindung herstellt AWS IoT, sollte sie eine HTTP-GET-Anfrage an den URLs Schatten senden, den sie verwendet, um den aktuellen Status der Schatten abzurufen, die sie verwendet. Dies ermöglicht es, die App oder den Service mit dem Schatten zu synchronisieren.

## Der Verarbeitungsstatus ändert sich, während die App oder der Dienst verbunden ist AWS IoT

Solange die App oder der Dienst verbunden ist AWS IoT, kann sie den aktuellen Status regelmäßig abfragen, indem sie eine HTTP-GET-Anfrage an die URLs von ihr verwendeten Shadows sendet.

Wenn ein Endbenutzer mit der App oder dem Dienst interagiert, um den Status des Geräts zu ändern, kann die App oder der Dienst eine HTTP-POST-Anfrage an den URLs Shadow senden, mit dem sie den `desired` Status des Shadows aktualisiert. Diese Anforderung gibt die Änderung zurück, die akzeptiert wurde, aber Sie müssen möglicherweise den Schatten abfragen, indem Sie HTTP-GET-Anforderungen vornehmen, bis das Gerät den Schatten mit seinem neuen Status aktualisiert hat.

## Erkennen, dass ein Gerät verbunden ist

Um festzustellen, ob ein Gerät derzeit verbunden ist, schließen Sie eine `connected`-Eigenschaft in das Schattendokument ein und verwenden eine MQTT Last Will and Testament (LWT)-Meldung, um die `connected`-Eigenschaft auf `false` festzulegen, wenn ein Gerät aufgrund eines Fehlers getrennt wird.

> **Note**
>
> MQTT-LWT-Nachrichten, die an AWS IoT reservierte Themen (Themen, die mit $ beginnen) gesendet werden, werden vom AWS IoT Device Shadow-Dienst ignoriert. Sie werden jedoch von abonnierten Clients und von der AWS IoT Rules Engine verarbeitet, sodass Sie eine LWT-Nachricht erstellen müssen, die an ein nicht reserviertes Thema gesendet wird, und eine Regel, die die MQTT-LWT-Nachricht als Shadow-Update-Nachricht für das reservierte Update-Thema des Shadows erneut veröffentlicht. *`ShadowTopicPrefix`*`/update`

So senden Sie dem Device Shadow-Service eine LWT-Nachricht

1. Erstellen Sie eine Regel, die die MQTT LWT-Nachricht im reservierten Thema erneut veröffentlicht. Das folgende Beispiel ist eine Regel, die auf Nachrichten zu dem `my/things/myLightBulb/update`-Thema wartet und sie erneut in `$aws/things/myLightBulb/shadow/update` veröffentlicht.

```
{
    "rule": {
    "ruleDisabled": false,
    "sql": "SELECT * FROM 'my/things/myLightBulb/update'",
    "description": "Turn my/things/ into $aws/things/",
    "actions": [
        {
        "republish": {
            "topic": "$$aws/things/myLightBulb/shadow/update",
            "roleArn": "arn:aws:iam:123456789012:role/aws_iot_republish"
            }
        }
     ]
   }
}
```

2. Wenn das Gerät eine Verbindung herstellt AWS IoT, registriert es eine LWT-Nachricht zu einem nicht reservierten Thema, damit die Regel zur erneuten Veröffentlichung diese erkennt. In diesem Beispiel ist dieses Thema `my/things/myLightBulb/update`, und die verbundene Eigenschaft wird auf `false` festgelegt.

```
{
    "state": {
        "reported": {
            "connected":"false"
        }
    }
}
```

3. Nach der Verbindung veröffentlicht das Gerät eine Nachricht zu seinem Shadow-Update-Thema, `$aws/things/myLightBulb/shadow/update`, um seinen aktuellen Status zu melden, einschließlich der Einstellung seiner `connected`-Eigenschaft auf `true`.

```
{
```

```
     "state": {
        "reported": {
            "connected":"true"
        }
    }
}
```

4. Bevor das Gerät die Verbindung ordnungsgemäß trennt, veröffentlicht es eine Nachricht zu seinem Schattenaktualisierungsthema, `$aws/things/myLightBulb/shadow/update`, um seinen neuesten Status zu melden, einschließlich der Einstellung seiner `connected`-Eigenschaft auf `false`.

```
{
    "state": {
        "reported": {
            "connected":"false"
        }
    }
}
```

5. Wenn das Gerät aufgrund eines Fehlers die Verbindung trennt, veröffentlicht der AWS IoT Message Broker die LWT-Nachricht des Geräts im Namen des Geräts. Die Regel zum erneuten Veröffentlichen erkennt diese Nachricht und veröffentlicht die Schattenaktualisierungsmeldung, um die `connected`-Eigenschaft des Geräteschattens zu aktualisieren.

# Simulieren der Device Shadow-Servicekommunikation

In diesem Thema wird veranschaulicht, wie der Device Shadow-Service als Vermittler fungiert und es Geräten und Apps ermöglicht, einen Schatten zum Aktualisieren, Speichern und Abrufen des Status eines Geräts zu verwenden.

Um die in diesem Thema beschriebene Interaktion zu demonstrieren und sie weiter zu untersuchen, benötigen Sie ein AWS-Konto und ein System, auf dem Sie das ausführen können. AWS CLI Wenn Sie diese nicht haben, können Sie die Interaktion immer anhand der Codebeispiele untersuchen.

In diesem Beispiel steht die AWS IoT Konsole für das Gerät. Das AWS CLI steht für die App oder den Dienst, der über den Shadow auf das Gerät zugreift. Die AWS CLI Schnittstelle ist der API sehr ähnlich, mit AWS IoT der eine App möglicherweise kommuniziert. Das Gerät in diesem Beispiel ist eine intelligente Glühlampe, und die App zeigt den Status der Glühlampe an und kann ihren Status ändern.

## Einrichten der Simulation

Diese Verfahren initialisieren die Simulation, indem Sie die AWS IoT -Konsole öffnen, die Ihr Gerät simuliert, und das Befehlszeilenfenster, das Ihre App simuliert.

So richten Sie Ihre Simulationsumgebung ein:

1. Sie benötigen eine AWS-Konto , um die Beispiele aus diesem Thema selbst ausführen zu können. Wenn Sie noch keine haben AWS-Konto, erstellen Sie eine, wie unter beschriebenEinrichten AWS-Konto.
2. Öffnen Sie die AWS IoT -Konsole und wählen Sie im linken Menü Test, um den MQTT-Client zu öffnen.
3. Öffnen Sie in einem anderen Fenster ein Terminalfenster auf einem System, auf dem das AWS CLI installiert ist.

Sie sollten zwei Fenster geöffnet haben: eines mit der AWS IoT Konsole auf der Testseite und eines mit einer Befehlszeilenaufforderung.

## Initialisieren des Geräts

In dieser Simulation arbeiten wir mit einem Dingobjekt mit dem Namen SimShadow1 und seinem Schatten mit dem Namen SimShadow1. mySimulatedThing

Erstellen des Objekts und seiner IoT-Richtlinie

Um ein Objekt zu erstellen, gehen Sie in der AWS IoT Konsole wie folgt vor:

1. Wählen Sie Verwalten und dann Things.
2. Klicken Sie auf die Schaltfläche Erstellen, wenn Dinge aufgelistet sind, andernfalls klicken Sie auf Einzelne Sache registrieren, um eine einzelne Sache zu erstellen. AWS IoT
3. Geben Sie den Namen `mySimulatedThing` ein, behalten Sie die Standardeinstellungen für andere Einstellungen bei und klicken Sie dann auf Weiter.
4. Generieren Sie mithilfe der Zertifikatserstellung mit nur einem Klick die Zertifikate, mit denen die Verbindung des Geräts mit AWS IoT authentifiziert wird. Klicken Sie auf Aktivieren, um das Zertifikat zu aktivieren.
5. Sie können die Richtlinie `My_IoT_Policy` anhängen, die dem Gerät die Erlaubnis erteilt, die reservierten MQTT-Themen zu veröffentlichen und zu abonnieren. Genauere Anweisungen zum

Erstellen AWS IoT eines Dings und zum Erstellen dieser Richtlinie finden Sie unterDies erstellt ein Objekt.

Erstellen Sie einen benannten Schatten für das Objekt.

Sie können einen benannten Schatten für ein Objekt erstellen, indem Sie eine Aktualisierungsanfrage für das Thema `$aws/things/mySimulatedThing/shadow/name/simShadow1/update`, wie unten beschrieben, veröffentlichen.

Oder, um einen benannten Schatten zu erstellen:

1. Wählen Sie in der AWS IoT -Konsole Ihr Objekt in der Liste der angezeigten Objekte aus und wählen Sie dann Schatten.
2. Wählen Sie Schatten hinzufügen, geben Sie den Namen `simShadow1` ein und wählen Sie dann Erstellen, um den benannten Schatten hinzuzufügen.

Abonnieren und veröffentlichen Sie reservierte MQTT-Themen

Abonnieren Sie in der Konsole die reservierten MQTT-Schatten-Themen. Diese Themen sind die Antworten auf die Aktionen `get`, `update` und `delete`, damit Ihr Gerät bereit ist, die Antworten zu empfangen, nachdem es eine Aktion veröffentlicht hat.

So abonnieren Sie ein MQTT-Thema im MQTT-Client:

1. Wählen Sie im MQTT-Client die Option In einem Thema veröffentlichen aus.
2. Geben Sie `get`, `update`, und `delete` Themen ein, die Sie abonnieren möchten. Kopieren Sie jeweils ein Thema aus der folgenden Liste, fügen Sie es in das Feld Themenfilter ein und klicken Sie dann auf Abonnieren. Die Themen müssten dann unter Abonnements aufgeführt werden.

   - `$aws/things/mySimulatedThing/shadow/name/simShadow1/delete/accepted`
   - `$aws/things/mySimulatedThing/shadow/name/simShadow1/delete/rejected`
   - `$aws/things/mySimulatedThing/shadow/name/simShadow1/get/accepted`
   - `$aws/things/mySimulatedThing/shadow/name/simShadow1/get/rejected`
   - `$aws/things/mySimulatedThing/shadow/name/simShadow1/update/accepted`
   - `$aws/things/mySimulatedThing/shadow/name/simShadow1/update/rejected`
   - `$aws/things/mySimulatedThing/shadow/name/simShadow1/update/delta`
   - `$aws/things/mySimulatedThing/shadow/name/simShadow1/update/documents`

An diesem Punkt ist Ihr simuliertes Gerät bereit, die Themen zu erhalten, wie sie von AWS IoT veröffentlicht werden.

So abonnieren Sie ein MQTT-Thema im MQTT-Client:

Nachdem ein Gerät sich selbst initialisiert und die Antwortthemen abonniert hat, sollte Abfragen nach den unterstützten Schatten durchführen. Diese Simulation unterstützt nur einen Schatten, nämlich den Schatten, der ein Dingobjekt namens SimShadow1 unterstützt. mySimulatedThing

So rufen Sie den aktuellen Schattenstatus vom MQTT-Client ab:

1. Wählen Sie im MQTT-Client die Option Publish to a topic (In einem Thema veröffentlichen) aus.
2. Geben Sie unter Veröffentlichen folgendes Thema ein und löschen Sie alle Inhalte aus dem Nachrichtentextfenster, in dem Sie das Thema für GET eingegeben haben. Sie können dann In Thema veröffentlichen auswählen, um die Anfrage zu veröffentlichen. `$aws/things/mySimulatedThing/shadow/name/simShadow1/get`.

   Wenn Sie den benannten Schatten nicht erstellt haben, `simShadow1`, erhalten Sie eine Nachricht im `$aws/things/mySimulatedThing/shadow/name/simShadow1/get/rejected` Thema, und der `code` ist `404`, wie in diesem Beispiel, und da der Schatten nicht erstellt wurde, erstellen wir ihn als Nächstes.

   ```
   {
     "code": 404,
     "message": "No shadow exists with name: 'simShadow1'"
   }
   ```

So erstellen Sie einen Schatten mit dem aktuellen Status des Geräts:

1. Wählen Sie im MQTT-Client die Option In einem Thema veröffentlichen aus.

   ```
   $aws/things/mySimulatedThing/shadow/name/simShadow1/update
   ```

2. Geben Sie im Nachrichtentextfenster, in dem Sie das Thema eingegeben haben, dieses Schattendokument ein, um anzuzeigen, dass das Gerät seine ID und seine aktuelle Farbe in RGB-Werten meldet. Wählen Sie Veröffentlichen, um die Anfrage zu veröffentlichen.

```
{
  "state": {
    "reported": {
      "ID": "SmartLamp21",
      "ColorRGB": [
        128,
        128,
        128
      ]
    }
  },
  "clientToken": "426bfd96-e720-46d3-95cd-014e3ef12bb6"
}
```

Wenn Sie eine Nachricht zum Thema erhalten:

- `$aws/things/mySimulatedThing/shadow/name/simShadow1/update/accepted`: Das bedeutet, dass der Schatten erstellt wurde und der Nachrichtentext das aktuelle Schattendokument enthält.
- `$aws/things/mySimulatedThing/shadow/name/simShadow1/update/rejected`: Überprüfen Sie den Fehler im Nachrichtentext.
- `$aws/things/mySimulatedThing/shadow/name/simShadow1/get/accepted`: Der Schatten ist bereits vorhanden und der Nachrichtentext hat den aktuellen Schattenstatus, wie in diesem Beispiel. Damit können Sie Ihr Gerät einstellen oder bestätigen, dass es mit dem Schattenstatus übereinstimmt.

```
{
  "state": {
    "reported": {
      "ID": "SmartLamp21",
      "ColorRGB": [
        128,
        128,
        128
      ]
    }
  },
  "metadata": {
    "reported": {
```

```
      "ID": {
        "timestamp": 1591140517
      },
      "ColorRGB": [
        {
          "timestamp": 1591140517
        },
        {
          "timestamp": 1591140517
        },
        {
          "timestamp": 1591140517
        }
      ]
    }
  },
  "version": 3,
  "timestamp": 1591140517,
  "clientToken": "426bfd96-e720-46d3-95cd-014e3ef12bb6"
}
```

## Senden einer Aktualisierung von der App

In diesem Abschnitt wird anhand von demonstriert AWS CLI , wie eine App mit einem Schatten interagieren kann.

Um den aktuellen Status des Schattens mit dem zu ermitteln AWS CLI

Geben Sie in der Befehlszeile den folgenden Befehl ein.

```
aws iot-data get-thing-shadow --thing-name mySimulatedThing --shadow-name simShadow1 /
dev/stdout
```

Auf Windows-Plattformen können Sie `con` anstelle von `/dev/stdout` verwenden.

```
aws iot-data get-thing-shadow --thing-name mySimulatedThing --shadow-name simShadow1
 con
```

Da der Schatten vorhanden ist und vom Gerät initialisiert wurde, um seinen aktuellen Zustand wiederzugeben, sollte das folgende Schattendokument zurückgegeben werden.

```
{
  "state": {
    "reported": {
      "ID": "SmartLamp21",
      "ColorRGB": [
        128,
        128,
        128
      ]
    }
  },
  "metadata": {
    "reported": {
      "ID": {
        "timestamp": 1591140517
      },
      "ColorRGB": [
        {
          "timestamp": 1591140517
        },
        {
          "timestamp": 1591140517
        },
        {
          "timestamp": 1591140517
        }
      ]
    }
  },
  "version": 3,
  "timestamp": 1591141111
}
```

Die App kann diese Antwort verwenden, um die Darstellung des Gerätestatus zu initialisieren.

Wenn die App den Status aktualisiert, z. B. wenn ein Endbenutzer die Farbe unserer intelligenten Glühlampe zu Gelb ändert, sendet die App einen update-thing-shadow-Befehl. Dieser Befehl entspricht der `UpdateThingShadow`-REST-API.

So aktualisieren Sie einen Schatten aus einer App:

Geben Sie in der Befehlszeile den folgenden Befehl ein.

AWS CLI v2.x

```
aws iot-data update-thing-shadow --thing-name mySimulatedThing --shadow-name
 simShadow1 \
    --cli-binary-format raw-in-base64-out \
    --payload '{"state":{"desired":{"ColorRGB":
[255,255,0]}},"clientToken":"21b21b21-bfd2-4279-8c65-e2f697ff4fab"}' /dev/stdout
```

AWS CLI v1.x

```
aws iot-data update-thing-shadow --thing-name mySimulatedThing --shadow-name
 simShadow1 \
    --payload '{"state":{"desired":{"ColorRGB":
[255,255,0]}},"clientToken":"21b21b21-bfd2-4279-8c65-e2f697ff4fab"}' /dev/stdout
```

Wenn dieser Befehl erfolgreich ist, sollte das folgende Schattendokument zurückgegeben werden.

```
{
  "state": {
    "desired": {
      "ColorRGB": [
        255,
        255,
        0
      ]
    }
  },
  "metadata": {
    "desired": {
      "ColorRGB": [
        {
          "timestamp": 1591141596
        },
        {
          "timestamp": 1591141596
        },
        {
          "timestamp": 1591141596
        }
      ]
    }
  },
```

```
  "version": 4,
  "timestamp": 1591141596,
  "clientToken": "21b21b21-bfd2-4279-8c65-e2f697ff4fab"
}
```

## Reaktion auf eine Aktualisierung im Gerät

Wenn Sie zum MQTT-Client in der AWS Konsole zurückkehren, sollten Sie die Meldungen sehen, die AWS IoT veröffentlicht wurden, um den im vorherigen Abschnitt ausgegebenen Aktualisierungsbefehl widerzuspiegeln.

So zeigen Sie die Aktualisierungsmeldungen im MQTT-Client an:

Wählen Sie im MQTT-Client aws/things/mySimulatedThing/shadow/name/simShadow1/update/delta in der Spalte Abonnements die Option $ aus. Wenn der Themenname abgeschnitten wird, können Sie ihn anhalten, um das vollständige Thema anzuzeigen. Im Themenprotokoll zu diesem Thema sollten Sie eine `/delta` Meldung sehen, die dieser ähnelt.

```
{
  "version": 4,
  "timestamp": 1591141596,
  "state": {
    "ColorRGB": [
      255,
      255,
      0
    ]
  },
  "metadata": {
    "ColorRGB": [
      {
        "timestamp": 1591141596
      },
      {
        "timestamp": 1591141596
      },
      {
        "timestamp": 1591141596
      }
    ]
  },
  "clientToken": "21b21b21-bfd2-4279-8c65-e2f697ff4fab"
```

```
}
```

Ihr Gerät verarbeitet den Inhalt dieser Nachricht, um den Gerätestatus so festzulegen, dass er mit dem `desired`-Status in der Nachricht übereinstimmt.

Nachdem das Gerät den Status aktualisiert hat, sodass er dem `desired` Status in der Nachricht entspricht, muss es den neuen gemeldeten Status AWS IoT durch Veröffentlichung einer Aktualisierungsnachricht an den neuen Status zurücksenden. Dieses Verfahren simuliert dies im MQTT-Client.

So aktualisieren Sie den Schatten vom Gerät aus:

1. Wählen Sie im MQTT-Client die Option Publish to a topic (In einem Thema veröffentlichen) aus.
2. Geben Sie im Nachrichtentextfenster im Themenfeld über dem Nachrichtentext das Schattenthema ein, gefolgt von der `/update`-Aktion: `$aws/things/mySimulatedThing/shadow/name/simShadow1/update` und geben Sie im Nachrichtentext dieses aktualisierte Shadow-Dokument ein, das den aktuellen Status des Geräts beschreibt. Wählen Sie Veröffentlichen, um den aktualisierten Gerätestatus zu veröffentlichen.

   ```
   {
     "state": {
       "reported": {
         "ColorRGB": [255,255,0]
         }
     },
     "clientToken": "a4dc2227-9213-4c6a-a6a5-053304f60258"
   }
   ```

   Wenn die Nachricht erfolgreich von empfangen wurde AWS IoT, sollten Sie im $ aws/things/mySimulatedThing/shadow/name/simShadow1/update/accepted message log des MQTT-Clients eine neue Antwort mit dem aktuellen Status des Shadows sehen, wie in diesem Beispiel.

   ```
   {
     "state": {
       "reported": {
         "ColorRGB": [
           255,
           255,
           0
         ]
   ```

```
    }
  },
  "metadata": {
    "reported": {
      "ColorRGB": [
        {
          "timestamp": 1591142747
        },
        {
          "timestamp": 1591142747
        },
        {
          "timestamp": 1591142747
        }
      ]
    }
  },
  "version": 5,
  "timestamp": 1591142747,
  "clientToken": "a4dc2227-9213-4c6a-a6a5-053304f60258"
}
```

Eine erfolgreiche Aktualisierung des gemeldeten Status des Geräts führt auch AWS IoT dazu, dass eine umfassende Beschreibung des Shadow-Status in einer Nachricht an das `update/documents` Thema gesendet wird, z. B. dieser Nachrichtentext, der auf das Shadow-Update zurückzuführen ist, das das Gerät im vorherigen Verfahren durchgeführt hat.

```
{
  "previous": {
    "state": {
      "desired": {
        "ColorRGB": [
          255,
          255,
          0
        ]
      },
      "reported": {
        "ID": "SmartLamp21",
        "ColorRGB": [
          128,
          128,
```

```
          128
        ]
      }
    },
    "metadata": {
      "desired": {
        "ColorRGB": [
          {
            "timestamp": 1591141596
          },
          {
            "timestamp": 1591141596
          },
          {
            "timestamp": 1591141596
          }
        ]
      },
      "reported": {
        "ID": {
          "timestamp": 1591140517
        },
        "ColorRGB": [
          {
            "timestamp": 1591140517
          },
          {
            "timestamp": 1591140517
          },
          {
            "timestamp": 1591140517
          }
        ]
      }
    },
    "version": 4
  },
  "current": {
    "state": {
      "desired": {
        "ColorRGB": [
          255,
          255,
          0
```

```
        ]
      },
      "reported": {
        "ID": "SmartLamp21",
        "ColorRGB": [
          255,
          255,
          0
        ]
      }
    },
    "metadata": {
      "desired": {
        "ColorRGB": [
          {
            "timestamp": 1591141596
          },
          {
            "timestamp": 1591141596
          },
          {
            "timestamp": 1591141596
          }
        ]
      },
      "reported": {
        "ID": {
          "timestamp": 1591140517
        },
        "ColorRGB": [
          {
            "timestamp": 1591142747
          },
          {
            "timestamp": 1591142747
          },
          {
            "timestamp": 1591142747
          }
        ]
      }
    },
    "version": 5
  },
```

```
  "timestamp": 1591142747,
  "clientToken": "a4dc2227-9213-4c6a-a6a5-053304f60258"
}
```

## Beobachten Sie das Update in der App

Die App kann jetzt den Schatten nach dem aktuellen Status abfragen, wie vom Gerät gemeldet.

Um den aktuellen Status des Schattens abzurufen, verwenden Sie den AWS CLI

1. Geben Sie in der Befehlszeile den folgenden Befehl ein.

   ```
   aws iot-data get-thing-shadow --thing-name mySimulatedThing --shadow-name
    simShadow1 /dev/stdout
   ```

   Auf Windows-Plattformen können Sie `con` anstelle von `/dev/stdout` verwenden.

   ```
   aws iot-data get-thing-shadow --thing-name mySimulatedThing --shadow-name
    simShadow1 con
   ```

2. Da der Schatten gerade vom Gerät aktualisiert wurde, um seinen aktuellen Zustand wiederzugeben, sollte er das folgende Schattendokument zurückgeben.

   ```
   {
     "state": {
       "desired": {
         "ColorRGB": [
           255,
           255,
           0
         ]
       },
       "reported": {
         "ID": "SmartLamp21",
         "ColorRGB": [
           255,
           255,
           0
         ]
       }
     },
     "metadata": {
   ```

```
    "desired": {
      "ColorRGB": [
        {
          "timestamp": 1591141596
        },
        {
          "timestamp": 1591141596
        },
        {
          "timestamp": 1591141596
        }
      ]
    },
    "reported": {
      "ID": {
        "timestamp": 1591140517
      },
      "ColorRGB": [
        {
          "timestamp": 1591142747
        },
        {
          "timestamp": 1591142747
        },
        {
          "timestamp": 1591142747
        }
      ]
    }
  },
  "version": 5,
  "timestamp": 1591143269
}
```

## Über die Simulation hinaus

Experimentieren Sie mit der Interaktion zwischen der AWS CLI (für die App) und der Konsole (für das Gerät), um Ihre IoT-Lösung zu modellieren.

# Interaktion mit Schatten

In diesem Thema werden die Nachrichten beschrieben, die jeder der drei Methoden zugeordnet sind, die AWS IoT für das Arbeiten mit Schatten bereitstellt. Zu diesen Methoden gehören die folgenden:

`UPDATE`

Erstellt einen Schatten, wenn er nicht vorhanden ist, oder aktualisiert den Inhalt eines vorhandenen Schattens mit den Statusinformationen, die im Nachrichtentext bereitgestellt werden. AWS IoT zeichnet mit jeder Aktualisierung einen Zeitstempel auf, um anzugeben, wann der Status zuletzt aktualisiert wurde. Wenn sich der Status des Shadows ändert, werden `/delta` Nachrichten AWS IoT an alle MQTT-Abonnenten gesendet, wobei der Unterschied zwischen den `desired` und den `reported` Zuständen angegeben wird. Geräte oder Apps, die eine `/delta`-Nachricht empfangen, können basierend auf dem Unterschied Aktionen durchführen. Bei einem Gerät kann z. B. der Status auf den Sollstatus oder bei einer Anwendung die Benutzeroberfläche aktualisiert werden, um die Änderung des Gerätestatus zu reflektieren.

`GET`

Ruft ein aktuelles Schattendokument ab, das den vollständigen Status des Schattens einschließlich Metadaten enthält.

`DELETE`

Löscht den Geräteschatten und seinen gesamten Inhalt.

Sie können ein gelöschtes Geräteschatten-Dokument nicht wiederherstellen, aber Sie können ein neues Geräteschatten-Dokument mit dem Namen eines gelöschten Geräteschatten-Dokuments erstellen. Wenn Sie ein Geräteschatten-Dokument erstellen, das denselben Namen hat wie eines, das innerhalb der letzten 48 Stunden gelöscht wurde, folgt die Versionsnummer des neuen Geräteschatten-Dokuments der Versionsnummer des gelöschten. Wenn ein Geräteschatten-Dokument länger als 48 Stunden gelöscht wurde, lautet die Versionsnummer eines neuen Geräteschatten-Dokuments mit demselben Namen 0.

## Protokollunterstützung

AWS IoT unterstützt MQTT und eine REST-API über HTTPS-Protokolle, um mit Schatten zu interagieren. AWS IoT bietet eine Reihe von reservierten Anfrage- und Antwortthemen für MQTT-Aktionen zum Veröffentlichen und Abonnieren. Geräte und Apps sollten die Antwortthemen

abonnieren, bevor sie in einem Anfragethema veröffentlichen, um Informationen darüber zu erhalten, wie AWS IoT mit der Anfrage umgegangen wurde. Weitere Informationen erhalten Sie unter MQTT-Themen für Geräteschatten und Geräteschatten-REST-API.

## Anforderungs- und Meldestatus

Wenn Sie Ihre IoT-Lösung mithilfe von AWS IoT Schatten entwerfen, sollten Sie festlegen, welche Apps oder Geräte Änderungen anfordern und welche diese implementieren. In der Regel implementiert und meldet ein Gerät Änderungen an den Schatten zurück, und Apps und Services reagieren auf Änderungen im Schatten und fordern Änderungen an. Ihre Lösung könnte davon abweichen, aber die Beispiele in diesem Thema gehen jedoch davon aus, dass die Client-App oder der Service Änderungen im Schatten anfordert und das Gerät die Änderungen durchführt und sie an den Schatten zurückmeldet.

## Aktualisieren eines Shadows

Ihre App oder Ihr Service kann den Status eines Schattens mithilfe der UpdateThingShadow-API oder durch Veröffentlichung im /update-Thema aktualisieren. Aktualisierungen betreffen lediglich die in der Anfrage angegebenen Felder.

### Aktualisieren eines Schattens, wenn ein Client eine Statusänderung anfordert

Wenn ein Client eine Statusänderung in einem Schatten mithilfe des MQTT-Protokolls anfordert

1. Der Client sollte über ein aktuelles Schattendokument verfügen, damit er die zu ändernden Eigenschaften identifizieren kann. Weitere Informationen zum Abrufen des aktuellen Schattendokuments finden Sie unter der Aktion /get.
2. Der Client abonniert diese MQTT-Themen:
   - `$aws/things/thingName/shadow/name/shadowName/update/accepted`
   - `$aws/things/thingName/shadow/name/shadowName/update/rejected`
   - `$aws/things/thingName/shadow/name/shadowName/update/delta`
   - `$aws/things/thingName/shadow/name/shadowName/update/documents`
3. Der Client veröffentlicht ein `$aws/things/thingName/shadow/name/shadowName/update`-Anforderungsthema mit einem Statusdokument, das den gewünschten Status des Schattens enthält. Nur die zu ändernden Eigenschaften müssen in das Dokument aufgenommen werden. Dies ist ein Beispiel für ein Dokument mit dem gewünschten Status.

```
{
  "state": {
    "desired": {
      "color": {
        "r": 10
      },
      "engine": "ON"
    }
  }
}
```

4. Wenn die Aktualisierungsanfrage gültig ist, AWS IoT aktualisiert sie den gewünschten Status im Shadow und veröffentlicht Meldungen zu den folgenden Themen:

   - `$aws/things/thingName/shadow/name/shadowName/update/accepted`
   - `$aws/things/thingName/shadow/name/shadowName/update/delta`

   Die `/update/accepted`-Nachricht enthält ein Antwortstatusdokument „/accepted“-Schattendokument, und die `/update/delta`-Nachricht enthält ein Antwortstatusdokument „/delta“-Schattendokument.

5. Wenn die Aktualisierungsanforderung nicht gültig ist, wird eine Nachricht mit dem `$aws/things/thingName/shadow/name/shadowName/update/rejected` Thema zusammen mit einem Fehlerantwortdokument Schattendokument AWS IoT veröffentlicht, das den Fehler beschreibt.

Wenn ein Client eine Statusänderung in einem Schatten mithilfe der API anfordert

1. Der Client ruft die `UpdateThingShadow`-API mit einem Anfragestatusdokument-Statusdokument als Nachrichtentext auf.
2. Wenn die Anfrage gültig war, wird ein HTTP-Erfolgsantwortcode und ein Antwortstatusdokument „/accepted“ Shadow-Dokument als Hauptteil der Antwortnachricht AWS IoT zurückgegeben.

   AWS IoT veröffentlicht außerdem eine MQTT-Nachricht zu dem `$aws/things/thingName/shadow/name/shadowName/update/delta` Thema mit einem Antwortstatusdokument „/delta“ Shadow-Dokument für alle Geräte oder Clients, die es abonnieren.
3. Wenn die Anfrage nicht gültig war, wird ein HTTP-Fehlerantwortcode an Fehlerantwortdokument als Hauptteil der Antwortnachricht AWS IoT zurückgegeben.

Wenn das Gerät den `/desired`-Status zum `/update/delta`-Thema erhält, nimmt es die gewünschten Änderungen im Gerät vor. Anschließend wird eine Nachricht an das `/update`-Thema gesendet, um den aktuellen Status an den Schatten zu melden.

## Aktualisieren eines Schattens, wenn ein Gerät seinen aktuellen Status meldet

Wenn ein Gerät seinen aktuellen Status an den Schatten mithilfe des MQTT-Protokolls meldet

1. Das Gerät sollte diese MQTT-Themen abonnieren, bevor Sie den Schatten aktualisieren:

   - `$aws/things/thingName/shadow/name/shadowName/update/accepted`
   - `$aws/things/thingName/shadow/name/shadowName/update/rejected`
   - `$aws/things/thingName/shadow/name/shadowName/update/delta`
   - `$aws/things/thingName/shadow/name/shadowName/update/documents`

2. Das Gerät meldet seinen aktuellen Status, indem es eine Nachricht zum `$aws/things/thingName/shadow/name/shadowName/update`-Thema veröffentlicht, das den aktuellen Status meldet, wie etwa in diesem Beispiel.

   ```
   {
       "state": {
           "reported" : {
               "color" : { "r" : 10 },
               "engine" : "ON"
           }
       }
   }
   ```

3. Wenn das Update AWS IoT akzeptiert wird, veröffentlicht es eine Nachricht zu den `$aws/things/thingName/shadow/name/shadowName/update/accepted` Themen zusammen mit einem Antwortstatusdokument „/accepted“ Schattendokument.

4. Wenn die Aktualisierungsanforderung nicht gültig ist, wird eine Nachricht mit dem `$aws/things/thingName/shadow/name/shadowName/update/rejected` Thema zusammen mit einem Fehlerantwortdokument Schattendokument AWS IoT veröffentlicht, das den Fehler beschreibt.

Wenn ein Gerät den aktuellen Status mithilfe der API an den Schatten meldet

1. Das Gerät ruft die UpdateThingShadow-API mit einem Anfragestatusdokument-Statusdokument als Nachrichtentext auf.
2. Wenn die Anfrage gültig war, wird der Shadow AWS IoT aktualisiert und ein HTTP-Erfolgsantwortcode mit einem Antwortstatusdokument „/accepted“ Shadow-Dokument als Hauptteil der Antwortnachricht zurückgegeben.

   AWS IoT veröffentlicht außerdem eine MQTT-Nachricht zum `$aws/things/thingName/shadow/name/shadowName/update/delta` Thema mit einem Antwortstatusdokument „/delta“ Shadow-Dokument für alle Geräte oder Clients, die es abonnieren.
3. Wenn die Anfrage nicht gültig war, wird ein HTTP-Fehlerantwortcode an Fehlerantwortdokument als Hauptteil der Antwortnachricht AWS IoT zurückgegeben.

## Optimistische Sperre

Sie können die Version des Statusdokuments verwenden, um sicherzustellen, dass Sie die neueste Version eines Geräteschattendokuments aktualisieren. Geben Sie bei einer Aktualisierungsanfrage eine Version an, lehnt der Service die Anfrage mit einem Konflikt-Antwortcode HTTP 409 ab, wenn die aktuelle Version des Statusdokuments nicht der angegebenen Version entspricht. Der Konfliktreaktionscode kann auch in jeder API vorkommen, die Änderungen am `ThingShadow` vornimmt, darunter `DeleteThingShadow`:

Zum Beispiel:

Ausgangsdokument:

```
{
  "state": {
    "desired": {
      "colors": [
        "RED",
        "GREEN",
        "BLUE"
      ]
    }
  },
  "version": 10
}
```

Aktualisierung: (die Versionen stimmen nicht überein; die Anfrage wird abgelehnt)

```
{
  "state": {
    "desired": {
      "colors": [
        "BLUE"
      ]
    }
  },
  "version": 9
}
```

Ergebnis:

```
{
  "code": 409,
  "message": "Version conflict",
  "clientToken": "426bfd96-e720-46d3-95cd-014e3ef12bb6"
}
```

Aktualisierung: (die Versionen stimmen überein; die Anfrage wird angenommen)

```
{
  "state": {
    "desired": {
      "colors": [
        "BLUE"
      ]
    }
  },
  "version": 10
}
```

Endzustand:

```
{
  "state": {
    "desired": {
      "colors": [
        "BLUE"
      ]
```

```
    }
  },
  "version": 11
}
```

## Abrufen eines Shadow-Dokuments

Sie können ein Schattendokument abrufen, indem Sie die GetThingShadow-API verwenden oder indem Sie das /get-Thema abonnieren und dazu veröffentlichen. Hierdurch wird ein vollständiges Schattendokument einschließlich aller Unterschiede zwischen den Statusarten `desired` und `reported` abgerufen. Die Vorgehensweise für diese Aufgabe ist unabhängig davon, ob das Gerät oder ein Client die Anforderung durchführt.

So rufen Sie ein Schattendokument mithilfe des MQTT-Protokolls ab:

1. Das Gerät oder der Client sollte diese MQTT-Themen abonnieren, bevor der Schatten aktualisiert wird:
   - `$aws/things/thingName/shadow/name/shadowName/get/accepted`
   - `$aws/things/thingName/shadow/name/shadowName/get/rejected`
2. Das Gerät oder der Client veröffentlicht eine Nachricht mit einem leeren Nachrichtentext zum `$aws/things/thingName/shadow/name/shadowName/get`-Thema.
3. Wenn die Anfrage erfolgreich ist, wird eine Nachricht zum `$aws/things/thingName/shadow/name/shadowName/get/accepted` Thema mit einem Antwortstatusdokument „/accepted“ im Nachrichtentext AWS IoT veröffentlicht.
4. Wenn die Anfrage nicht gültig war, AWS IoT veröffentlicht eine Nachricht zum `$aws/things/thingName/shadow/name/shadowName/get/rejected` Thema mit einem Fehlerantwortdokument im Nachrichtentext.

So rufen Sie ein Schattendokument mithilfe einer REST-API ab:

1. Das Gerät oder Client ruft die `GetThingShadow`-API mit einem leeren Nachrichtentext auf.
2. Wenn die Anfrage gültig ist, wird ein HTTP-Erfolgsantwortcode mit einem Antwortstatusdokument „/accepted“ Schattendokument als Hauptteil der Antwortnachricht AWS IoT zurückgegeben.
3. Wenn die Anfrage nicht gültig ist, wird ein HTTP-Fehlerantwortcode an Fehlerantwortdokument als Hauptteil der Antwortnachricht AWS IoT zurückgegeben.

# Löschen von Schattendaten

Es gibt zwei Möglichkeiten, Schattendaten zu löschen: Sie können bestimmte Eigenschaften im Schattendokument löschen oder den Schatten vollständig löschen.

- Um bestimmte Eigenschaften aus einem Schatten zu löschen, aktualisieren Sie den Schatten. Legen Sie jedoch den Wert der Eigenschaften, die Sie löschen möchten, auf `null` fest. Felder mit dem Wert `null` werden aus dem Schattendokument entfernt.
- Um den gesamten Schatten zu löschen, verwenden Sie die DeleteThingShadow-API oder veröffentlichen Sie zum /delete-Thema.

> **Note**
>
> Durch das Löschen eines Shadows wird seine Versionsnummer nicht sofort auf Null zurückgesetzt. Er wird nach 48 Stunden auf null zurückgesetzt.

## Löschen einer Eigenschaft aus einem Schattendokument

So löschen Sie eine Eigenschaft aus einem Schatten mithilfe des MQTT-Protokolls:

1. Das Gerät oder der Client sollte über ein aktuelles Schattendokument verfügen, damit es/er die zu ändernden Eigenschaften identifizieren kann. Weitere Informationen zum Abrufen des aktuellen Schattendokuments finden Sie unter Abrufen eines Shadow-Dokuments.
2. Das Gerät oder der Client abonniert diese MQTT-Themen:
   - `$aws/things/thingName/shadow/name/shadowName/update/accepted`
   - `$aws/things/thingName/shadow/name/shadowName/update/rejected`
3. Das Gerät oder der Client veröffentlicht ein `$aws/things/thingName/shadow/name/shadowName/update`-Anforderungsthema mit einem Statusdokument, das den Eigenschaften des zu löschenden Schattens `null`-Werte zuweist. Nur die zu ändernden Eigenschaften müssen in das Dokument aufgenommen werden. Dies ist ein Beispiel für ein Dokument, das die `engine`-Eigenschaft löscht.

```
{
  "state": {
    "desired": {
```

```
      "engine": null
    }
  }
}
```

4. Wenn die Aktualisierungsanforderung gültig ist, AWS IoT werden die angegebenen Eigenschaften im Shadow gelöscht und eine Nachricht mit dem `$aws/things/thingName/shadow/name/shadowName/update/accepted` Thema mit einem Antwortstatusdokument „/accepted“ Shadow-Dokument im Nachrichtentext veröffentlicht.
5. Wenn die Aktualisierungsanforderung nicht gültig ist, wird eine Nachricht mit dem `$aws/things/thingName/shadow/name/shadowName/update/rejected` Thema zusammen mit einem Fehlerantwortdokument Schattendokument AWS IoT veröffentlicht, das den Fehler beschreibt.

So löschen Sie eine Eigenschaft aus einem Schatten mithilfe der REST-API:

1. Das Gerät oder der Client ruft die `UpdateThingShadow`-API mit einer Anfragestatusdokument auf die den Eigenschaften des zu löschenden Schattens `null`-Werte zuweist. Fügen Sie nur die Eigenschaften, die Sie löschen möchten, in das Dokument ein. Dies ist ein Beispiel für ein Dokument, das die `engine`-Eigenschaft löscht.

```
{
  "state": {
    "desired": {
      "engine": null
    }
  }
}
```

2. Wenn die Anfrage gültig war, wird ein HTTP-Erfolgsantwortcode und ein Antwortstatusdokument „/accepted“ Shadow-Dokument als Hauptteil der Antwortnachricht AWS IoT zurückgegeben.
3. Wenn die Anfrage nicht gültig war, wird ein HTTP-Fehlerantwortcode an Fehlerantwortdokument als Hauptteil der Antwortnachricht AWS IoT zurückgegeben.

## Löschen eines Shadows

Im Folgenden werden einige Aspekte beschrieben, die beim Löschen des Schattens eines Geräts berücksichtigt werden sollten.

- Wenn Sie den Schattenstatus des Geräts auf `null` festlegen, wird der Schatten nicht gelöscht. Die Schattenversion wird beim nächsten Update erhöht.
- Das Löschen eines Geräteschattens löscht das Objekt nicht. Das Löschen eines Objekts löscht den entsprechenden Geräteschatten nicht.
- Durch das Löschen eines Shadows wird seine Versionsnummer nicht sofort auf Null zurückgesetzt. Er wird nach 48 Stunden auf null zurückgesetzt.

So löschen Sie einen Schatten mithilfe des MQTT-Protokolls:

1. Das Gerät oder der Client abonniert diese MQTT-Themen:
   - `$aws/things/thingName/shadow/name/shadowName/delete/accepted`
   - `$aws/things/thingName/shadow/name/shadowName/delete/rejected`
2. Das Gerät oder der Client veröffentlicht eine `$aws/things/thingName/shadow/name/shadowName/delete`-mit einem leeren Nachrichtenpuffer.
3. Wenn die Löschanforderung gültig ist, wird der Shadow AWS IoT gelöscht und eine Nachricht mit dem `$aws/things/thingName/shadow/name/shadowName/delete/accepted` Thema und einem abgekürzten Antwortstatusdokument „/accepted“ Shadow-Dokument im Nachrichtentext veröffentlicht. Dies ist ein Beispiel für eine akzeptierte Löschmeldung:

   ```
   {
     "version": 4,
     "timestamp": 1591057529
   }
   ```

4. Wenn die Aktualisierungsanforderung nicht gültig ist, wird eine Nachricht mit dem `$aws/things/thingName/shadow/name/shadowName/delete/rejected` Thema zusammen mit einem Fehlerantwortdokument Shadow-Dokument AWS IoT veröffentlicht, das den Fehler beschreibt.

So löschen Sie einen Schatten mithilfe der REST-API:

1. Das Gerät oder der Client ruft die `DeleteThingShadow`-API mit einem leeren Nachrichtenpuffer auf.
2. Wenn die Anfrage gültig war, werden ein HTTP-Erfolgsantwortcode Antwortstatusdokument „/accepted“ und ein abgekürztes Antwortstatusdokument „/accepted“ Schattendokument

im Nachrichtentext AWS IoT zurückgegeben. Dies ist ein Beispiel für eine akzeptierte Löschmeldung:

```
{
  "version": 4,
  "timestamp": 1591057529
}
```

3. Wenn die Anfrage nicht gültig war, wird ein HTTP-Fehlerantwortcode an Fehlerantwortdokument als Hauptteil der Antwortnachricht AWS IoT zurückgegeben.

## Geräteschatten-REST-API

Ein Schatten stellt den folgenden URI für die Aktualisierung der Statusinformationen bereit:

```
https://account-specific-prefix-ats.iot.region.amazonaws.com/things/thingName/shadow
```

Der Endpunkt ist spezifisch für Ihren AWS-Konto. Um Ihren Endpunkt zu finden, können Sie:

- den Befehl describe-endpoint aus dem AWS CLI verwenden.
- Verwenden Sie die AWS IoT Konsoleneinstellungen. In den Einstellungen ist der Endpunkt unter Benutzerdefinierter Endpunkt aufgeführt
- Verwenden Sie die Seite mit den Details der AWS IoT Konsolenelemente. In der Konsole:
  1. Öffnen Sie Verwalten und wählen Sie unter Verwalten die Option Objekte aus.
  2. Wählen Sie in der Liste der Objekte das Objekt aus, für das Sie den Endpunkt-URI abrufen möchten.
  3. Wählen Sie die Registerkarte Geräteschatten und wählen Sie Ihren Schatten aus. Sie können den Endpunkt-URI im Abschnitt Geräteschatten-URL der Geräteschatten-Detailseite einsehen.

Der Endpunkt hat folgendes Format:

```
identifier.iot.region.amazonaws.com
```

Die Shadow-REST-API verwendet die unter Gerätekommunikationsprotokolle beschriebenen HTTPS-Protokolle/Portzuweisungen.

> **Note**
>
> Um den zu verwenden APIs, müssen Sie ihn `iotdevicegateway` als Dienstnamen für die Authentifizierung verwenden. Weitere Informationen finden Sie unter Io TData Plane.

API-Aktionen

- GetThingShadow
- UpdateThingShadow
- DeleteThingShadow
- ListNamedShadowsForThing

Sie können die API auch verwenden, um einen benannten Schatten zu erstellen, indem Sie `name=`*`shadowName`* als Teil des Abfrageparameters der API angeben.

## GetThingShadow

Ruft das Schattengerät für das angegebene Objekt ab.

Das Antwort-Statusdokument enthält das Delta zwischen dem Status `desired` (Soll) und dem Status `reported` (gemeldet).

Anforderung

Die Anfrage enthält die Standard-HTTP-Kopfzeilen sowie das folgende URI:

```
HTTP GET https://endpoint/things/thingName/shadow?name=shadowName
Request body: (none)
```

Der `name`-Abfrageparameter ist für unbenannte (klassische) Schatten nicht erforderlich.

Antwort

Bei erfolgreicher Anfrage enthält die Antwort die Standard-HTTP-Kopfzeilen sowie den folgenden Code und Text:

```
HTTP 200
```

```
Response Body: response state document
```

Weitere Informationen finden Sie im Antwort-Statusdokumentenbeispiel.

Autorisierung

Für das Abrufen eine Schattens ist eine Richtlinie erforderlich, die es dem Aufrufer erlaubt, die Aktion `iot:GetThingShadow` durchzuführen. Der Geräteschatten-Service akzeptiert zwei Arten der Authentifizierung: die Signatur-Version 4 mit IAM-Anmeldeinformationen oder die gegenseitige TLS-Authentifizierung mit einem Client-Zertifikat.

Es folgt ein Beispiel für eine Richtlinie, die es dem Aufrufer erlaubt, einen Geräteschatten abzurufen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:GetThingShadow",
      "Resource": [
        "arn:aws:iot:region:account:thing/thing"
      ]
    }
  ]
}
```

## UpdateThingShadow

Aktualisiert das Schattengerät für das angegebene Objekt.

Aktualisierungen betreffen lediglich die im Anfragestatusdokument angegebenen Felder. Ein Feld mit dem Wert `null` (Null) wird aus dem Geräteschatten entfernt.

Anforderung

Die Anfrage enthält die Standard-HTTP-Kopfzeilen sowie das/den folgende(n) URI und Text:

```
HTTP POST https://endpoint/things/thingName/shadow?name=shadowName
Request body: request state document
```

Der `name`-Abfrageparameter ist für unbenannte (klassische) Schatten nicht erforderlich.

Weitere Informationen finden Sie im Anfragestatusdokumentenbeispiel.

Antwort

Bei erfolgreicher Anfrage enthält die Antwort die Standard-HTTP-Kopfzeilen sowie den folgenden Code und Text:

```
HTTP 200
Response body: response state document
```

Weitere Informationen finden Sie im Antwort-Statusdokumentenbeispiel.

Autorisierung

Für das Aktualisieren eines Schattens ist eine Richtlinie erforderlich, die es dem Aufrufer erlaubt, die Aktion `iot:UpdateThingShadow` durchzuführen. Der Geräteschatten-Service akzeptiert zwei Arten der Authentifizierung: die Signatur-Version 4 mit IAM-Anmeldeinformationen oder die gegenseitige TLS-Authentifizierung mit einem Client-Zertifikat.

Es folgt ein Beispiel für eine Richtlinie, die es dem Aufrufer erlaubt, einen Geräteschatten zu aktualisieren:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:UpdateThingShadow",
      "Resource": [
        "arn:aws:iot:region:account:thing/thing"
      ]
    }
  ]
}
```

## DeleteThingShadow

Löscht das Schattengerät für das angegebene Objekt.

Anforderung

Die Anfrage enthält die Standard-HTTP-Kopfzeilen sowie das folgende URI:

```
HTTP DELETE https://endpoint/things/thingName/shadow?name=shadowName
Request body: (none)
```

Der name-Abfrageparameter ist für unbenannte (klassische) Schatten nicht erforderlich.

Antwort

Bei erfolgreicher Anfrage enthält die Antwort die Standard-HTTP-Kopfzeilen sowie den folgenden Code und Text:

```
HTTP 200
Response body: Empty response state document
```

Beachten Sie, dass durch das Löschen eines Shadows seine Versionsnummer nicht auf 0 zurückgesetzt wird.

Autorisierung

Für das Löschen eine Geräteschattens ist eine Richtlinie erforderlich, die es dem Aufrufer erlaubt, die Aktion `iot:DeleteThingShadow` durchzuführen. Der Geräteschatten-Service akzeptiert zwei Arten der Authentifizierung: die Signatur-Version 4 mit IAM-Anmeldeinformationen oder die gegenseitige TLS-Authentifizierung mit einem Client-Zertifikat.

Es folgt ein Beispiel für eine Richtlinie, die es dem Aufrufer erlaubt, einen Geräteschatten zu löschen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:DeleteThingShadow",
      "Resource": [
        "arn:aws:iot:region:account:thing/thing"
      ]
    }
  ]
}
```

## ListNamedShadowsForThing

Listet die Schatten für das angegebene Objekt auf.

### Anforderung

Die Anfrage enthält die Standard-HTTP-Kopfzeilen sowie das folgende URI:

```
HTTP GET /api/things/shadow/ListNamedShadowsForThing/thingName?
nextToken=nextToken&pageSize=pageSize
Request body: (none)
```

nextToken

Das Token zum Abruf des nächsten Ergebnissatzes.

Dieser Wert wird für nach Seiten organisierte Ergebnisse zurückgegeben und in dem Aufruf verwendet, der die nächste Seite zurückgibt.

pageSize

Die Anzahl der Schattennamen, die bei jedem Aufruf zurückgegeben werden sollen. Siehe auch `nextToken`.

thingName

Der Name des Objekts, für das die benannten Schatten aufgelistet werden sollen.

### Antwort

Falls erfolgreich, enthält die Antwort die Standard-HTTP-Kopfzeilen sowie den folgenden Antwortcode und eine Antwortdokument für die Schattennamenliste.

> **Note**
>
> Der unbenannte (klassische) Schatten wird in dieser Liste nicht angezeigt. Die Antwort ist eine leere Liste, wenn Sie nur einen klassischen Schatten haben oder wenn der von `thingName` Ihnen angegebene Schatten nicht existiert.

```
HTTP 200
Response body: Shadow name list document
```

### Autorisierung

Für das Löschen eines Geräteschattens ist eine Richtlinie erforderlich, die es dem Aufrufer erlaubt, die Aktion `iot:ListNamedShadowsForThing` durchzuführen. Der Geräteschatten-Service akzeptiert zwei Arten der Authentifizierung: die Signatur-Version 4 mit IAM-Anmeldeinformationen oder die gegenseitige TLS-Authentifizierung mit einem Client-Zertifikat.

Es folgt ein Beispiel für eine Richtlinie, die es dem Aufrufer erlaubt, die benannten Schatten eines Objekts zu aktualisieren:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:ListNamedShadowsForThing",
      "Resource": [
        "arn:aws:iot:region:account:thing/thing"
      ]
    }
  ]
}
```

# MQTT-Themen für Geräteschatten

Der Device Shadow-Service verwendet reservierte MQTT-Themen, um es Anwendungen und Geräten zu ermöglichen, die Statusinformationen für ein Gerät (Schatten) abzurufen, zu aktualisieren oder zu löschen.

Das Veröffentlichen in und Abonnieren von Schattengerätethemen erfordert eine themenbasierte Autorisierung. AWS IoT behält sich das Recht vor, der vorhandenen Themenstruktur neue Themen hinzuzufügen. Aus diesem Grund empfehlen wir, Abonnements mit Platzhaltern von Schattengeräte-Topics zu vermeiden. Vermeiden Sie es beispielsweise, Themenfilter zu abonnieren, `$aws/things/thingName/shadow/#` weil die Anzahl der Themen, die diesem Themenfilter entsprechen, zunehmen könnte, wenn neue Schattenthemen eingeführt werden. AWS IoT Beispiele für Nachrichten, die zu diesen Topics veröffentlichten wurden, finden Sie unter Interaktion mit Schatten.

Schatten können benannt oder unbenannt sein (klassisch). Die jeweils verwendeten Themen unterscheiden sich nur durch das Themenpräfix. In dieser Tabelle wird das Themenpräfix angezeigt, das von jedem Schattentyp verwendet wird.

| *ShadowTopicPrefix* Wert | Schattentyp |
| --- | --- |
| $aws/things/ *thingName* /shadow | Unbenannter (klassischer) Schatten |
| $aws/things/ *thingName* /shadow/name/ *shadowName* | Benannter Schatten |

Um ein vollständiges Thema zu erstellen, wählen Sie die *ShadowTopicPrefix* für den Schattentyp aus, auf den Sie verweisen möchten, ersetzen Sie *thingName* und gegebenenfalls *shadowName* durch die entsprechenden Werte und fügen Sie diese dann an den Themen-Stub an, wie in den folgenden Abschnitten dargestellt.

Nachstehend finden Sie die MQTT-Themen, die für die Interaktion mit Schatten verwendet wurden.

Themen

- /get
- /get/accepted
- /update/rejected
- /update
- /update/delta
- /update/accepted
- /update/documents
- /update/rejected
- /delete
- /delete/accepted
- /delete/rejected

## /get

Veröffentlichen Sie eine leere Nachricht in diesem Thema, um den Geräteschatten abzurufen:

```
ShadowTopicPrefix/get
```

AWS IoT antwortet mit einer Veröffentlichung auf entweder /get/accepted oder/update/rejected.

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/get"
      ]
    }
  ]
}
```

## /get/accepted

AWS IoT veröffentlicht ein Antwort-Shadow-Dokument zu diesem Thema, wenn der Shadow des Geräts zurückgegeben wird:

```
ShadowTopicPrefix/get/accepted
```

Weitere Informationen finden Sie unter Antwortstatusdokumente.

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

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

```
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingName/shadow/get/
accepted"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/get/accepted"
      ]
    }
  ]
}
```

## /update/rejected

AWS IoT veröffentlicht ein Fehlerantwortdokument zu diesem Thema, wenn es den Schatten des Geräts nicht zurückgeben kann:

```
ShadowTopicPrefix/get/rejected
```

Weitere Informationen finden Sie unter Fehlerantwortdokument.

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingName/shadow/get/
rejected"
      ]
    },
```

```
    {
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/get/rejected"
      ]
    }
  ]
}
```

## /update

Veröffentlichen Sie in diesem Thema ein Anfragestatusdokument, um den Geräteschatten zu aktualisieren:

```
ShadowTopicPrefix/update
```

Der Nachrichtentext enthält ein partielles Anfragestatusdokument.

Ein Client, der versucht, den Status eines Geräts zu aktualisieren, sendet ein JSON-Anfragestatusdokument mit einer `desired`-Eigenschaft wie der folgenden:

```
{
  "state": {
    "desired": {
      "color": "red",
      "power": "on"
    }
  }
}
```

Ein Gerät, das seinen Schatten aktualisiert, würde ein JSON-Anfragestatusdokument mit der `reported`-Eigenschaft senden, z. B.:

```
{
  "state": {
    "reported": {
      "color": "red",
      "power": "on"
    }
  }
```

```
}
```

AWS IoT antwortet, indem es entweder /update/accepted oder veröffentlicht/update/rejected.

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/update"
      ]
    }
  ]
}
```

## /update/delta

AWS IoT veröffentlicht ein Antwortstatusdokument zu diesem Thema, wenn es eine Änderung für den Shadow des Geräts akzeptiert, und das Antwortstatusdokument verschiedene Werte für `desired` und gibt `reported` an:

```
ShadowTopicPrefix/update/delta
```

Der Nachrichtenpuffer enthält eine Antwortstatusdokument „/delta“.

### Nachrichtentextdetails

- Eine in `update/delta` veröffentlichte Nachricht umfasst nur die gewünschten Attribute, die sich zwischen dem Abschnitt `desired` (Soll) und dem Abschnitt `reported` (gemeldet) Abschnitt unterscheiden. Sie enthält alle diese Attribute, unabhängig davon, ob diese in der Nachricht zur aktuellen Aktualisierung enthalten waren oder bereits in AWS IoT gespeichert wurden. Attribute, die sich nicht zwischen dem Abschnitt `desired` (Soll) und dem Abschnitt `reported` (gemeldet) Abschnitt unterscheiden, sind nicht enthalten.

- Wenn sich ein Attribut im Abschnitt `reported` (gemeldet) befindet, jedoch kein Pendant im Abschnitt `desired` (Soll), dann ist es nicht enthalten.
- Ist ein Attribut im Abschnitt `desired` (Soll) vorhanden, besitzt jedoch kein Pendant im Abschnitt `reported` (gemeldet), dann ist es enthalten.
- Wenn ein Attribut aus dem Abschnitt `reported` (gemeldet) gelöscht wurde, aber sich nach wie vor im Abschnitt `desired` (Soll) befindet, dann ist es enthalten.

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingName/shadow/update/
delta"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/update/delta"
      ]
    }
  ]
}
```

## /update/accepted

AWS IoT veröffentlicht ein Antwortstatusdokument zu diesem Thema, wenn eine Änderung für den Shadow des Geräts akzeptiert wird:

```
ShadowTopicPrefix/update/accepted
```

Der Nachrichtenpuffer enthält eine Antwortstatusdokument „/accepted“.

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingName/shadow/update/
accepted"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/update/accepted"
      ]
    }
  ]
}
```

## /update/documents

AWS IoT veröffentlicht ein Statusdokument zu diesem Thema, wenn eine Aktualisierung des Shadows erfolgreich durchgeführt wurde:

```
ShadowTopicPrefix/update/documents
```

Der Nachrichtentext enthält eine /Dokumente, Antwortstatusdokument.

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingName/shadow/update/
documents"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/update/
documents"
      ]
    }
  ]
}
```

## /update/rejected

AWS IoT veröffentlicht ein Fehlerantwortdokument zu diesem Thema, wenn eine Änderung für den Shadow des Geräts abgelehnt wird:

```
ShadowTopicPrefix/update/rejected
```

Der Nachrichtentext enthält eine Fehlerantwortdokument.

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingName/shadow/update/
rejected"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/update/rejected"
      ]
    }
  ]
}
```

## /delete

Um einen Geräteschatten zu löschen, veröffentlichen Sie im Löschthema eine leere Nachricht.

```
ShadowTopicPrefix/delete
```

Der Inhalt der Nachricht wird ignoriert.

Beachten Sie, dass durch das Löschen eines Shadows seine Versionsnummer nicht auf 0 zurückgesetzt wird.

AWS IoT antwortet, indem es entweder /delete/accepted oder /delete/rejected veröffentlicht.

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/delete"
      ]
    }
  ]
}
```

## /delete/accepted

AWS IoT veröffentlicht eine Nachricht zu diesem Thema, wenn der Schatten eines Geräts gelöscht wird:

```
ShadowTopicPrefix/delete/accepted
```

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingName/shadow/delete/
accepted"
      ]
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/delete/accepted"
      ]
    }
  ]
}
```

## /delete/rejected

AWS IoT veröffentlicht ein Dokument mit einer Fehlermeldung zu diesem Thema, wenn der Schatten des Geräts nicht gelöscht werden kann:

```
ShadowTopicPrefix/delete/rejected
```

Der Nachrichtentext enthält eine Fehlerantwortdokument.

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topicfilter/$aws/things/thingName/shadow/delete/
rejected"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
```

```
        "arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/delete/rejected"
      ]
    }
  ]
}
```

# Dokumente des Device Shadow-Services

Der Device Shadow-Service befolgt alle Regeln der JSON-Spezifikation. Werte, Objekte und Arrays werden im Geräteschatten-Dokument gespeichert.

Inhalt


- Beispiele für Schatten-Dokumente
- Dokumenteigenschaften
- Delta-Status
- Versioning von Schattendokumenten
- Client-Tokens in Schattendokumenten
- Eigenschaften des leeren Schattendokuments
- Array-Werte in Schattendokumenten


## Beispiele für Schatten-Dokumente

Der Device Shadow-Service verwendet bei den Operationen UPDATE, GET und DELETE mithilfe der REST-API oder MQTT- Pub/Sub-Nachrichten die folgenden Dokumente.

Beispiele


- Anfragestatusdokument
- Antwortstatusdokumente
- Fehlerantwortdokument
- Antwortdokument für die Schattennamenliste


### Anfragestatusdokument

Ein Anfragestatusdokument hat das folgende Format:

```
{
    "state": {
        "desired": {
            "attribute1": integer2,
            "attribute2": "string2",
            ...
            "attributeN": boolean2
        },
        "reported": {
            "attribute1": integer1,
            "attribute2": "string1",
            ...
            "attributeN": boolean1
        }
    },
    "clientToken": "token",
    "version": version
}
```

- `state` – Aktualisierungen betreffen lediglich die angegebenen Felder. In der Regel verwenden Sie entweder die `desired`- oder die `reported`-Eigenschaft, aber nicht beide, in derselben Anforderung.
  - `desired` – Die Statuseigenschaften und Werte, deren Aktualisierung im Gerät angefordert wurde.
  - `reported` – Die vom Gerät gemeldeten Zustandseigenschaften und -werte.
- `clientToken` – Falls verwendet, können Sie die Anfrage und die entsprechende Antwort anhand des Client-Tokens abgleichen.
- `version` — Bei Verwendung verarbeitet der Device Shadow-Service nur dann die Aktualisierung, wenn die angegebene Version mit seiner neuesten Version übereinstimmt.

## Antwortstatusdokumente

Antwortstatusdokumente haben je nach Antworttyp das folgende Format.

Antwortstatusdokument „/accepted“

```
{
    "state": {
        "desired": {
```

```
            "attribute1": integer2,
            "attribute2": "string2",
            ...
            "attributeN": boolean2
        }
    },
    "metadata": {
        "desired": {
            "attribute1": {
                "timestamp": timestamp
            },
            "attribute2": {
                "timestamp": timestamp
            },
            ...
            "attributeN": {
                "timestamp": timestamp
            }
        }
    },
    "timestamp": timestamp,
    "clientToken": "token",
    "version": version
}
```

Antwortstatusdokument „/delta“

```
{
    "state": {
        "attribute1": integer2,
        "attribute2": "string2",
        ...
        "attributeN": boolean2
    },
    "metadata": {
        "attribute1": {
            "timestamp": timestamp
        },
        "attribute2": {
            "timestamp": timestamp
        },
        ...
        "attributeN": {
```

```
            "timestamp": timestamp
        }
    },
    "timestamp": timestamp,
    "clientToken": "token",
    "version": version
}
```

/Dokumente, Antwortstatusdokument

```
{
  "previous" : {
    "state": {
        "desired": {
            "attribute1": integer2,
            "attribute2": "string2",
            ...
            "attributeN": boolean2
        },
        "reported": {
            "attribute1": integer1,
            "attribute2": "string1",
            ...
            "attributeN": boolean1
        }
    },
    "metadata": {
        "desired": {
            "attribute1": {
                "timestamp": timestamp
            },
            "attribute2": {
                "timestamp": timestamp
            },
            ...
            "attributeN": {
                "timestamp": timestamp
            }
        },
        "reported": {
            "attribute1": {
                "timestamp": timestamp
            },
```

```
            "attribute2": {
                "timestamp": timestamp
            },
            ...
            "attributeN": {
                "timestamp": timestamp
            }
        }
    },
    "version": version-1
},
"current": {
    "state": {
        "desired": {
            "attribute1": integer2,
            "attribute2": "string2",
            ...
            "attributeN": boolean2
        },
        "reported": {
            "attribute1": integer2,
            "attribute2": "string2",
            ...
            "attributeN": boolean2
        }
    },
    "metadata": {
        "desired": {
            "attribute1": {
                "timestamp": timestamp
            },
            "attribute2": {
                "timestamp": timestamp
            },
            ...
            "attributeN": {
                "timestamp": timestamp
            }
        },
        "reported": {
            "attribute1": {
                "timestamp": timestamp
            },
            "attribute2": {
```

```
                "timestamp": timestamp
            },
            ...
            "attributeN": {
                "timestamp": timestamp
            }
        }
    },
    "version": version
  },
  "timestamp": timestamp,
  "clientToken": "token"
}
```

Eigenschaften des Antwortstatusdokuments

- `previous` – Enthält nach einer erfolgreichen Aktualisierung den `state` des Objekts vor dem Update.
- `current` – Enthält nach einer erfolgreichen Aktualisierung den `state` des Objekts nach dem Update.
- `state`
  - `reported` – Liegt nur dann vor, wenn ein Objekt Daten im `reported`-Abschnitt gemeldet hat, und enthält nur Felder, die im Anfragestatusdokument enthalten waren.
  - `desired` – Liegt nur dann vor, wenn ein Gerät Daten im `desired`-Abschnitt gemeldet hat, und enthält nur Felder, die im Anfragestatusdokument enthalten waren.
  - `delta` – Liegt nur dann vor, wenn sich die `desired`-Daten von den aktuellen `reported`-Daten des Schattens unterscheiden.
- `metadata` –`desired` Enthält für jedes Attribut in den Abschnitten und `reported` die Zeitstempel, sodass Sie feststellen können, wann der Status aktualisiert wurde.
- `timestamp`— Datum und Uhrzeit der Epoche, zu der die Antwort generiert wurde AWS IoT.
- `clientToken` – Liegt nur dann vor, wenn bei der Veröffentlichung einer gültigen JSON im Thema `/update` ein Client-Token verwendet wurde.
- `version` – Die aktuelle Version des Dokuments für den Geräteschatten, freigegeben in AWS IoT. Sie erhöht sich zur vorherigen Versionsnummer des Dokuments um die Zahl eins.

## Fehlerantwortdokument

Ein Fehlerantwortdokument hat das folgende Format:

```
{
    "code": error-code,
    "message": "error-message",
    "timestamp": timestamp,
    "clientToken": "token"
}
```

- `code` – Einen HTTP-Antwortcode, der auf die Art des Fehlers hinweist.
- `message` – Eine Textnachricht mit zusätzlichen Informationen.
- `timestamp`— Datum und Uhrzeit der Generierung der Antwort. AWS IoT Diese Eigenschaft ist nicht in allen Fehlerantwortdokumenten vorhanden.
- `clientToken` – Liegt nur dann vor, wenn ein Client-Token in der veröffentlichten Nachricht verwendet wurde.

Weitere Informationen finden Sie unter Device Shadow-Fehlermeldungen.

## Antwortdokument für die Schattennamenliste

Ein Antwortdokument für die Schattennamenliste hat das folgende Format:

```
{
    "results": [
        "shadowName-1",
        "shadowName-2",
        "shadowName-3",
        "shadowName-n"
    ],
    "nextToken": "nextToken",
    "timestamp": timestamp
}
```

- `results` – Das Array von Schattennamen.
- `nextToken` – Der Token-Wert, der in nach Seiten organisierten Anforderungen verwendet wird, um die nächste Seite in der Sequenz abzurufen. Diese Eigenschaft ist nicht vorhanden, wenn keine weiteren Schattennamen zurückgegeben werden sollen.

- `timestamp`— Datum und Uhrzeit der Generierung der Antwort AWS IoT.

## Dokumenteigenschaften

Ein Geräteschatten-Dokument besitzt die folgenden Eigenschaften:

`state`

`desired`

Den gewünschte Status des Geräts. Anwendungen können diesen Teil des Dokuments beschreiben, um den Status eines Geräts zu aktualisieren, ohne direkt mit diesem verbunden zu sein.

`reported`

Der gemeldete Status des Geräts. Geräte schreiben in diesen Teil des Dokuments, um ihren neuen Status zu melden. Apps lesen diesen Teil des Dokuments, um den zuletzt gemeldeten Zustand des Geräts zu bestimmen.

`metadata`

Informationen über die im Abschnitt `state` (Status) des Dokuments gespeicherten Daten. Dazu zählen Zeitstempel, in Epoche-Uhrzeit, für das jeweilige Attribut im Abschnitt `state` (Status), anhand derer Sie den Zeitpunkt ermitteln können, zu dem sie aktualisiert wurden.

> **Note**
>
> Metadaten zählen nicht zur Dokumentengröße für Service Limits oder Preise. Weitere Informationen finden Sie unter Service Limits AWS IoT.

`timestamp`

Gibt an, von wann die Nachricht gesendet wurde AWS IoT. Durch Verwendung des Zeitstempels in der Nachricht und der Zeitstempel für einzelne Attribute im Abschnitt `desired` oder `reported` kann ein Gerät das Alter einer Eigenschaft bestimmen, selbst wenn das Gerät über keine interne Uhr verfügt.

`clientToken`

Eine für das Gerät einmalige Zeichenfolge, die es Ihnen ermöglicht, Anfragen in einer MQTT-Umgebung Antworten zuzuordnen.

`version`

Die Dokumentversion. Jedes Mal, wenn das Dokument aktualisiert wird, erhöht sich diese Versionsnummer. Wird verwendet, um sicherzustellen, dass die Versionsnummer des aktualisierten Dokuments die neueste ist.

Weitere Informationen finden Sie unter Beispiele für Schatten-Dokumente.

## Delta-Status

Der Delta-Status ist ein virtueller Typ eines Status, in dem der Unterschied zwischen dem Status `desired` (Soll) Status und dem Status `reported` (gemeldet) enthalten ist. Felder im Abschnitt `desired` (Soll), die nicht im Abschnitt `reported` (gemeldet) enthalten sind, sind im Delta enthalten. Felder, die im Abschnitt `reported` (gemeldet) und nicht im Abschnitt `desired` (Soll) enthalten sind, sind nicht im Delta enthalten. Das Delta enthält Metadaten und seine Werte entsprechen den Metadaten im Feld `desired` (Soll). Zum Beispiel:

```
{
  "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
        }
      }
    },
    "version": 17,
    "timestamp": 123456789
  }
}
```

Wenn die verschachtelten Objekte differieren, enthält das Delta den Pfad bis hin zum Stammverzeichnis.

```
{
  "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
}
```

Der Device Shadow-Service berechnet das Delta, indem er jedes einzelne Feld im Status `desired` (Soll) durchläuft und mit dem Status `reported` (gemeldet) abgleicht.

Arrays werden wie Werte behandelt. Stimmt ein Array im Abschnitt `desired` (Soll) nicht mit dem Array im Abschnitt `reported` (gemeldet) überein, dann wird das gesamte "Soll”-Array in das Delta kopiert.

## Versioning von Schattendokumenten

Der Device Shadow-Service unterstützt das Versioning für jede Aktualisierungsnachricht, sowohl Anforderung als auch Antwort. Dies bedeutet, dass bei jeder Aktualisierung eines Schattens die Version des JSON-Dokuments erhöht wird. Dies gewährleistet Folgendes:

- Ein Client kann eine Fehlermeldung empfangen, wenn versucht wird, einen Schatten mit einer älteren Versionsnummer zu überschreiben. Der Client wurde darüber informiert, dass eine neue Synchronisation erfolgen muss, bevor ein Geräteschatten aktualisiert werden kann.
- Ein Client kann entscheiden, bei einer erhaltenen Nachricht nicht tätig zu werden, wenn die Nachricht über eine niedrigere Version verfügt als die vom Client gespeicherte Version.

Ein Client kann den Versionsabgleich umgehen, indem er keine Version in das Schattendokument aufnimmt.

## Client-Tokens in Schattendokumenten

Bei MQTT-basiertem Messaging können Sie einen Client-Token verwenden, um zu überprüfen, ob derselbe Client-Token in einer Anfrage und Antwort auf eine Anfrage enthalten ist. Dies stellt sicher, dass Antwort und Anfrage miteinander verknüpft sind.

> **Note**
>
> Das Client-Token darf nicht länger als 64 Bytes sein. Ein Client-Token, das länger als 64 Bytes ist, verursacht eine 400er-Antwort (Bad Request) und die Fehlermeldung Invalid clientToken (Ungültiges Client-Token).

## Eigenschaften des leeren Schattendokuments

Die Eigenschaften `reported` und `desired` in einem Schattendokument können leer sein oder weggelassen werden, wenn sie nicht für den aktuellen Schattenstatus gelten. Ein Schattendokument enthält beispielsweise nur dann eine `desired`-Eigenschaft, wenn es einen gewünschten Status hat. Der folgende Code ist ein gültiges Beispiel für ein Statusdokument ohne `desired`-Eigenschaft:

```
{
    "reported" : { "temp": 55 }
}
```

Die `reported`-Eigenschaft kann auch leer sein, z. B. wenn der Schatten nicht vom Gerät aktualisiert wurde:

```
{
    "desired" : { "color" : "RED" }
}
```

Wenn eine Aktualisierung bewirkt, dass die Eigenschaft `desired` oder `reported` null wird, wird diese aus dem Dokument entfernt. Nachfolgend wird gezeigt, wie Sie die `desired`-Eigenschaft entfernen, indem Sie sie auf `null` festlegen. Sie können dies beispielsweise tun, wenn ein Gerät seinen Status aktualisiert.

```
{
```

```
    "state": {
        "reported": {
            "color": "red"
        },
        "desired": null
    }
}
```

Ein Schattendokument kann auch keine `desired`- oder `reported`-Eigenschaft haben, wodurch das Schattendokument leer wird. Dies ist ein Beispiel für ein leeres, aber gültiges Schattendokument.

```
{
}
```

## Array-Werte in Schattendokumenten

Schatten unterstützen zwar Arrays, können diese jedoch so als normale Werte behandeln, dass bei einer Aktualisierung eines Arrays das gesamte Array ersetzt wird. Es ist nicht möglich, einen Teil eines Arrays zu aktualisieren.

Ursprungszustand:

```
{
    "desired" : { "colors" : ["RED", "GREEN", "BLUE" ] }
}
```

Aktualisieren:

```
{
    "desired" : { "colors" : ["RED"] }
}
```

Endzustand:

```
{
    "desired" : { "colors" : ["RED"] }
}
```

Arrays können keine Nullwerte besitzen. Das folgende Array ist z. B. ungültig und wird abgelehnt.

```
{
    "desired" : {
        "colors" : [ null, "RED", "GREEN" ]
    }
}
```

# Device Shadow-Fehlermeldungen

Der Device Shadow-Service veröffentlicht (über MQTT) eine Meldung im Thema "Fehler”, wenn ein Versuch, das Statusdokument zu ändern, fehlschlägt. Diese Meldung wird lediglich als Antwort auf eine Veröffentlichungsanfrage zu einem der reservierten `$aws`-Topics ausgegeben. Aktualisiert der Client das Dokument mittels REST-API, erhält er den HTTP-Fehlercode als Teil seiner Antwort, und es werden keine MQTT-Fehlermeldungen ausgegeben.

| HTTP-Fehlercode | Fehlermeldungen |
| --- | --- |
| 400 (Ungültige Anfrage) | • Ungültige JSON<br>• Erforderlicher Knoten fehlt: Status<br>• Der Statusknoten muss ein Objekt sein<br>• Der "Soll”-Knoten muss ein Objekt sein<br>• Der "Gemeldet”-Knoten muss ein Objekt sein<br>• Ungültige Version<br>• Ungültiger Client-Token<br>**Note**<br>Ein Client-Token, das länger als 64 Bytes ist, verursacht diese Antwort.<br>• Die JSON enthält zu viele Verschachtelungsebenen; maximal 6 sind zulässig<br>• Der Status enthält einen ungültigen Knoten |
| 401 (Unauthorized) (Unautorisiert) | • Nicht autorisiert |
| 403 (Forbidden) (Unzulässig) | • Forbidden |

| HTTP-Fehlercode | Fehlermeldungen |
| --- | --- |
| 404 (Not Found) (Nicht gefunden) | • Gerät nicht gefunden<br>• Es gibt keinen Schatten mit dem Namen: *shadowName* |
| 409 (Conflict) (Konflikt) | • Versionskonflikt |
| 413 (Payload Too Large) (Nutzlast zu hoch) | • Die Nutzlast überschreitet die maximal zulässige Größe |
| 415 (Unsupported Media Type) (Nicht unterstützter Medientyp) | • Nicht unterstützte Dokumentkodierung; unterstützte Kodierung: UTF-8 |
| 429 (Too Many Requests) (Zu viele Anfragen) | • Bei mehr als 10 übertragenen Anfragen auf eine einzelne Verbindung erzeugt der Geräteschatten-Service diese Fehlermeldung. Bei einer laufenden Anfrage handelt es sich um eine Anfrage in Bearbeitung, die zwar gestartet, aber noch nicht abgeschlossen wurde. |
| 500 (Internal Server Error) (Interner Serverfehler) | • Interner Service-Fehler |

# AWS IoT Device Management Softwarepaketkatalog

Mit dem AWS IoT Device Management Softwarepaketkatalog können Sie ein Inventar von Softwarepaketen und deren Versionen verwalten. Sie können Paketversionen einzelnen Dingen und AWS IoT dynamischen Dinggruppen zuordnen und sie über interne Prozesse oder AWS IoT Jobs bereitstellen.

Ein Softwarepaket enthält eine oder mehrere Paketversionen, eine Sammlung von Dateien, die als einzelne Einheit bereitgestellt werden können. Paketversionen können Firmware, Betriebssystemupdates, Geräteanwendungen, Konfigurationen und Sicherheitspatches enthalten. Da sich die Software im Laufe der Zeit weiterentwickelt, können Sie eine neue Paketversion erstellen und sie in Ihrer Flotte einsetzen.

Der Hub für AWS IoT Softwarepakete befindet sich darin AWS IoT Core. Sie können den Hub verwenden, um Ihr Softwarepaketinventar und Ihre Metadaten zentral zu registrieren und zu verwalten, wodurch ein Katalog von Softwarepaketen und deren Versionen erstellt wird. Sie können Geräte auf der Grundlage von Softwarepaketen und Paketversionen gruppieren, die auf dem Gerät bereitgestellt werden. Diese Funktion bietet die Möglichkeit, das geräteseitige Paketinventar als benannten Schatten zu verwalten, Geräte anhand von Versionen zuzuordnen und zu gruppieren und die Verteilung der Paketversionen innerhalb der Flotte anhand von Flottenmetriken zu visualisieren.

Wenn Sie ein internes Softwarebereitstellungssystem eingerichtet haben, können Sie diesen Prozess weiterhin für die Bereitstellung Ihrer Paketversionen verwenden. Wenn Sie noch keinen Bereitstellungsprozess eingerichtet haben oder wenn Sie es vorziehen, empfehlen wir, AWS IoT Jobs zu verwenden, um die Funktionen im Softwarepaket-Katalog zu verwenden. Weitere Informationen finden Sie unter AWS IoT Jobs vorbereiten.

Dieses Kapitel enthält die folgenden Abschnitte:

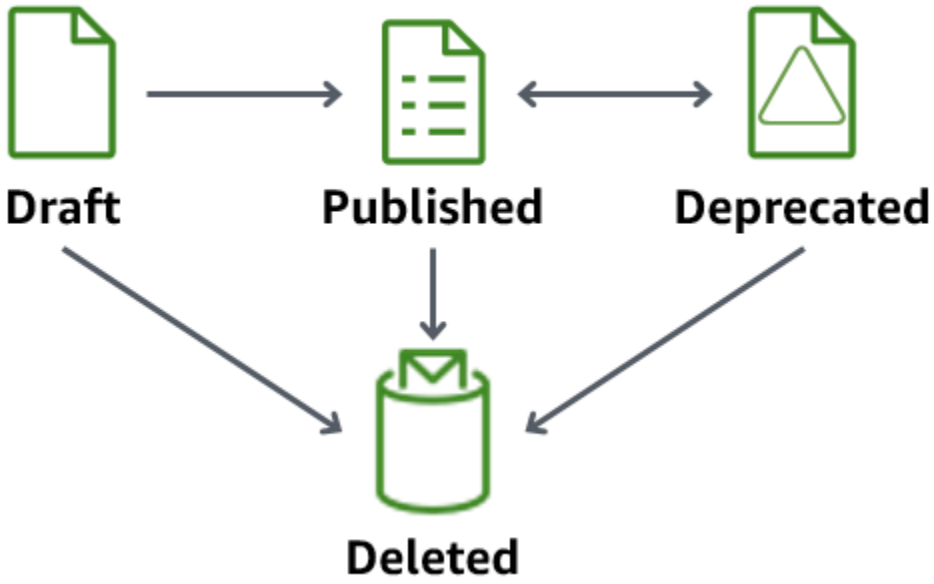
- Vorbereitung der Verwendung des Softwarepaket-Katalogs
- Vorbereitung der Sicherheit
- Vorbereitung der Flottenindizierung
- Jobs vorbereiten AWS IoT
- Erste Schritte mit dem Softwarepaket-Katalog

# Vorbereitung der Verwendung des Softwarepaket-Katalogs

Der folgende Abschnitt bietet einen Überblick über den Lebenszyklus der Paketversionen und Informationen zur Verwendung des AWS IoT Device Management Softwarepaketkatalogs.

## Lebenszyklus der Paketversion

Eine Paketversion kann sich in den folgenden Lebenszyklusstatus weiterentwickeln: `draft`, `published`, und `deprecated`. Sie kann auch `deleted` sein.




- Entwurf

  Wenn Sie eine Paketversion erstellen, befindet sie sich in einem `draft` Status. Dieser Status weist darauf hin, dass das Softwarepaket vorbereitet wird oder unvollständig ist.

  Solange sich die Paketversion in diesem Zustand befindet, können Sie sie nicht bereitstellen. Sie können die Beschreibung, Attribute und Tags der Paketversion bearbeiten.

  Sie können eine Paketversion, die sich im `draft` Status befindet, mithilfe der Konsole `published` oder `deleted` durch Ausführen von DeletePackageVersionAPI-Vorgängen in den Status „In“ UpdatePackageVersionoder „Befinden“ umwandeln.
- Veröffentlicht

  Wenn Ihre Paketversion bereit für die Bereitstellung ist, stellen Sie die Paketversion in einen `published` Status um. In diesem Status können Sie wählen, ob Sie die Paketversion als

Standardversion identifizieren möchten, indem Sie das Softwarepaket in der Konsole oder über den UpdatePackageAPI-Vorgang bearbeiten. In diesem Status können Sie nur die Beschreibung und die Tags bearbeiten.

Sie können eine Paketversion, die sich im `published` Status befindet, mithilfe der Konsole `deprecated` oder mithilfe der API-Operationen oder `deleted` durch Ausführen von DeletePackageVersionAPI-Operationen auf den Status „UpdatePackageVersionBefinden“ umstellen.

- Als veraltet gekennzeichnet

  Wenn eine neue Paketversion verfügbar ist, können Sie frühere Paketversionen auf `deprecated` umstellen. Sie können weiterhin Jobs mit einer veralteten Paketversion bereitstellen. Sie können auch eine veraltete Paketversion als Standardversion benennen und nur die Beschreibung und die Tags bearbeiten.

  Erwägen Sie, eine Paketversion auf eine Version umzustellen, `deprecated` wenn die Version veraltet ist, Sie aber immer noch Geräte im Einsatz haben, die die ältere Version verwenden, oder müssen sie aufgrund von Laufzeitabhängigkeiten warten.

  Sie können eine Paketversion, die sich im `deprecated` Status befindet, mithilfe der Konsole `published` oder `deleted` durch Ausführen von API-Vorgängen auf die aktuelle Version umstellen. UpdatePackageVersionDeletePackageVersion

- Deleted (Gelöscht)

  Wenn Sie eine Paketversion nicht mehr verwenden möchten, können Sie sie löschen, indem Sie die Konsole verwenden oder den DeletePackageVersionAPI-Vorgang ausführen.

  > **Note**
  >
  > Wenn Sie eine Paketversion löschen, während noch ausstehende Aufträge darauf verweisen, erhalten Sie eine Fehlermeldung, wenn der Auftrag erfolgreich abgeschlossen wurde und versucht wird, den reservierten Named Shadow zu aktualisieren.
  > Wenn die Softwarepaketversion, die Sie löschen möchten, als Standardpaketversion benannt ist, müssen Sie das Paket zuerst aktualisieren, um eine andere Version als Standardversion zu benennen, oder das Feld unbenannt lassen. Sie können dies mithilfe der Konsole oder der UpdatePackageVersionAPI-Operation tun. (Um eine benannte

Paketversion als Standard zu entfernen, setzen Sie den unsetDefaultVersionParameter auf true, wenn Sie den UpdatePackageAPI-Vorgang ausführen.)

Wenn Sie ein Softwarepaket über die Konsole löschen, werden alle mit diesem Paket verknüpften Paketversionen gelöscht, sofern nicht eine als Standardversion benannt ist.

## Namenskonventionen für Paketversionen

Wenn Sie Paketversionen benennen, ist es wichtig, eine logische Benennungsstrategie zu planen und anzuwenden, damit Sie und andere leicht die neueste Paketversion und den Versionsverlauf erkennen können. Sie müssen bei der Erstellung der Paketversion einen Versionsnamen angeben, aber die Strategie und das Format hängen weitgehend von Ihrem Geschäftsszenario ab.

Als bewährte Methode empfehlen wir die Verwendung des Semantic SemVerVersioning-Formats. Zum Beispiel, `1.2.3` wo `1` die Hauptversion für funktionell inkompatible Änderungen ist, `2` die Hauptversion für funktionell kompatible Änderungen und `3` die Patch-Version (für Fehlerbehebungen) ist. Weitere Informationen finden Sie unter Semantic Versioning 2.0.0. Weitere Informationen zu den Anforderungen an die Paketversionsnamen finden Sie unter VersionName im AWS IoT API-Referenzhandbuch.

## Standardversion

Das Festlegen einer Version als Standard ist optional. Sie können Standard-Paketversionen hinzufügen oder entfernen. Sie können auch eine Paketversion bereitstellen, die nicht als Standardversion benannt ist.

Wenn Sie eine Paketversion erstellen, wird sie in einen `draft` Status versetzt und kann erst dann als Standardversion bezeichnet werden, wenn Sie die Paketversion auf veröffentlicht umstellen. Der Softwarepaket-Katalog wählt nicht automatisch eine Version als Standard aus oder aktualisiert eine neuere Paketversion als Standard. Sie müssen die von Ihnen gewählte Paketversion bewusst über die Konsole oder durch Ausführen des UpdatePackageVersionAPI-Vorgangs benennen.

## Versionsattribute

Versionsattribute und ihre Werte enthalten wichtige Informationen über Ihre Paketversionen. Wir empfehlen Ihnen, allgemeine Attribute für ein Paket oder eine Paketversion zu definieren.

Sie können beispielsweise ein Name-Wert-Paar für Plattform, Architektur, Betriebssystem, Veröffentlichungsdatum, Autor oder Amazon-S3-URL erstellen.

Wenn Sie einen AWS IoT Job mit einem Jobdokument erstellen, können Sie auch eine Substitutionsvariable (`$parameter`) verwenden, die auf den Wert eines Attributs verweist. Weitere Informationen finden Sie unter AWS IoT Jobs vorbereiten.

Versionsattribute, die in Paketversionen verwendet werden, werden nicht automatisch zum reservierten benannten Schatten hinzugefügt und können nicht direkt über Fleet Indexing indexiert oder abgefragt werden. Um Paketversionsattribute über Fleet Indexing zu indizieren oder abzufragen, können Sie das Versionsattribut im reservierten benannten Schatten auffüllen.

Wir empfehlen, dass der Versionsattributparameter im reservierten Schatten die vom Gerät gemeldeten Eigenschaften erfasst, z. B. das Betriebssystem und die Installationszeit. Sie können auch über Fleet Indexing indexiert und abgefragt werden.

Für Versionsattribute ist es nicht erforderlich, dass sie einer bestimmten Benennungskonvention entsprechen. Sie können Name-Wert-Paare erstellen, um Ihren Geschäftsanforderungen gerecht zu werden. Die Gesamtgröße aller Attribute in einer Paketversion ist auf 3 KB begrenzt. Weitere Informationen finden Sie unter Beschränkungen für Softwarepakete und Paketversionen im Softwarepaket-Katalog.

Alle Attribute in einem Jobdokument verwenden

Sie können festlegen, dass alle Attribute der Paketversion automatisch zu Ihrer Auftragsbereitstellung für ausgewählte Geräte hinzugefügt werden. Informationen zur automatischen programmgesteuerten Verwendung aller Paketversionsattribute in einem API- oder CLI-Befehl finden Sie im folgenden Beispiel für ein Jobdokument:

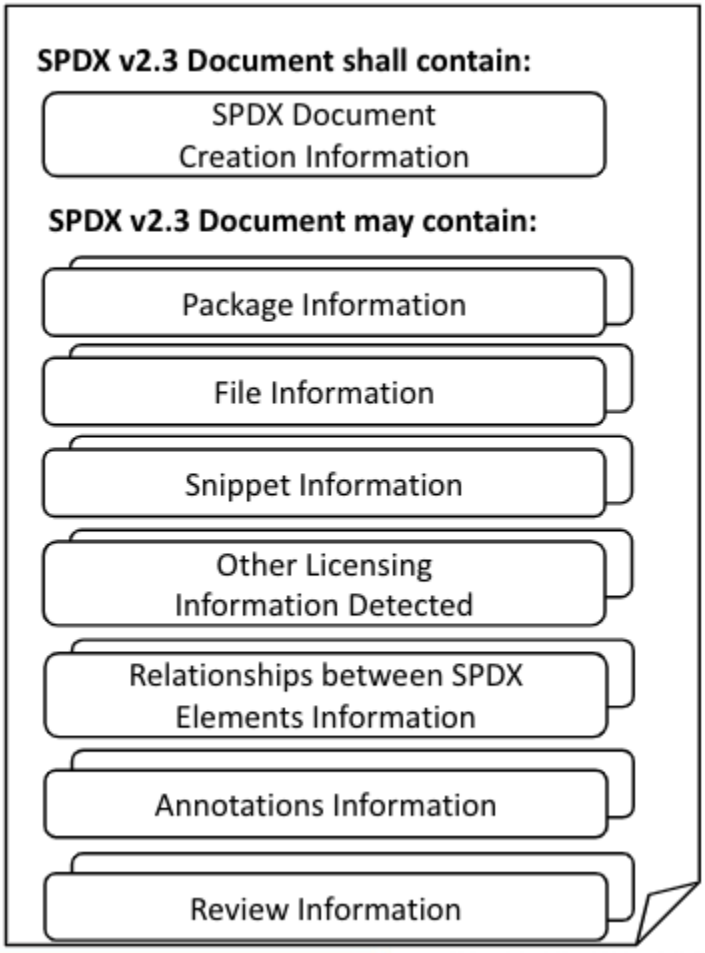
```
"TestPackage": "${aws:iot:package:TestPackage:version:PackageVersion:attributes}"
```

## Stückliste der Software

Die Softwareliste (SBOM) bietet eine zentrale Ablage für alle Aspekte Ihres Softwarepakets. Zusätzlich zum Speichern von Softwarepaketen und Paketversionen können Sie die mit jeder Paketversion verknüpfte Softwareliste (SBOM) im AWS IoT Device Management Softwarepaketkatalog speichern. Ein Softwarepaket enthält eine oder mehrere Paketversionen, und jede Paketversion besteht aus einer oder mehreren Komponenten. Jede dieser Komponenten, die die Zusammenstellung einer bestimmten Paketversion unterstützen, kann anhand einer Softwareliste beschrieben und katalogisiert werden. Die unterstützten Industriestandards für Softwarelisten

sind SPDX und CyclonedX. Wenn eine SBOM zum ersten Mal erstellt wird, wird sie anhand des Industriestandardformats SPDX und CyclonedX validiert. Weitere Informationen zu SPDX finden Sie unter System Package Data Exchange. Weitere Informationen zu CyclonedX finden Sie unter CyclonedX.

Die Softwareliste beschreibt alle Aspekte der Komponenten einer bestimmten Paketversion wie Paketinformationen, Dateiinformationen und andere relevante Metadaten. Das folgende Beispiel zeigt die Dokumentstruktur einer Software-Stückliste im SPDX-Format:




## Vorteile der Softwareliste

Einer der wichtigsten Vorteile des Hinzufügens Ihrer Softwareliste für eine Paketversion im Softwarepaketkatalog ist das Schwachstellenmanagement.

Verwaltung von Sicherheitslücken

Die Bewertung und Minderung Ihrer Anfälligkeit gegenüber offensichtlichen Sicherheitsrisiken in Softwarekomponenten ist nach wie vor von entscheidender Bedeutung für den Schutz der

Integrität Ihrer Geräteflotte. Mit der zusätzlichen Softwareliste, die im Softwarepaketkatalog für jede Paketversion gespeichert ist, können Sie proaktiv Sicherheitslücken aufdecken, indem Sie mithilfe Ihrer eigenen internen Schwachstellen-Management-Lösung wissen, welche Geräte je nach Paketversion und SBOM gefährdet sind. Sie können Fixes auf den betroffenen Geräten installieren und Ihre Geräteflotte schützen.

## Aufbewahrung von Softwarelisten

Die Softwarelisten (SBOM) für jede Softwarepaketversion werden mithilfe der Amazon S3 S3-Versionierungsfunktion in einem Amazon S3 S3-Bucket gespeichert. Der Amazon S3 S3-Bucket, in dem die SBOM gespeichert ist, muss sich in derselben Region befinden, in der die Paketversion erstellt wurde. Ein Amazon S3 S3-Bucket, der die Versionierungsfunktion verwendet, verwaltet mehrere Varianten eines Objekts in demselben Bucket. Weitere Informationen zur Verwendung der Versionierung in einem Amazon S3 S3-Bucket finden Sie unter Verwenden der Versionierung in Amazon S3 S3-Buckets.

> **Note**
>
> An jede Softwarepaketversion können mehrere SBOM-Dateien angehängt werden, aber die SBOM-Dateien müssen in einer einzigen Zip-Archivdatei gespeichert werden.

Der spezifische Amazon S3 S3-Schlüssel und die Versions-ID für Ihren Bucket werden verwendet, um jede Version einer Softwareliste für eine Paketversion eindeutig zu identifizieren.

> **Note**
>
> Für eine Paketversion mit einer einzelnen SBOM-Datei können Sie diese SBOM-Datei in Ihrem Amazon S3-Bucket als Zip-Archivdatei speichern.
> Für eine Paketversion mit mehreren SBOM-Dateien müssen Sie alle SBOM-Dateien in einer einzigen Zip-Archivdatei platzieren und diese Zip-Archivdatei dann in Ihrem Amazon S3 S3-Bucket speichern.
> Alle SBOM-Dateien, die in beiden Szenarien in der einzigen Zip-Archivdatei gespeichert sind, sind entweder als SPDX- oder CyclonedX-.json-Dateien formatiert.

### Richtlinie für Berechtigungen

Um als spezifizierter AWS IoT Principal auf die im Amazon S3-Bucket gespeicherten SBOM-Zip-Archivdateien zugreifen zu können, benötigen Sie eine ressourcenbasierte Berechtigungsrichtlinie. Im folgenden Beispiel finden Sie die richtige ressourcenbasierte Berechtigungsrichtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "iot.amazonaws.com"
                ]
            },
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::bucketName/*"
        }
    ]
}
```

Weitere Informationen zu ressourcenbasierten Berechtigungsrichtlinien finden Sie unter Ressourcenbasierte AWS IoT -Richtlinien

Aktualisierung der SBOM

Sie können die Softwareliste so oft wie nötig aktualisieren, um Ihre Geräteflotte zu schützen und zu erweitern. Jedes Mal, wenn die Softwareliste in Ihrem Amazon S3 S3-Bucket aktualisiert wird, ändert sich die Versions-ID und Sie müssen die neue Amazon S3 S3-Bucket-URL der entsprechenden Softwarepaketversion zuordnen. Sie werden die neue Versions-ID in der Spalte Amazon S3 S3-Objekt-Versions-ID auf der Seite mit der Paketversion im sehen AWS Management Console. Darüber hinaus können Sie den API-Vorgang `GetPackageVersion` oder den CLI-Befehl verwenden`get-package-version`, um die neue Versions-ID anzuzeigen.

> **Note**
>
> Wenn Sie Ihre Softwareliste aktualisieren, was zu einer neuen Versions-ID führt, wird keine neue Paketversion erstellt.

Weitere Informationen zu Amazon S3 S3-Objektschlüsseln finden Sie unter Objektschlüsselnamen erstellen.

# Aktivierung der AWS IoT Flottenindizierung

Die Aktivierung der AWS IoT Flottenindizierung ist eine Voraussetzung für die Verwendung des AWS IoT Device Management Softwarepaketkatalogs. Um die AWS IoT Flottenindizierung mit dem Softwarepaketkatalog zu nutzen, legen Sie den reservierten benannten Schatten (`$package`) als Datenquelle für jedes Gerät fest, auf dem Sie indizieren und Metriken sammeln möchten. Weitere Informationen zu reservierten benannten Schatten finden Sie unterReservierter benannter Schatten.

Die Flottenindizierung bietet Unterstützung, sodass AWS IoT Dinge anhand dynamischer Dinggruppen gruppiert werden können, die nach der Version des Softwarepakets gefiltert werden. Mit der Flottenindizierung können beispielsweise Objekte identifiziert werden, für die eine bestimmte Paketversion installiert ist oder für die keine Paketversionen installiert sind oder die bestimmten Name-Wert-Paaren entsprechen. Schließlich bietet die Flottenindizierung standardmäßige und benutzerdefinierte Messwerte, anhand derer Sie sich einen Überblick über den Status Ihrer Geräteflotte verschaffen können. Weitere Informationen finden Sie unter Vorbereitung der Flottenindizierung.

> **Note**
>
> Die Aktivierung der Flottenindizierung für den Softwarepaket-Katalog verursacht Standard-Servicekosten. Weitere Informationen finden Sie unter AWS IoT Device Management-Preisgestaltung.

## Reservierter benannter Schatten

Der reservierte, benannte Schatten, `$package`, gibt den Status der auf dem Gerät installierten Softwarepakete und Paketversionen wieder. Die Flottenindizierung verwendet den reservierten benannten Schatten als Datenquelle, um Standard- und benutzerdefinierte Messwerte zu erstellen, mit denen Sie den Status Ihrer Flotte abfragen können. Weitere Informationen finden Sie unter Vorbereitung der Flottenindizierung

Ein reservierter benannter Schatten ähnelt einem benannten Schatten mit der Ausnahme, dass sein Name vordefiniert ist und Sie ihn nicht ändern können. Darüber hinaus aktualisiert sich der reservierte benannte Schatten nicht mit Metadaten und verwendet nur die Schlüsselwörter `version` und `attributes`.

Bei Aktualisierungsanfragen, die andere Stichwörter enthalten, wie z. B. `description`, wird unter dem `rejected` Thema eine Fehlermeldung angezeigt. Weitere Informationen finden Sie unter Geräteschatten-Fehlermeldungen.

Es kann erstellt werden, wenn Sie AWS IoT etwas über die Konsole erstellen, wenn ein AWS IoT Job erfolgreich abgeschlossen und der Shadow aktualisiert wurde und wenn Sie den `UpdateThingShadow`API-Vorgang ausführen. Weitere Informationen finden Sie UpdateThingShadowim AWS IoT Core Entwicklerhandbuch.

> **Note**
>
> Die Indizierung des reservierten benannten Schattens wird nicht auf die Anzahl der benannten Schatten angerechnet, die von der Flottenindizierung indexiert werden können. Weitere Informationen finden Sie unter AWS IoT Device Management Flottenindizierungsgrenzen und -quoten. Wenn Sie außerdem festlegen, dass AWS IoT Jobs den reservierten Named Shadow aktualisieren, wenn ein Job erfolgreich abgeschlossen wurde, wird der API-Aufruf auf Ihre Device Shadow- und Registrierungsvorgänge angerechnet und kann Kosten verursachen. Weitere Informationen finden Sie unter Limits und Kontingente für AWS IoT Device Management Jobs und IndexingFilterAPI-Datentyp.

Struktur des **`$package`** Schattens

Der reservierte benannte Schatten enthält Folgendes:

```
{
    "state": {
        "reported": {
            "<packageName>": {
                "version": "",
                "attributes": {
                }
            }
        }
    },
    "version" : 1
    "timestamp" : 1672531201
}
```

Die Schatteneigenschaften werden mit den folgenden Informationen aktualisiert:

- `<packageName>`: Der Name des installierten Softwarepakets, das mit dem PackageName-Parameter aktualisiert wird.
- `version`: Der Name der installierten Paketversion, die mit dem VersionName-Parameter aktualisiert wird.
- `attributes`: Optionale Metadaten, die vom Gerät gespeichert und durch Flottenindizierung indexiert werden. Auf diese Weise können Kunden ihre Indizes auf der Grundlage der gespeicherten Daten abfragen.
- `version`: Die Versionsnummer des Schattens. Sie wird jedes Mal, wenn der Schatten aktualisiert wird, automatisch erhöht und beginnt bei 1.
- `timestamp`: Gibt an, wann der Schatten zuletzt aktualisiert wurde, und wird in Unix-Zeit aufgezeichnet.

Weitere Informationen zum Format und Verhalten eines benannten Schattens finden Sie unter AWS-IoT-Device-Shadow-Service Reihenfolge der Nachrichten.

## Löschen eines Softwarepakets und seiner Paketversionen

Führen Sie vor dem Löschen eines Softwarepakets die folgenen Schritte aus:

- Vergewissern Sie sich, dass das Paket und seine Versionen nicht aktiv bereitgestellt werden.
- Löschen Sie zuerst alle zugehörigen Versionen. Wenn eine der Versionen als Standardversion gekennzeichnet ist, müssen Sie die benannte Standardversion aus dem Paket entfernen. Da die Angabe einer Standardversion optional ist, besteht kein Konflikt darin, sie zu entfernen. Um die Standardversion aus dem Softwarepaket zu entfernen, bearbeiten Sie das Paket über die Konsole oder verwenden Sie den UpdatePackageVersionAPI-Vorgang.

Solange es keine benannte Standardpaketversion gibt, können Sie die Konsole verwenden, um ein Softwarepaket zu löschen. Alle zugehörigen Paketversionen werden ebenfalls gelöscht. Wenn Sie einen API-Aufruf zum Löschen von Softwarepaketen verwenden, müssen Sie zuerst die Paketversionen und dann das Softwarepaket löschen.

# Vorbereitung der Sicherheit

In diesem Abschnitt werden die wichtigsten Sicherheitsanforderungen für den AWS IoT Device Management Softwarepaketkatalog beschrieben.

# Ressourcenbasierte Authentifizierung

Der Softwarepaket-Katalog verwendet ressourcenbasierte Autorisierung, um zusätzliche Sicherheit bei der Aktualisierung von Software auf Ihrer Flotte zu bieten. Das bedeutet, dass Sie eine AWS Identity and Access Management (IAM-) Richtlinie erstellen müssen, die Rechte zur Ausführung von`create`,`read`, `update`,`delete`, und `list` Aktionen für Softwarepakete und Paketversionen gewährt, und in diesem `Resources` Abschnitt auf die spezifischen Softwarepakete und Paketversionen verweisen müssen, die Sie bereitstellen möchten. Sie benötigen diese Rechte auch, damit Sie den reservierten benannten Schatten aktualisieren können. Sie verweisen auf die Softwarepakete und Paketversionen, indem Sie einen Amazon-Ressourcennamen (ARN) für jede Entität angeben.

> **Note**
>
> Wenn Sie beabsichtigen, mit der Richtlinie Rechte für API-Aufrufe von Paketversionen (wie CreatePackageVersion, UpdatePackageVersion, DeletePackageVersion) zu gewähren, müssen Sie sowohl das Softwarepaket als auch die Paketversion ARNs in die Richtlinie aufnehmen. Wenn Sie beabsichtigen, dass die Richtlinie Rechte für Softwarepaket-API-Aufrufe (wie CreatePackageUpdatePackage, und DeletePackage) gewährt, müssen Sie nur den Softwarepaket-ARN in die Richtlinie aufnehmen.

Strukturieren Sie das Softwarepaket und die Paketversion ARNs wie folgt:

- Softwarepaket: `arn:aws:iot:<region>:<accountID>:package/<packageName>/package`
- Paketversion: `arn:aws:iot:<region>:<accountID>:package/<packageName>/version/<versionName>`

> **Note**
>
> Es gibt weitere verwandte Rechte, die Sie möglicherweise in diese Richtlinie aufnehmen. Sie könnten beispielsweise einen ARN für `job`, `thinggroup`, und `jobtemplate` angeben. Weitere Informationen und eine vollständige Liste der Richtlinienoptionen finden Sie unter Schützen von Benutzern und Geräten mit AWS IoT Aufträgen.

Wenn Sie beispielsweise über ein Softwarepaket und eine Paketversion verfügen, die wie folgt benannt sind:

- AWS IoT Sache: `myThing`
- Paketname: `samplePackage`
- Version `1.0.0`

Die Richtlinie könnte wie das folgende Beispiel aussehen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:createPackage",
                "iot:createPackageVersion",
                "iot:updatePackage",
                "iot:updatePackageVersion"
            ],
            "Resource": [
               "arn:aws:iot:us-east-1:111122223333:package/samplePackage",
               "arn:aws:iot:us-east-1:111122223333:package/samplePackage/version/1.0.0"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:GetThingShadow",
                "iot:UpdateThingShadow"
            ],
            "Resource": "arn:aws:iot:us-east-1:111122223333:thing/myThing/$package"
        }
    ]
}
```

## AWS IoT Berufsrechte für die Bereitstellung von Paketversionen

Aus Sicherheitsgründen ist es wichtig, dass Sie Rechte zur Bereitstellung von Paketen und Paketversionen gewähren und die spezifischen Pakete und Paketversionen benennen, die sie bereitstellen dürfen. Zu diesem Zweck erstellen Sie eine IAM-Rolle und eine IAM-Richtlinie, die

die Erlaubnis zum Bereitstellen von Aufträgen mit Paketversionen erteilt. Die Richtlinie muss die Zielpaketversionen als Ressource angeben.

IAM-Richtlinie

Die IAM-Richtlinie gewährt das Recht, einen Job zu erstellen, der das Paket und die Version enthält, die im `Resource` Abschnitt genannt werden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:CreateJob",
                "iot:CreateJobTemplate"
            ],
            "Resource":[
                "arn:aws:iot:*:111122223333:job/<jobId>",
                "arn:aws:iot:*:111122223333:thing/<thingName>/$package",
                "arn:aws:iot:*:111122223333:thinggroup/<thingGroupName>",
                "arn:aws:iot:*:111122223333:jobtemplate/<jobTemplateName>",
                "arn:aws:iot:*:111122223333:package/<packageName>/
version/<versionName>"
            ]
        }
    ]
}
```

> **Note**
>
> Wenn Sie einen Auftrag bereitstellen möchten, der ein Softwarepaket und eine Paketversion deinstalliert, müssen Sie einen ARN autorisieren, in dem sich die Paketversion `$null` befindet, z. B. im Folgenden:

```
arn:aws:iot:<regionCode>:111122223333:package/<packageName>/version/$null
```

# AWS IoT Jobrechte zur Aktualisierung des reservierten benannten Schattens

Damit Aufträge den reservierten Namensschatten des Objekts aktualisieren können, wenn der Auftrag erfolgreich abgeschlossen wurde, müssen Sie eine IAM-Rolle und eine Richtlinie erstellen. Dafür gibt es zwei Möglichkeiten in der AWS IoT Konsole. Die erste Möglichkeit besteht darin, ein Softwarepaket in der Konsole zu erstellen. Wenn das Dialogfeld Abhängigkeiten für die Paketverwaltung aktivieren angezeigt wird, können Sie wählen, ob Sie eine vorhandene Rolle verwenden oder eine neue Rolle erstellen möchten. Oder wählen Sie in der AWS IoT Konsole Einstellungen, Indizierung verwalten und dann Indizierung für Gerätepakete und Versionen verwalten aus.

> **Note**
>
> Wenn Sie sich dafür entscheiden, dass der AWS IoT Job Service den reservierten Named Shadow aktualisiert, wenn ein Job erfolgreich abgeschlossen wurde, wird der API-Aufruf auf Ihre Device Shadow- und Registrierungsvorgänge angerechnet und kann Kosten verursachen. Weitere Informationen finden Sie unter AWS IoT Core Preise.

Wenn Sie die Option Rolle erstellen verwenden, beginnt der Name der generierten Rolle mit `aws-iot-role-update-shadows` und enthält die folgenden Richtlinien:

Einrichten einer Rolle

Berechtigungen

Die Berechtigungsrichtlinie gewährt die Rechte, den Objektschatten abzufragen und zu aktualisieren. Der `$package` Parameter im Ressourcen-ARN zielt auf den reservierten benannten Schatten ab.

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

```
        {
            "Effect": "Allow",
            "Action": [
                "iot:GetThingShadow",
                "iot:UpdateThingShadow"
            ],
            "Resource": [
                "arn:aws:iot:<regionCode>:111122223333:thing/<thingName>/$package"
            ]
        }
    ]
}
```

Vertrauensstellung

Zusätzlich zur Berechtigungsrichtlinie erfordert die Rolle eine Vertrauensbeziehung mit AWS IoT Core , sodass die Entität die Rolle übernehmen und den reservierten benannten Schatten aktualisieren kann.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "iot.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Eine Benutzerrichtlinie einrichten

iam: Erlaubnis PassRole

Schließlich müssen Sie die Erlaubnis haben, die Rolle zu übergeben, AWS IoT Core wenn Sie den UpdatePackageConfigurationAPI-Vorgang aufrufen.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iot:UpdatePackageConfiguration"
            ],
            "Resource": "arn:aws:iam::111122223333:role/<roleName>"
        }
    ]
}
```

## AWS IoT Jobs, Berechtigungen zum Herunterladen von Amazon S3

Das Auftragsdokument wird in Amazon S3 gespeichert. Sie beziehen sich beim Versand über AWS IoT Jobs auf diese Datei. Sie müssen AWS IoT Jobs die Rechte zum Herunterladen der Datei (`s3:GetObject`) gewähren. Sie müssen auch eine Vertrauensbeziehung zwischen Amazon S3 und AWS IoT Jobs einrichten. Anweisungen zum Erstellen dieser Richtlinien finden Sie unter Presigned URLs in Managing Jobs.

## Berechtigungen zur Aktualisierung der Softwareliste für eine Paketversion

Um die Softwareliste für eine Paketversion im `Deprecated` Lebenszyklusstatus `DraftPublished`, oder zu aktualisieren, benötigen Sie eine AWS Identity and Access Management Rolle und Richtlinien für das Auffinden der neuen Softwareliste in Amazon S3 und das Aktualisieren der Paketversion in AWS IoT Core.

Zunächst platzieren Sie die aktualisierte Softwareliste in Ihrem versionierten Amazon S3 S3-Bucket und rufen den `UpdatePackageVersion` API-Vorgang mit dem enthaltenen `sboms` Parameter auf. Als Nächstes übernimmt Ihr autorisierter Principal die von Ihnen erstellte IAM-Rolle, sucht die aktualisierte Softwareliste in Amazon S3 und aktualisiert die Paketversion im AWS IoT Core Softwarepaketkatalog.

Die folgenden Richtlinien sind erforderlich, um dieses Update durchzuführen:

Richtlinien

- Vertrauensrichtlinie, die eine Vertrauensbeziehung mit dem autorisierten Principal herstellt, der die IAM-Rolle übernimmt, sodass dieser die aktualisierte Softwareliste aus Ihrem versionierten Bucket in Amazon S3 finden und die Paketversion aktualisieren kann. AWS IoT Core

- ```
  {
      "Version": "2012-10-17",
      "Statement": [
          {
              "Effect": "Allow",
              "Principal": {
                  "Service": "s3.amazonaws.com"
              },
              "Action": "sts:AssumeRole"
          }
      ]
  }
  ```
- ```
  {
      "Version": "2012-10-17",
      "Statement": [
          {
              "Effect": "Allow",
              "Principal": {
                  "Service": "iot.amazonaws.com"
              },
              "Action": "sts:AssumeRole"
          }
      ]
  }
  ```

- Berechtigungsrichtlinie: Richtlinie für den Zugriff auf den Amazon S3 S3-versionierten Bucket, in dem die Softwarelisten für eine Paketversion gespeichert sind, und für die Aktualisierung der Paketversion. AWS IoT Core

  - ```
    {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Action": [
                    "s3:GetObject"
                ],
                "Resource": [
                    "arn:aws:s3:::awsexamplebucket1"
                ]
            }
        ]
    ```
    ```

```
}
```

- ```
  {
      "Version": "2012-10-17",
      "Statement": [
          {
              "Effect": "Allow",
              "Action": [
                  "iot:UpdatePackageVersion"
              ],
              "Resource": [
                  "arn:aws:iot:*:111122223333:package/<packageName>/
  version/<versionName>"
              ]
          }
      ]
  }
  ```

- Rollenberechtigungen weitergeben: Richtlinie, die die Erlaubnis erteilt, die IAM-Rolle an Amazon S3 weiterzugeben und AWS IoT Core wann Sie den UpdatePackageVersion API-Vorgang aufrufen.

  - ```
    {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Action": [
                    "iam:PassRole",
                    "s3:GetObject"
                ],
                    "arn:aws:s3:::awsexamplebucket1"
            }
        ]
    }
    ```

  - ```
    {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Action": [
                    "iam:PassRole",
    ```
    ```

```
                "iot:UpdatePackageVersion"
            ],
            "Resource": "arn:aws:iam::111122223333:role/<roleName>"
        }
    ]
}
```

> **Note**
>
> Sie können die Softwareliste für eine Paketversion, die in den `Deleted` Lebenszyklusstatus übergegangen ist, nicht aktualisieren.

Weitere Informationen zum Erstellen einer IAM-Rolle für einen AWS Dienst finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen für einen Dienst. AWS

Weitere Informationen zum Erstellen eines Amazon S3 S3-Buckets und zum Hochladen von Objekten in diesen Bucket finden Sie unter Bucket erstellen und Objekte hochladen.

# Vorbereitung der Flottenindizierung

Mit der AWS IoT Flottenindizierung können Sie Daten suchen und aggregieren, indem Sie den reservierten Namen shadow () verwenden. `$package` Sie können AWS IoT Dinge auch gruppieren, indem Sie die Reservierter benannter Schatten und dynamische Dinggruppen abfragen. Sie können beispielsweise Informationen darüber finden, welche AWS IoT Dinge eine bestimmte Paketversion verwenden, für die keine bestimmte Paketversion installiert ist oder für die keine Paketversion installiert ist. Sie können weitere Erkenntnisse gewinnen, indem Sie Attribute kombinieren. Zum Beispiel die Identifizierung von Objekten, die eine bestimmte Version und einen bestimmten Objekttyp haben (wie Version 1.0.0 und den Objekttyp pump_sensor). Weitere Informationen finden Sie unter Flottenindizierung.

## Den **$package** Schatten als Datenquelle festlegen

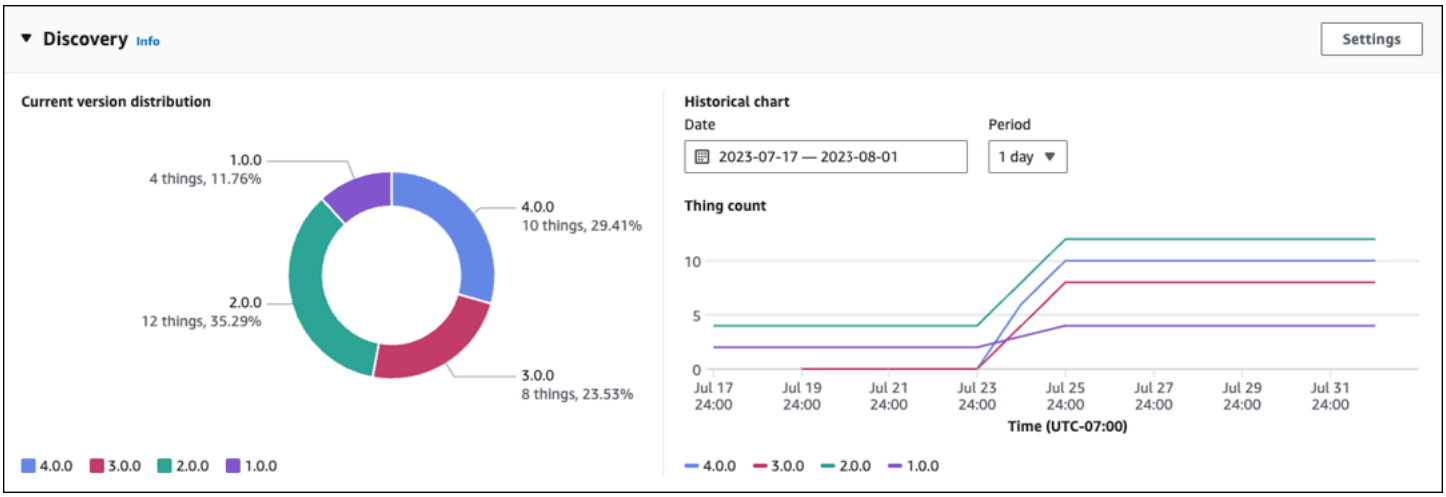
Um die Flottenindizierung mit dem Softwarepaket-Katalog zu verwenden, müssen Sie die Flottenindizierung aktivieren, den benannten Schatten als Datenquelle festlegen und `$package` als benannten Schattenfilter definieren. Wenn Sie die Flottenindizierung nicht aktiviert haben, können Sie sie im Rahmen dieses Vorgangs aktivieren. Öffnen Sie von AWS IoT Core in der Konsole Einstellungen, wählen Sie Indizierung verwalten, dann Benannte Schatten hinzufügen,

Gerätesoftwarepakete und -versionen hinzufügen und Aktualisieren. Weitere Informationen finden Sie unter Verwalten der Objektindizierung.

Alternativ können Sie die Flottenindizierung aktivieren, wenn Sie Ihr erstes Paket erstellen. Wenn das Dialogfeld Abhängigkeiten für die Paketverwaltung aktivieren angezeigt wird, wählen Sie die Option, Gerätesoftwarepakete und -versionen als Datenquellen zur Flottenindizierung hinzuzufügen. Durch Auswahl dieser Option aktivieren Sie auch die Flottenindizierung.

> **Note**
>
> Die Aktivierung der Flottenindizierung für den Softwarepaket-Katalog verursacht Standard-Servicekosten. Weitere Informationen finden Sie unter AWS IoT Device Management-Preisgestaltung.

## In der Konsole dargestellte Metriken




Auf der Detailseite des AWS IoT Konsolen-Softwarepakets werden im Discovery-Bereich Standardmetriken angezeigt, die über den `$package` Shadow aufgenommen wurden.

- Das Diagramm zur Verteilung der aktuellen Version zeigt die Anzahl der Geräte und den Prozentsatz aller Geräte, die diesem Softwarepaket zugeordnet sind, für die 10 neuesten Paketversionen, die einer AWS IoT Sache zugeordnet sind. Hinweis: Wenn das Softwarepaket mehr Paketversionen als die in der Tabelle angegebenen enthält, finden Sie diese unter Andere gruppiert.
- Das Verlaufsdiagramm zeigt die Anzahl der Geräte, die den ausgewählten Paketversionen über einen bestimmten Zeitraum zugeordnet sind. Das Diagramm ist zunächst leer, bis Sie bis zu

5 Paketversionen auswählen und den Datumsbereich und das Zeitintervall definieren. Um die Parameter des Diagramms auszuwählen, wählen Sie Einstellungen. Die im Verlaufsdiagramm angezeigten Daten unterscheiden sich möglicherweise vom Verteilungsdiagramm der aktuellen Version. Dies liegt an der unterschiedlichen Anzahl der angezeigten Paketversionen und auch daran, dass Sie im Verlaufsdiagramm auswählen können, welche Paketversionen analysiert werden sollen. Hinweis: Wenn Sie eine Paketversion zur Visualisierung auswählen, wird diese auf die maximale Anzahl von Flottenkennzahlen angerechnet. Weitere Informationen finden Sie unter Flottenindizierungsgrenzen und -quoten.

Eine weitere Methode, um einen Einblick in die Erfassung der Paketversionsverteilung zu erhalten, finden Sie unter Erfassung der Paketversionsverteilung durch `getBucketsAggregation`.

## Abfragemuster

Die Flottenindizierung mit dem Softwarepaket-Katalog verwendet die meisten der unterstützten Funktionen (z. B. Begriffe und Ausdrücke und Suchfelder), die für die Flottenindizierung Standard sind. Die Ausnahme ist, dass die Abfragen `comparison` und `range` für den reservierten benannten Schattenschlüssel (`$package`) `version` nicht verfügbar sind. Diese Abfragen sind jedoch für den `attributes` Schlüssel verfügbar. Weitere Informationen finden Sie unter Abfragesyntax.

### Beispiel für Daten

Hinweis: Informationen zum reservierten benannten Schatten und seiner Struktur finden Sie unter Reservierter benannter Schatten.

In diesem Beispiel wird ein erstes Gerät `AnyThing` benannt und es sind die folgenden Pakete installiert:

- Softwarepaket: `SamplePackage`

  Paketversion: `1.0.0`

  Paket-ID: `1111`

Der Schatten sieht wie folgt aus:

```
{
    "state": {
```

```
        "reported": {
            "SamplePackage": {
                "version": "1.0.0",
                "attributes": {
                    "s3UrlForSamplePackage": "https://EXAMPIEBUCKET.s3.us-
west-2.amazonaws.com/exampleCodeFile1",
                    "packageID": "1111"
                    }
            }
        }
    }
}
```

Ein zweites Gerät wird `AnotherThing` benannt und hat das folgende Paket installiert:

- Softwarepaket: `SamplePackage`

  Paketversion: `1.0.0`

  Paket-ID: `1111`
- Softwarepaket: `OtherPackage`

  Paketversion: `1.2.5`

  Paket-ID: `2222`

Der Schatten sieht wie folgt aus:

```
{
    "state": {
        "reported": {
            "SamplePackage": {
                "version": "1.0.0",
                "attributes": {
                    "s3UrlForSamplePackage": "https://EXAMPIEBUCKET.s3.us-
west-2.amazonaws.com/exampleCodeFile1",
                    "packageID": "1111"
                }
            },
            "OtherPackage": {
                "version": "1.2.5",
                "attributes": {
```

```
                    "s3UrlForOtherPackage": "https://EXAMPIEBUCKET.s3.us-
west-2.amazonaws.com/exampleCodeFile2",
                    "packageID": "2222"
                    }
            },
        }
    }
}
```

## Beispielabfragen

In der folgenden Tabelle sind Beispielabfragen aufgeführt, die auf den Geräteschatten für `AnyThing` und `AnotherThing` basieren. Weitere Informationen finden Sie unter Beispiel-Objektabfragen.

Aktuelle Version von AWS IoT Device Tester for freeRTOS

| Angeforderte Informationen | Abfrage | Ergebnis |
|---|---|---|
| Objekte, auf denen eine bestimmte Paketversion installiert ist | `shadow.name.$package.reported.SamplePackage.version:1.0.0` | `AnyThing`, `OtherThing` |
| Objekte, auf denen keine bestimmte Paketversion installiert ist | `NOT shadow.name.$package.reported.OtherPackage.version:1.2.5` | `AnyThing` |
| Jedes Gerät, das eine Paketversion verwendet, deren Paket-ID größer als 1500 ist | `shadow.name.$package.reported.*.attributes.packageID>1500"` | `OtherThing` |
| Objekte, auf denen ein bestimmtes Paket installiert ist und auf denen mehr als ein Paket installiert ist | `shadow.name.$package.reported.SamplePackage.version:1.0.0 AND shadow.name.$package.reported.totalCount:2` | `OtherThing` |

## Sammeln der Paketversion und Verteilung über `getBucketsAggregation`

Zusätzlich zum Discovery-Bereich in der AWS IoT Konsole können Sie mithilfe der `GetBucketsAggregation`API-Operation auch Informationen zur Verteilung der Paketversion abrufen. Um die Distributionsinformationen der Paketversion zu erhalten, gehen Sie wie folgt vor:

- Definieren Sie in der Flottenindizierung für jedes Softwarepaket ein benutzerdefiniertes Feld. Hinweis: Die Erstellung benutzerdefinierter Felder wird auf die AWS IoT Service Quotas für die Flottenindexierung angerechnet.
- Formatieren Sie das benutzerdefinierte Feld wie folgt:

  `shadow.name.$package.reported.<packageName>.version`

Weitere Informationen finden Sie im Abschnitt Benutzerdefinierte Felder in der AWS IoT Flottenindizierung.

# Jobs vorbereiten AWS IoT

AWS IoT Device Management Der Softwarepaketkatalog erweitert AWS IoT Jobs um Ersetzungsparameter und die Integration mit AWS IoT Flottenindizierung, dynamischen Dinggruppen und dem reservierten Named AWS IoT Shadow des Dings.

> **Note**
>
> Um alle Funktionen nutzen zu können, die der Softwarepaketkatalog bietet, müssen Sie die folgenden AWS Identity and Access Management (IAM-) Rollen und Richtlinien erstellen: AWS IoT Job-Rechte zum Bereitstellen von Paketversionen und AWS IoT Job-Rechte zum Aktualisieren des reservierten Named Shadow. Weitere Informationen finden Sie unter Vorbereitung der Sicherheit

## Ersetzungsparameter für Jobs AWS IoT

Sie können Substitutionsparameter als Platzhalter in Ihrem AWS IoT Jobdokument verwenden. Wenn der Auftragsservice auf einen Substitutionsparameter stößt, verweist er den Auftrag auf das Attribut einer benannten Softwareversion für den Parameterwert. Sie können diesen Prozess verwenden,

um ein einzelnes Auftragsdokument zu erstellen und die Metadaten über allgemeine Attribute an den Auftrag zu übergeben. Sie könnten z. B. eine Amazon Simple Storage Service (Amazon S3) - URL, einen Amazon-Ressourcennamen (ARN) eines Softwarepakets (ARN) oder eine Signatur über Paketversionsattribute an das Auftragsdokument übergeben.

Die Substitutionsparameter sollten im Jobdokument wie folgt formatiert sein:

- Name und Paketversion des Softwarepakets
  - Die leere Zeichenfolge zwischen `package::version` steht für den Ersatzparameter für den Softwarepaketnamen. Die leere Zeichenfolge zwischen `version::attribute` steht für den Ersetzungsparameter für die Softwarepaketversion. Das folgende Beispiel zeigt, wie Sie die Ersetzungsparameter für den Paketnamen und die Paketversion in einem Jobdokument verwenden:. `${aws:iot:package::version::attributes:<attributekey>}`
  - Das Jobdokument füllt diese Ersetzungsparameter automatisch mit dem Versions-ARN aus den Paketversionsdetails aus. Wenn Sie einen Job oder eine Jobvorlage für eine Einzelpaket-Bereitstellung mithilfe eines API- oder CLI-Befehls erstellen, wird der Versions-ARN für eine Paketversion durch den `destinationPackageVersions` Parameter in `CreateJob` und `DescribeJob` dargestellt.
- Alle Attribute für eine Softwarepaketversion
  - Das folgende Beispiel zeigt, wie Sie den Ersatzparameter „Alle Attribute“ einer Softwarepaketversion in einem Jobdokument verwenden: `${aws:iot:package:<packageName>:version:<versionName>:attributes}`

> **Note**
>
> Der Paketname, die Paketversion und alle Ersetzungsparameter für Attribute können zusammen verwendet werden. Das folgende Beispiel zeigt, wie alle drei Substitutionsparameter in einem Jobdokument verwendet werden: `${aws:iot:package::version::attributes}`

Im folgenden Beispiel gibt es ein Softwarepaket mit dem Namen `samplePackage` und dem Namen einer Paketversion mit `2.1.5` den folgenden Attributen:

- Name: `s3URL`, Wert: `https://EXAMPIEBUCKET.s3.us-west-2.amazonaws.com/exampleCodeFile`

  - Dieses Attribut identifiziert den Speicherort der Codedatei, die in Amazon S3 gespeichert ist.
- Name: `signature`, Wert: `aaaaabbbbbccccddddeeeeeffffgggggghhhhhiiiiijjjj`
  - Dieses Attribut stellt einen Wert für die Codesignatur bereit, den das Gerät als Sicherheitsmaßnahme benötigt. Weitere Informationen finden Sie unter Codesignatur für Aufträge. Hinweis: Dieses Attribut ist ein Beispiel und nicht als Teil des Softwarepaket-Katalogs oder von Aufträgen erforderlich.

Für `s3URL` wird der Auftragsdokumentparameter wie folgt geschrieben:

```
{
"samplePackage": "${aws:iot:package:samplePackage1:version:2.1.5:attributes:s3URL}"
}
```

Für `signature` wird der Auftragsdokumentparameter wie folgt geschrieben:

```
{
"samplePackage": "${aws:iot:package:samplePackage1:version:2.1.5:attributes:signature}"
}
```

Das vollständige Auftragsdokument ist wie folgt geschrieben:

```
{
  ...
  "Steps": {
    "uninstall": ["samplePackage"],
    "download": [
      {
        "samplePackage":
 "${aws:iot:package:samplePackage1:version:2.1.5:attributes:s3URL}"
      },
    ],
    "signature": [
      "samplePackage" :
 "${aws:iot:package:samplePackage1:version:2.1.5:attributes:signature}"
    ]
  }
}
```

Nachdem die Ersetzung vorgenommen wurde, wird das folgende Auftragsdokument auf den Geräten bereitgestellt:

```
{
  ...
  "Steps": {
    "uninstall": ["samplePackage"],
    "download": [
      {
        "samplePackage": "https://EXAMPIEBUCKET.s3.us-west-2.amazonaws.com/
exampleCodeFile"
      },
    ],
    "signature": [
      "samplePackage" : "aaaaabbbbbcccccdddddeeeeeffffffgggggghhhhhiiiiijjjj"
    ]
  }
}
```

Ersetzungsparameter (Vorher- und Nachher-Ansicht)

Ersetzungsparameter vereinfachen die Erstellung eines Auftragsdokuments mithilfe verschiedener Flags, z. B. `$default` für die Standardpaketversion. Dadurch entfällt die Notwendigkeit, spezifische Paketversionsmetadaten für jede Auftragsbereitstellung manuell einzugeben, da diese Flags automatisch mit den referenzierten Metadaten in der jeweiligen Paketversion gefüllt werden. Weitere Informationen zu Paketversionsattributen, z. B. `$default` zur Standard-Paketversion, finden Sie unter. Vorbereitung des Auftragsdokuments und der Paketversion für die Bereitstellung

Klicken Sie im Fenster des AWS Management ConsoleEditors für die Installationsanweisungsdatei während der Bereitstellung einer Paketversion auf die Schaltfläche Substitution in der Vorschau anzeigen, um das Auftragsdokument mit und ohne die Ersetzungsparameter anzuzeigen.

Mithilfe des Parameters „before-substitution“ im Feld und können Sie sich die API-Antwort vor `DescribeJob` und `GetJobDocument` APIs nach dem Entfernen der Substitutionsparameter anzeigen lassen. Sehen Sie sich die folgenden Beispiele mit dem und an: `DescribeJob` `GetJobDocument` APIs

- `DescribeJob`
  - Standardansicht

    ```
    {
    ```

```
    "jobId": "<jobId>",
    "description": "<description>",
    "destinationPackageVersions": ["arn:aws:iot:us-west-2:123456789012:package/
TestPackage/version/1.0.2"]
}
```

- Ansicht „Vor der Ersetzung“

```
{
    "jobId": "<jobId>",
    "description": "<description>",
    "destinationPackageVersions": ["arn:aws:iot:us-west-2:123456789012:package/
TestPackage/version/$default"]
}
```

- `GetJobDocument`
  - Standardansicht

```
{
    "attributes": {
        "location": "prod-artifacts.s3.us-east-1.amazonaws.com/mqtt-core",
        "signature": "IQoJb3JpZ2luX2VjEIrwEaCXVzLWVhc3QtMSJHMEUCIAofPNPpZ9cI",
        "streamName": "mqtt-core",
        "fileId": "0"
    },
}
```

  - Ansicht „Vor der Ersetzung“

```
{
    "attributes": "${aws:iot:package:TestPackage:version:$default:attributes}",
}
```

Weitere Informationen zu AWS IoT Jobs, zum Erstellen von Jobdokumenten und zum Bereitstellen von Jobs finden Sie unter Jobs.

# Vorbereitung des Auftragsdokuments und der Paketversion für die Bereitstellung

Wenn eine Paketversion erstellt wird, befindet sie sich in einem `draft` Zustand, der anzeigt, dass sie für die Bereitstellung vorbereitet wird. Um die Paketversion für die Bereitstellung vorzubereiten, müssen Sie ein Job-Dokument erstellen, das Dokument an einem Ort speichern, auf den der Job zugreifen kann (z. B. Amazon S3), und sicherstellen, dass die Paketversion die Attributwerte enthält, die das Job-Dokument verwenden soll. (Hinweis: Sie können Attribute für eine Paketversion nur aktualisieren, solange sie sich im `draft` Status befindet.)

Wenn Sie einen AWS IoT Job oder eine Job-Vorlage für eine Einzelpaket-Bereitstellung erstellen, haben Sie die folgenden Optionen, um Ihr Job-Dokument anzupassen:

Anweisungsdatei für die Bereitstellung () **`recipe`**

- Die Bereitstellungsanweisungsdatei für eine Paketversion enthält die Bereitstellungsanweisungen, einschließlich eines Inline-Jobdokuments, für die Bereitstellung einer Paketversion auf mehreren Geräten. Die Datei ordnet einer Paketversion spezifische Bereitstellungsanweisungen zu, um eine schnelle und effiziente Auftragsbereitstellung zu ermöglichen.

  In können Sie die AWS Management Console Datei im Vorschaufenster mit den Bereitstellungsanweisungen auf der Registerkarte Konfigurationen für die Versionsbereitstellung des Workflows „Neues Paket erstellen“ erstellen. Mithilfe der Option Mit  AWS IoT empfohlener Datei beginnen können Sie automatisch eine Anweisungsdatei aus Ihren Paketversionsattributen generieren oder Ihr vorhandenes Auftragsdokument verwenden, das in einem Amazon S3 S3-Bucket gespeichert ist, indem Sie Ihre eigene Bereitstellungsanweisungsdatei verwenden. AWS IoT

  > **Note**
  >
  > Wenn Sie Ihr eigenes Auftragsdokument verwenden, können Sie es direkt im Vorschaufenster mit den Bereitstellungsanweisungen aktualisieren. Ihr ursprüngliches Auftragsdokument, das in Ihrem Amazon S3 S3-Bucket gespeichert ist, wird dadurch jedoch nicht automatisch aktualisiert.

Wenn Sie den AWS CLI oder verwenden, `recipe` steht ein API-Befehl wie`CreatePackageVersion`, `GetPackageVersion``UpdatePackageVersion`, oder für die Bereitstellungsanweisungsdatei, die ein Inline-Jobdokument enthält.

Weitere Informationen darüber, was ein Jobdokument ist, finden Sie unterGrundkonzepte.

Im folgenden Beispiel finden Sie die Bereitstellungsanweisungsdatei, dargestellt durch`recipe`:

```
{
    "packageName": "sample-package-name",
    "versionName": "sample-package-version",
    ...
    "recipe": "{...}"
}
```

> **Note**
>
> Die Bereitstellungsanweisungsdatei, wie sie durch dargestellt wird, `recipe` kann aktualisiert werden, wenn sich eine Paketversion im `published` Statusstatus befindet, da sie von den Metadaten der Paketversion getrennt ist. Während der Arbeitsbereitstellung wird sie unveränderlich.

**`Artifact`**Versionsattribut

- Mithilfe des Versionsattributs `artifact` in Ihrer Softwarepaketversion können Sie den Amazon S3 S3-Speicherort für Ihre Paketversionsartefakte hinzufügen. Wenn eine Auftragsbereitstellung für Ihre Paketversion mithilfe von AWS IoT Jobs ausgelöst wird, wird der vorsignierte URL-Platzhalter `${aws:iot:package:<packageName>:version:<versionName>:artifact-location:s3-presigned-url}` im Jobdokument mithilfe des Amazon S3 S3-Buckets, des Bucket-Schlüssels und der Version der im Amazon S3 S3-Bucket gespeicherten Datei aktualisiert. Der Amazon S3 S3-Bucket, in dem die Paketversionsartefakte gespeichert sind, muss sich in derselben Region befinden, in der die Paketversion erstellt wurde.

> **Note**
>
> Um mehrere Objektversionen derselben Datei in Ihrem Amazon S3 S3-Bucket zu speichern, müssen Sie die Versionierung in Ihrem Bucket aktivieren. Weitere Informationen finden Sie unter Versionierung für Buckets aktivieren.

Um auf die Paketversionsartefakte im Amazon S3 S3-Bucket zuzugreifen, wenn Sie die Operation `CreatePackageVersion` oder `UpdatePackageVersion` API verwenden, benötigen Sie die folgenden Berechtigungen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetObjectVersion",
            "Resource": "arn:<partition>:s3:::<bucket>/<key>"
        }
    ]
}
```

Weitere Informationen zum Versionsattribut `artifact` in den Operationen `CreatePackageVersion` und `UpdatePackageVersion` API finden Sie unter CreatePackageVersionund UpdatePackageVersion.

Sehen Sie sich das folgende Beispiel an, das das Versionsattribut zeigt, das die Artefaktposition in Amazon S3 `artifact` unterstützt, wenn eine neue Paketversion erstellt wird:

```
{
    "packageName": "sample package name",
    "versionName": "1.0",
    "artifact": {
        "s3Location": {
            "bucket": "firmware",
            "key": "image.bin",
            "version": "12345"
        }
    }
```

```
}
```

> **Note**
>
> Wenn eine Paketversion von einem Statusstatus in einen `draft` Statusstatus aktualisiert wird, werden die Paketversionsattribute und der Speicherort der Artefakte unveränderlich. `published` Um diese Informationen zu aktualisieren, müssen Sie eine neue Paketversion erstellen und diese Aktualisierungen durchführen, während Sie sich im Statusstatus befinden. `draft`

Version Package

- In den verfügbaren Versionen des Softwarepakets kann eine Standardversion des Softwarepakets angegeben werden, die eine sichere und stabile Paketversion bietet. Dies dient als Basisversion des Softwarepakets, wenn Sie die Standardpaketversion mithilfe AWS IoT von Jobs für Ihre Geräteflotte bereitstellen. Beim Erstellen eines Auftrags zur Bereitstellung der `$default` Paketversion für ein Softwarepaket müssen die Paketversion im Auftragsdokument und in der neuen Auftragsbereitstellung mit übereinstimmen`$default`. Die Paketversion in der Jobbereitstellung wird durch API `destinationPackageVersions` - und CLI-Befehle und `VersionARN` in der dargestellt AWS Management Console. Die Paketversion im Jobdokument wird durch den folgenden Platzhalter für das Jobdokument dargestellt (siehe unten):

  ```
  arn:aws:iot:<regionCode>:111122223333:package/<packageName>/version/$default
  ```

  Um einen Job oder eine Jobvorlage mit der Standard-Paketversion zu erstellen, verwenden Sie das `$default` Flag im `CreateJobTemplate` API-Befehl `CreateJob` oder wie unten dargestellt:

  ```
  "$ aws iot create-job \
      --destination-package-versions "arn:aws:iot:us-west-2:123456789012:package/
  TestPackage/version/$default"
      --document file://jobdoc.json
  ```

> **Note**
>
> Das `$default` Paketversionsattribut, das auf die Standardversion verweist, ist ein optionales Attribut, das nur erforderlich ist, wenn über AWS IoT Jobs auf die Standardpaketversion für eine Auftragsbereitstellung verwiesen wird.

Wenn Sie mit der Paketversion zufrieden sind, veröffentlichen Sie sie entweder über die Seite mit den Softwarepaketdetails in der AWS IoT Konsole oder indem Sie den UpdatePackageVersionAPI-Vorgang ausführen. Sie können dann bei der Erstellung des Jobs entweder über die AWS IoT Konsole oder durch Ausführen des CreateJobAPI-Vorgangs auf die Paketversion verweisen.

## Benennen der Pakete und Versionen bei der Bereitstellung

Um eine Softwarepaketversion auf einem Gerät bereitzustellen, stellen Sie sicher, dass das Softwarepaket und die Paketversion, auf die im Jobdokument verwiesen wird, mit dem Softwarepaket und der Paketversion übereinstimmen, die im `destinationPackageVersions` Parameter des `CreateJob` API-Vorgangs angegeben sind. Wenn sie nicht übereinstimmen, erhalten Sie eine Fehlermeldung, in der Sie aufgefordert werden, beide Referenzen zuzuordnen. Weitere Informationen zu Fehlermeldungen im Softwarepaketkatalog finden Sie unterAllgemeine Fehlermeldungen zur Fehlerbehebung.

Zusätzlich zu den Softwarepaketen und Paketversionen, auf die im Jobdokument verwiesen wird, können Sie zusätzliche Softwarepakete und Paketversionen in den `destinationPackageVersions` Parameter des `CreateJob` API-Vorgangs aufnehmen, auf die im Jobdokument nicht verwiesen wird. Stellen Sie sicher, dass die erforderlichen Installationsinformationen im Jobdokument enthalten sind, damit die Geräte die zusätzlichen Softwarepaketversionen ordnungsgemäß installieren können. Weitere Informationen zur `CreateJob` API-Operation finden Sie unter CreateJob.

## Gezielte Jobsuche mithilfe AWS IoT dynamischer Dinggruppen

Der Softwarepaketkatalog arbeitet mit Flottenindizierung, AWS IoT Aufträgen und AWS IoT dynamischen Objektgruppen, um Geräte innerhalb Ihrer Flotte zu filtern und gezielt auszuwählen, um auszuwählen, welche Paketversion auf Ihren Geräten bereitgestellt werden soll. Sie können eine Flottenindizierungsabfrage auf der Grundlage der aktuellen Paketinformationen Ihres Geräts ausführen und diese Dinge gezielt für einen AWS IoT Job auswählen. Sie können auch

Softwareupdates veröffentlichen, jedoch nur für geeignete Zielgeräte. Sie können beispielsweise angeben, dass Sie eine Konfiguration nur für die Geräte bereitstellen möchten, auf denen derzeit die `iot-device-client 1.5.09` ausgeführt wird. Weitere Informationen finden Sie unter Erstellen einer dynamischen Objektgruppe.

## Reservierte benannte Schatten- und Paketversionen

Falls konfiguriert, können AWS IoT Jobs den reservierten Namen shadow (`$package`) einer Sache aktualisieren, wenn der Job erfolgreich abgeschlossen wurde. In diesem Fall müssen Sie dem reservierten benannten Schatten eines Objekts keine Paketversion manuell zuordnen.

In den folgenden Situationen können Sie sich dafür entscheiden, eine Paketversion manuell dem reservierten benannten Schatten des Objekts zuzuordnen oder zu aktualisieren:

- Sie registrieren eine Sache unter, AWS IoT Core ohne die installierte Paketversion zuzuordnen.
- AWS IoT Jobs ist nicht so konfiguriert, dass es den reservierten Namen Shadow des Dings aktualisiert.
- Sie verwenden ein internes Verfahren, um Paketversionen an Ihre Flotte zu versenden, und dieser Prozess wird nicht aktualisiert, AWS IoT Core wenn er abgeschlossen ist.

> **Note**
>
> Wir empfehlen Ihnen, AWS IoT Jobs zu verwenden, um die Paketversion im reservierten Shadow (`$package`) zu aktualisieren. Das Aktualisieren des Versionsparameters im `$package` Shadow durch andere Prozesse (z. B. manuelle oder programmatische API-Aufrufe), wenn AWS IoT Jobs ebenfalls für die Aktualisierung des Shadows konfiguriert ist, kann zu Inkonsistenzen zwischen der tatsächlichen Version auf dem Gerät und der Version führen, die an den reservierten benannten Shadow gemeldet wurde.

Sie können eine Paketversion zum reservierten Schatten (`$package`) eines Objekts über die Konsole oder den `UpdateThingShadow`-API-Vorgang hinzufügen oder aktualisieren. Weitere Informationen finden Sie unter Eine Paketversion einer Sache zuordnen. AWS IoT

> **Note**
>
> Durch das Zuordnen einer Paketversion zu einem AWS IoT Ding wird die Gerätesoftware nicht direkt aktualisiert. Sie müssen die Paketversion auf dem Gerät bereitstellen, um die Gerätesoftware zu aktualisieren.

### Deinstallation eines Softwarepakets und seiner Paketversion

`$null`ist ein reservierter Platzhalter, der den AWS IoT Jobs-Dienst auffordert, das vorhandene Softwarepaket und die Paketversion aus dem reservierten benannten Schatten des Geräts zu entfernen. `$package` Weitere Informationen finden Sie unter Reservierter benannter Schatten.

Um diese Funktion zu verwenden, ersetzen Sie den Versionsnamen am Ende des destinationPackageVersionAmazon-Ressourcennamens (ARN) durch`$null`. Anschließend müssen Sie Ihren Service anweisen, die Software vom Gerät zu entfernen.

Der autorisierte ARN verwendet das folgende Format:

```
arn:aws:iot:<regionCode>:111122223333:package/<packageName>/version/$null
```

Zum Beispiel

```
$ aws iot create-job \
    ... \
    --destinationPackageVersions ["arn:aws:iot:us-east-1:111122223333:package/
samplePackage/version/$null"]
```

## Erste Schritte mit dem Softwarepaket-Katalog

Sie können den AWS IoT Device Management Softwarepaketkatalog mithilfe der AWS Management Console AWS IoT Core API-Operationen und AWS Command Line Interface (AWS CLI) erstellen und verwalten.

> **Note**
>
> Die Aktivierung der AWS IoT Flottenindizierung ist eine Voraussetzung für die Verwendung des Softwarepaketkatalogs. Grundlegende Operationen wie das Erstellen einer Softwarepaketversion im AWS Management Console und das Verwenden des

`CreatePackage` API-Befehls schlagen fehl, wenn die AWS IoT Flottenindizierung nicht aktiviert ist.
Weitere Informationen zur Verwendung der AWS IoT Flottenindizierung mit dem Softwarepaketkatalog finden Sie unterVorbereitung der Flottenindizierung.

Verwenden der Konsole

Um den zu verwenden AWS Management Console, melden Sie sich in Ihrem AWS Konto an und navigieren Sie zu AWS IoT Core. Wählen Sie im Navigationsbereich Softwarepakete aus. In diesem Abschnitt können Sie dann Pakete und deren Versionen erstellen und verwalten.

Verwenden von API- oder CLI-Operationen

Sie können die AWS IoT Core API-Operationen verwenden, um Funktionen des Softwarepaketkatalogs zu erstellen und zu verwalten. Weitere Informationen finden Sie unter AWS IoT API-Referenz AWS SDKs und Toolkits. Mit den AWS CLI Befehlen wird auch Ihr Katalog verwaltet. Weitere Informationen finden Sie in der AWS IoT CLI Befehlsreferenz.

Dieses Kapitel enthält die folgenden Abschnitte:

- Ein Softwarepaket und eine Paketversion erstellen
- Bereitstellen einer Paketversion über Jobs AWS IoT
- Einer Sache eine Paketversion zuordnen AWS IoT

## Ein Softwarepaket und eine Paketversion erstellen

Sie können die folgenden Schritte verwenden, um ein Paket und eine erste Version über die AWS Management Console zu erstellen.

So erstellen Sie ein Softwarepaket

1. Loggen Sie sich in Ihr AWS Konto ein und navigieren Sie zur AWS IoT Konsole.
2. Wählen Sie im Navigationsbereich Softwarepakete aus.
3. Wählen Sie auf der Seite AWS IoT Softwarepaket die Option Paket erstellen aus. Das Dialogfeld Abhängigkeiten für die Paketverwaltung aktivieren wird angezeigt.
4. Wählen Sie unter Flottenindizierung die Option Gerätesoftwarepakete und Version hinzufügen aus. Dies ist für den Softwarepaket-Katalog erforderlich und bietet Flottenindizierung und Kennzahlen zu Ihrer Flotte.

5. [Optional] Wenn Sie möchten, dass AWS IoT Jobs den reservierten benannten Shadow aktualisieren, wenn Jobs erfolgreich abgeschlossen wurden, wählen Sie Shadows automatisch aus Jobs aktualisieren. Wenn Sie nicht möchten, dass AWS IoT Jobs diese Aktualisierung vornehmen, lassen Sie dieses Kontrollkästchen deaktiviert.
6. [Optional] Um AWS IoT Jobs die Rechte zur Aktualisierung des reservierten benannten Shadows zu gewähren, wählen Sie unter Rolle auswählen die Option Rolle erstellen aus. Wenn Sie nicht möchten, dass AWS IoT Jobs diese Aktualisierung vornehmen, ist diese Rolle nicht erforderlich.
7. Erstellen oder wählen Sie eine Rolle aus.

   a. Wenn Sie keine Rolle für diesen Zweck haben: Wenn das Dialogfeld Rolle erstellen angezeigt wird, geben Sie einen Rollennamen ein, und wählen Sie dann Erstellen aus.

   b. Falls Sie über eine Rolle für diesen Zweck verfügen: Wählen Sie unter Rolle auswählen Ihre Rolle aus und stellen Sie dann sicher, dass das Kontrollkästchen Richtlinie an IAM-Rolle anhängen aktiviert ist.
8. Wählen Sie Bestätigen aus. Die Seite Neues Paket erstellen wird angezeigt.
9. Geben Sie unter Paketdetails einen Paketnamen ein.
10. Geben Sie unter Paketbeschreibung Informationen ein, die Ihnen helfen, dieses Paket zu identifizieren und zu verwalten.
11. [Optional] Mit Tags können Sie dieses Paket besser kategorisieren und verwalten. Um Tags hinzuzufügen, erweitern Sie Tags, wählen Sie Tag hinzufügen und geben Sie ein Schlüssel-Wert-Paar ein. Sie können bis zu 50 Tags eingeben. Weitere Informationen finden Sie unter AWS IoT Ressourcen taggen.

Um beim Erstellen eines neuen Pakets eine Paketversion hinzuzufügen

1. Geben Sie unter Erste Version einen Versionsnamen ein.

   Wir empfehlen, das SemVer Format (z. B. `1.0.0.0`) zu verwenden, um Ihre Paketversion eindeutig zu identifizieren. Sie können auch eine andere Formatierungsstrategie verwenden, die besser zu Ihrem Anwendungsfall passt. Weitere Informationen finden Sie unter Lebenszyklus der Paketversion.
2. Geben Sie unter Versionsbeschreibung Informationen ein, anhand derer Sie diese Paketversion identifizieren und verwalten können.

> **Note**
>
> Das Kontrollkästchen Standardversion ist deaktiviert, da Paketversionen in einem bestimmten `draft` Status erstellt werden. Sie können der Standardversion einen Namen geben, nachdem Sie die Paketversion erstellt haben und wenn Sie den Status in ändern`published`. Weitere Informationen finden Sie unter Lebenszyklus der Paketversion.

3. [Optional] Um Ihnen bei der Verwaltung dieser Version zu helfen oder Informationen an Ihre Geräte zu übermitteln, geben Sie ein oder mehrere Name-Wert-Paare für Versionsattribute ein. Wählen Sie für jedes Name-Wert-Paar, das Sie eingeben, die Option Attribut hinzufügen aus. Weitere Informationen finden Sie unter Versionsattribute.
4. [Optional] Mit Tags können Sie dieses Paket besser kategorisieren und verwalten. Um Tags hinzuzufügen, erweitern Sie Tags, wählen Sie Tag hinzufügen und geben Sie ein Schlüssel-Wert-Paar ein. Sie können bis zu 50 Tags eingeben. Weitere Informationen finden Sie unter AWS IoT Ressourcen taggen.
5. Wählen Sie Weiter aus.

Ordnen Sie die Softwareliste einer Paketversion zu (optional)

1. Wählen Sie unter Schritt 3: Version SBOMs (optional) im Fenster SBOM-Konfigurationen das Standard-SBOM-Dateiformat und den Validierungsmodus aus, mit denen Ihre Softwareliste validiert wird, bevor sie Ihrer Paketversion zugeordnet wird.
2. Geben Sie im Fenster SBOM-Datei hinzufügen den Amazon-Ressourcennamen (ARN) für Ihren versionierten Amazon S3-Bucket und das bevorzugte SBOM-Dateiformat ein, falls der Standardtyp nicht funktioniert.

> **Note**
>
> Sie können entweder eine einzelne SBOM-Datei oder eine einzelne ZIP-Datei mit mehreren Dateien hinzufügen, SBOMs wenn Sie mehr als eine Softwareliste für Ihre Paketversion haben.

3. Im Fenster Hinzugefügte SBOM-Datei können Sie die SBOM-Datei anzeigen, die Sie für Ihre Paketversion hinzugefügt haben.

4. Wählen Sie Paket und Version erstellen aus. Die Seite mit der Paketversion wird angezeigt, und Sie können den Validierungsstatus Ihrer SBOM-Datei im Fenster „SBOM-Datei hinzugefügt“ sehen. Der Anfangsstatus lautet, dass die `In progress` SBOM-Datei validiert wird.

> **Note**
>
> Der Validierungsstatus der SBOM-Datei ist`Invalid file`,,,, `Not startedIn progress`, `Validated (SPDX)` und die Gründe für den Fehler bei der Überprüfung. `Validated (CycloneDX)`

## Bereitstellen einer Paketversion über Jobs AWS IoT

Sie können die folgenden Schritte ausführen, um eine Paketversion über den AWS Management Console bereitzustellen.

Voraussetzungen:

Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- AWS IoT Dinge registrieren bei AWS IoT Core. Anweisungen zum Hinzufügen Ihrer Geräte finden Sie AWS IoT Core unter Ein Ding-Objekt erstellen.
- [Optional] Erstellen Sie eine AWS IoT Dinggruppe oder dynamische Dinggruppe für die Geräte, für die Sie die Paketversion bereitstellen werden. Anweisungen zum Erstellen einer Objektgruppe finden Sie unter Erstellen einer statischen Objektgruppe. Anweisungen zum Erstellen einer dynamischen Objektgruppe finden Sie unter Erstellen einer dynamischen Objektgruppe.
- Erstellen Sie ein Softwarepaket und eine Paketversion. Weitere Informationen finden Sie unter Ein Softwarepaket und eine Paketversion erstellen.
- Erstellen eines Auftragsdokuments. Weitere Informationen finden Sie unter Vorbereiten des Auftragsdokuments und der Paketversion für die Bereitstellung.

Um einen AWS IoT Job bereitzustellen

1. Wählen Sie auf der AWS IoT Konsole Softwarepakete aus.
2. Wählen Sie das Softwarepaket aus, das Sie bereitstellen möchten. Die Seite mit den Details zum Softwarepaket wird angezeigt.

3. Wählen Sie unter Versionen die Paketversion aus, die Sie bereitstellen möchten, und wählen Sie dann Auftragsversion bereitstellen aus.
4. Wenn Sie zum ersten Mal einen Auftrag über dieses Portal bereitstellen, wird ein Dialogfeld mit einer Beschreibung der Anforderungen angezeigt. Prüfen Sie die Informationen und wählen Sie Bestätigen aus.
5. Geben Sie einen Namen für die Bereitstellung ein, oder lassen Sie den automatisch generierten Namen im Feld Name stehen.
6. [Optional] Geben Sie im Feld Beschreibung eine Beschreibung ein, die den Zweck oder den Inhalt der Bereitstellung identifiziert, oder lassen Sie die automatisch generierten Informationen übrig.

   Hinweis: Wir empfehlen, dass Sie in den Feldern Auftragsname und Beschreibung keine personenbezogenen Daten verwenden.
7. [Optional] Fügen Sie alle Tags hinzu, die mit diesem Auftrag verknüpft werden sollen.
8. Wählen Sie Weiter aus.
9. Wählen Sie unter Auftragsziele die Objekte oder Objektgruppen aus, die den Auftrag erhalten sollen.
10. Geben Sie im Feld Auftragsdatei die JSON-Datei des Auftragsdokuments an.
11. Öffnen Sie Auftragsintegration mit dem Paketkatalogdienst.
12. Wählen Sie die Pakete und Versionen aus, die in Ihrem Auftragsdokument angegeben sind.

    > **Note**
    >
    > Sie müssen dieselben Pakete und Paketversionen auswählen, die im Auftragsdokument angegeben sind. Sie können mehr hinzufügen, aber der Auftrag gibt Anweisungen nur für die Pakete und Versionen aus, die im Auftragsdokument enthalten sind. Weitere Informationen finden Sie unter Benennen der Pakete und Versionen bei der Bereitstellung.
13. Wählen Sie Weiter aus.
14. Wählen Sie auf der Seite Auftragskonfiguration im Dialogfeld Auftragskonfiguration einen der folgenden Auftragstypen aus:

    - Snapshot-Auftrag: Ein Snapshot-Auftrag ist abgeschlossen, wenn er abgeschlossen ist. Er wird auf den Zielgeräten und -gruppen ausgeführt.

- Kontinuierlicher Auftrag: Ein kontinuierlicher Auftrag gilt für Objektgruppen und wird auf jedem Gerät ausgeführt, das Sie später zu einer bestimmten Zielgruppe hinzufügen.

15. Überprüfen Sie im Dialogfeld Zusätzliche Konfigurationen — optional die folgenden optionalen Auftragskonfigurationen und treffen Sie Ihre Auswahl entsprechend. Weitere Informationen finden Sie unter Konfigurationen für Auftrags-Rollout, Planung und Abbruch sowie Konfigurationen für Timeout und Wiederholungsversuche bei der Auftragsausführung.

    - Konfiguration des Rollouts
    - Konfiguration des Zeitplans
    - Konfiguration des Timeouts für Auftragsausführungen
    - Auftragsausführungen: Konfiguration wiederholen
    - Abbruch der Konfiguration

16. Überprüfen Sie die Auftragsauswahl und klicken Sie dann auf Absenden.

Nachdem Sie den Auftrag erstellt haben, generiert die Konsole eine JSON-Signatur und setzt sie in Ihr Auftragsdokument. Sie können die AWS IoT Konsole verwenden, um den Status eines Jobs anzuzeigen oder einen Job abzubrechen oder zu löschen. Gehen Sie zum Auftrags-Hub der Konsole, um Aufträge zu verwalten.

## Einer Sache eine Paketversion zuordnen AWS IoT

Nachdem Sie Software auf Ihrem Gerät installiert haben, können Sie dem reservierten Shadow einer AWS IoT Sache eine Paketversion zuordnen. Wenn AWS IoT Jobs so konfiguriert wurden, dass der reservierte Named Shadow des Dings aktualisiert wird, nachdem der Job bereitgestellt und erfolgreich abgeschlossen wurde, müssen Sie dieses Verfahren nicht abschließen. Weitere Informationen finden Sie unter Reservierter benannter Schatten.

Voraussetzungen:

Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- Erstellen Sie ein oder AWS IoT mehrere Dinge und richten Sie die Telemetrie mithilfe von ein. AWS IoT Core Weitere Informationen finden Sie unter Erste Schritte mit AWS IoT Core.
- Erstellen Sie ein Softwarepaket und eine Paketversion. Weitere Informationen finden Sie unter Ein Softwarepaket und eine Paketversion erstellen.
- Installieren Sie die Software der Paketversion auf dem Gerät.

> **Note**
>
> Durch das Zuordnen einer Paketversion zu AWS IoT einem Objekt wird keine Software auf dem physischen Gerät aktualisiert oder installiert. Die Paketversion muss auf dem Gerät bereitgestellt werden.

Um einer Sache eine Paketversion zuzuordnen AWS IoT

1. Erweitern Sie im Navigationsbereich der AWS IoT -Konsole das Menü Alle Geräte und wählen Sie Objekte aus.
2. Identifizieren Sie das AWS IoT Ding, das Sie aktualisieren möchten, aus der Liste und wählen Sie den Namen des Dings aus, um die zugehörige Detailseite anzuzeigen.
3. Wählen Sie im Abschnitt Details die Option Pakete und Versionen aus.
4. Wählen Sie Zu Paket und Version hinzufügen.
5. Wählen Sie unter Gerätepaket auswählen das gewünschte Softwarepaket aus.
6. Wählen Sie unter Version auswählen die gewünschte Softwareversion aus.
7. Wählen Sie Gerätepaket hinzufügen.

   Das Paket und die Version werden in der Liste Ausgewählte Pakete und Versionen angezeigt.
8. Wiederholen Sie diese Schritte für jedes Paket und jede Version, die Sie diesem Objekt zuordnen möchten.
9. Wenn Sie fertig sind, wählen Sie Paket- und Versionsdetails hinzufügen. Die Seite mit den Objektdetails wird geöffnet, und Sie können das neue Paket und die neue Version in der Liste sehen.

# AWS IoT Jobs

Verwenden Sie AWS IoT Jobs, um eine Reihe von Fernvorgängen zu definieren, die an ein oder mehrere verbundene Geräte gesendet und auf diesen ausgeführt werden können AWS IoT. Sie können beispielsweise einen Auftrag definieren, der eine Reihe von Geräten anweist, Anwendungen herunterzuladen und zu installieren, Firmware-Updates auszuführen, einen Neustart vorzunehmen, die Zertifikate zu rotieren oder Remote-Fehlerbehebungsvorgänge auszuführen.

## Auf AWS IoT Jobs zugreifen

Sie können mit AWS IoT Jobs beginnen, indem Sie die Konsole oder die AWS IoT Core API verwenden.

Verwenden der Konsole

Melden Sie sich bei der AWS Management Console an und wechseln Sie zur AWS IoT Konsole. Wählen Sie im Navigationsbereich Manage (Verwalten) und dann Jobs (Aufträge) aus. In diesem Bereich können Sie Aufträge erstellen und verwalten. Wenn Sie Auftragsvorlagen erstellen und verwalten möchten, wählen Sie im Navigationsbereich die Option Auftragsvorlagen aus. Weitere Informationen finden Sie unter Erstellen und Verwalten von Aufträgen mithilfe von AWS Management Console.

Verwenden der API oder CLI

Sie können beginnen, indem Sie die AWS IoT Core API-Operationen verwenden. Weitere Informationen finden Sie unter AWS IoT -API-Referenz. Die AWS IoT Core API, auf der AWS IoT Jobs basiert, wird vom AWS SDK unterstützt. Weitere Informationen finden Sie unter AWS SDKs und Toolkits.

Sie können die AWS CLI zum Ausführen von Befehlen zum Erstellen und Verwalten von Aufträgen und Auftragsvorlagen verwenden. Weitere Informationen finden Sie in der AWS IoT CLI-Referenz.

## AWS IoT Jobs, Regionen und Endpunkte

AWS IoT Jobs unterstützt API-Endpunkte der Steuerungsebene und der Datenebene, die für Sie spezifisch sind. AWS-Region Die API-Endpunkte der Datenebene sind spezifisch für Sie AWS-Konto und. AWS-RegionWeitere Informationen zu den AWS IoT Jobs-Endpunkten finden Sie unter AWS IoT Device Management — Job-Datenendpunkte in der AWS Allgemeinen Referenz.

# Was ist eine Fernsteuerung?

Ein Fernvorgang ist jede Aktualisierung oder Aktion, die Sie auf einem physischen Gerät, virtuellen Gerät oder Endpunkt ausführen können und die remote ausgeführt werden können, ohne dass die physische Anwesenheit eines Bedieners oder Technikers erforderlich ist. Die Fernsteuerung erfolgt mithilfe eines over-the-air (OTA-) Updates, sodass Ihre Geräte nicht physisch anwesend sein müssen. Die Verwaltung Ihrer Geräteflotte in AWS Cloud ermöglicht es Ihnen, Fernoperationen an Ihren Geräten durchzuführen, wenn diese registriert sind AWS IoT Core.

AWS IoT Device Management Jobs bietet einen skalierbaren Ansatz für die Durchführung von Fernaktionen auf Ihren Geräten, bei denen Sie registriert sind AWS IoT Core. Ein Job wird im erstellt AWS Cloud und mithilfe eines OTA-Updates über das MQTT- oder HTTP-Protokoll an alle Zielgeräte gesendet.

AWS IoT Device Management Jobs bieten Ihnen die Möglichkeit, Fernoperationen wie Zurücksetzen auf Werkseinstellungen, Geräteneustarts und Software-OTA-Updates auf sichere, skalierbare und kostengünstigere Weise durchzuführen.

Weitere Informationen zu finden Sie unter AWS IoT Core. Was ist AWS IoT?

Weitere Informationen zu AWS IoT Device Management Jobs finden Sie unter Was ist AWS IoT Jobs?.

## Vorteile der Verwendung von AWS IoT Device Management Jobs für Remote-Operationen

Wenn Sie AWS IoT Device Management Jobs für Ihre Fernoperationen verwenden, wird die Verwaltung Ihrer Geräteflotte optimiert. In der folgenden Liste sind einige der wichtigsten Vorteile aufgeführt, die sich aus der Verwendung von AWS IoT Device Management Jobs für die Ausführung Ihrer Fernoperationen ergeben:

- Nahtlose Integration mit anderen AWS-Services
  - AWS IoT Device Management Jobs ist eng mit den folgenden Mehrwerten AWS-Services und Funktionen integriert:
    - Amazon S3: Speichern Sie Ihre Anweisungen zur Remote-Steuerung in einem sicheren Amazon S3-Bucket, in dem Sie die Zugriffsberechtigungen für diese Inhalte kontrollieren. Die Verwendung eines Amazon S3 S3-Buckets bietet eine skalierbare und langlebige Speicherlösung, die nativ in den AWS IoT Device Management Software Package Catalog integriert ist, sodass AWS IoT Device Management Jobs in Aktualisierungsanweisungen

referenzieren und diese ersetzen können. Weitere Informationen finden Sie unter Was ist Amazon S3?.

- Amazon CloudWatch: Überwachen und protokollieren Sie den Status der Implementierung des Remote-Betriebs der Auftragsausführung für jedes Gerät sowie andere Geräteaktivitäten, um die gesamte Auftragsleistung unter AWS IoT Device Management Jobs zu verfolgen und zu analysieren. Weitere Informationen finden Sie unter Was ist Amazon CloudWatch? Überwachung von Auftragsprotokollen und Erfassung historischer Daten zur Fehlerbehebung. So funktioniert es mit Aufträgen.
- AWS-IoT-Device-Shadow-Service: Mithilfe von AWS IoT Device Management Jobs können Sie über einen AWS IoT Geräteshadow eine digitale Darstellung Ihres Geräts verwalten, sodass der Status Ihres Geräts unabhängig von der Gerätekonnektivität für Anwendungen und andere Dienste verfügbar ist. Weitere Informationen finden Sie unter AWS-IoT-Device-Shadow-Service.
- Fleet Hub für AWS IoT Geräteverwaltung: Erstellen Sie eigenständige Webanwendungen zur Überwachung des Zustands Ihrer Geräteflotte. Weitere Informationen finden Sie unter Was ist Fleet Hub for AWS IoT Device Management? .

- Bewährte Methoden für die Gewährleistung der Sicherheit
  - Berechtigungskontrolle: Steuern Sie die Zugriffsberechtigungen für Ihre Fernbedienungsanweisungen mithilfe von Amazon S3 und legen Sie mithilfe von AWS IoT Richtlinien und IAM-Benutzerrollen fest, welche IAM-Benutzer Ihre Fernbedienungsanweisungen für Ihre Geräteflotte bereitstellen können.
    - Weitere Informationen zu AWS IoT Richtlinien finden Sie unter. Erstellen Sie eine AWS IoT Richtlinie
    - Weitere Informationen zu IAM-Benutzerrollen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT.
- Skalierbarkeit
  - Gezielte Auftragsbereitstellung: Steuern Sie, welche Geräte das Auftragsdokument eines Auftrags mit einer gezielten Auftragsverteilung erhalten, indem Sie bei der Erstellung des Auftrags bestimmte Kriterien für die Gerätegruppierung in Ihrem Auftragsdokument eingeben. Wenn Sie für jedes Gerät AWS IoT etwas erstellen und diese Informationen in der AWS IoT Registrierung speichern, können Sie mithilfe der Flottenindizierung gezielte Suchen durchführen. Sie können auf der Grundlage der Suchergebnisse zur Flottenindizierung benutzerdefinierte Gruppen erstellen, um die Bereitstellung Ihres Zielauftrags zu unterstützen. Weitere Informationen finden Sie unter Geräte verwalten mit AWS IoT. Verwenden Sie Aufträge, um Snapshot-Aufträge im Vergleich zu kontinuierlichen Aufträgen auszuführen.

  - Auftragsstatus: Verfolgen Sie den Status des Rollouts des Auftragsdokuments für Ihre Geräteflotte und den gesamten Auftragsstatus auf Geräteflottenebene sowie den individuellen Implementierungsstatus des Auftragsdokuments auf jedem Gerät. Weitere Informationen finden Sie unter Aufträge und Status der Auftragsausführung.
  - Skalierbarkeit neuer Geräte: Stellen Sie Ihr Auftragsdokument ganz einfach auf einem neuen Gerät bereit, indem Sie es einer vorhandenen, benutzerdefinierten Gruppe hinzufügen, die mithilfe der Flottenindizierung über einen kontinuierlichen Auftrag erstellt wurde. Dadurch sparen Sie Zeit, anstatt das Auftragsdokument auf jedem neuen Gerät separat bereitstellen zu müssen. Oder Sie können einen gezielteren Ansatz mit einem Snapshot verwenden, indem Sie ein Auftragsdokument einmal für eine vorher festgelegte Gruppe von Geräten bereitstellen und der Job dann abgeschlossen ist.
- Flexibilität
  - Auftragskonfigurationen: Passen Sie Ihren Auftrag und Ihr Auftragsdokument mit den optionalen Auftragskonfigurationen Rollout, Terminplanung, Abbruch, Timeout und Wiederholung an Ihre spezifischen Anforderungen an. Weitere Informationen finden Sie unter Auftrags--Konfigurationen.
- Kosteneffektiv
  - Führen Sie eine effizientere Kostenstruktur für die Wartung Ihrer Geräteflotte ein, indem Sie AWS IoT Device Management Jobs nutzen, um wichtige Updates bereitzustellen und routinemäßige Wartungsaufgaben durchzuführen. Eine do-it-yourself (DIY-) Lösung zur Wartung Ihrer Geräteflotte beinhaltet wiederkehrende, variable Kosten wie die Infrastruktur, die zum Hosten und Verwalten der DIY-Lösung erforderlich ist, die Arbeitskosten für die Entwicklung, Wartung und Skalierung der DIY-Lösung sowie die Kosten für die Datenübertragung. Dank der transparenten, festen Kostenstruktur von AWS IoT Device Management Jobs wissen Sie genau, was jede Auftragsausführung für ein Gerät kosten wird, zusätzlich zu den Datenübertragungskosten, die erforderlich sind, um die Bereitstellung der Auftragsdokumente für Ihre Geräteflotte zu erleichtern und den Status der Auftragsausführung für jedes Gerät zu verfolgen. Weitere Informationen finden Sie unter AWS IoT Core Preise.

# Was ist AWS IoT Jobs?

Verwenden Sie AWS IoT Jobs, um eine Reihe von Remote-Vorgängen zu definieren, die an ein oder mehrere verbundene Geräte gesendet und auf diesen ausgeführt werden können AWS IoT.

Um Aufträge zu erstellen, definieren Sie zunächst ein Auftragsdokument, das eine Liste von Anweisungen enthält, in denen die Operationen beschrieben werden, die das Gerät aus der Ferne ausführen muss. Um diese Operationen auszuführen, geben Sie eine Liste von Zielen an, bei denen es sich um einzelne Objekte, Objektgruppen oder beides handelt. Das Arbeitsdokument und die Ziele bilden zusammen eine Bereitstellung.

Jede Bereitstellung kann zusätzliche Konfigurationen haben:

- Rollout: Definiert, wie viele Geräte das Auftragsdokument pro Minute erhalten.
- Abbrechen: Wenn eine bestimmte Anzahl von Geräten die Auftragsbenachrichtigung nicht erhält, verwenden Sie diese Konfiguration, um den Auftrag abzubrechen. Dadurch wird vermieden, dass ein fehlerhaftes Update an eine ganze Flotte gesendet wird.
- Timeout: Wenn innerhalb eines bestimmten Zeitraums keine Antwort von Ihren Auftragszielen eingeht, kann der Auftrag fehlschlagen. Sie können den Auftrag verfolgen, der auf diesen Geräten ausgeführt wird.
- Erneut versuchen: Wenn ein Gerät einen Fehler meldet oder das Zeitlimit für einen Job überschritten wird, können Sie AWS IoT Jobs verwenden, um das Auftragsdokument automatisch erneut an das Gerät zu senden.
- Planung: Mit dieser Konfiguration können Sie einen Auftrag für ein zukünftiges Datum und eine zukünftige Uhrzeit planen. Sie können damit auch wiederkehrende Wartungsfenster einrichten, in denen Geräte während vordefinierter Zeiträume mit geringem Datenverkehr aktualisiert werden.

AWS IoT Jobs sendet eine Nachricht, um die Ziele darüber zu informieren, dass ein Job verfügbar ist. Das Ziel startet die Ausführung des Jobs, indem es das Jobdokument herunterlädt, die darin angegebenen Operationen ausführt und den Status des Jobs meldet AWS IoT. Sie können den Fortschritt eines Jobs für ein bestimmtes Ziel oder für alle Ziele verfolgen, indem Sie Befehle ausführen, die von AWS IoT Jobs bereitgestellt werden. Wenn ein Auftrag gestartet wird, hat er den Status In Bearbeitung. Die Geräte melden dann inkrementelle Aktualisierungen und zeigen diesen Status an, bis der Auftrag erfolgreich ist, fehlschlägt oder das Zeitlimit überschritten wird.

In den folgenden Themen werden einige wichtige Konzepte von Aufträgen und der Lebenszyklus von Aufträgen und Auftragsausführungen beschrieben.

Themen

- Wichtige Konzepte von Jobs
- Aufträge und Status der Auftragsausführung

# Wichtige Konzepte von Jobs

Die folgenden Konzepte enthalten Einzelheiten zu AWS IoT Aufträgen und zur Erstellung und Bereitstellung von Aufträgen zur Ausführung von Fernoperationen auf Ihren Geräten.

## Grundkonzepte

Im Folgenden finden Sie grundlegende Konzepte, die Sie kennen müssen, wenn Sie AWS IoT Jobs verwenden.

Job

Ein Auftrag ist eine Remote-Operation, die an ein oder mehrere mit AWS IoT verbundene Geräte gesendet und dort ausgeführt werden. Sie können beispielsweise einen Auftrag definieren, der eine Reihe von Geräten anweist, eine Anwendung herunterzuladen und zu installieren oder Firmware-Updates auszuführen, einen Neustart vorzunehmen, die Zertifikate zu rotieren oder Remote-Fehlerbehebungsvorgänge auszuführen.

Auftragsdokument

Um einen Auftrag zu erstellen, müssen Sie zunächst ein Auftragsdokument erstellen, das ist eine Beschreibung der Remote-Operationen, die von den Geräten ausgeführt werden sollen.

Auftragsdokumente sind UTF-8-kodierte JSON-Dokumente, die die Informationen enthalten, die Ihr Gerät für die Ausführung eines Auftrags benötigt. Ein Jobdokument enthält ein oder mehrere Dokumente, aus URLs denen das Gerät ein Update oder andere Daten herunterladen kann. Das Auftragsdokument kann in einem Amazon S3-Bucket gespeichert sein oder inline in dem Befehl enthalten sein, der den Auftrag erstellt.

> **Note**
>
> In MQTT-Antworten ist das `jobDocument` Feld ein JSON-Objekt. In HTTP-Antworten ist es eine Zeichenkettendarstellung des JSON-Objekts.

Ziel

Beim Anlegen eines Auftrags geben Sie eine Liste von Zielen an, nämlich die Geräte, die die Operationen ausführen sollen. Bei den Zielen kann es sich um Objekte und/oder Objektgruppen

handeln. Der AWS IoT Jobs-Service sendet eine Nachricht an jedes Ziel, um es darüber zu informieren, dass ein Job verfügbar ist.

Bereitstellung

Nachdem Sie einen Auftrag erstellt haben, indem Sie das Auftragsdokument bereitgestellt und Ihre Zielliste angegeben haben, wird das Auftragsdokument dann auf den Remote-Zielgeräten bereitgestellt, für die Sie das Update durchführen möchten. Bei Snapshot-Aufträgen wird der Auftrag nach der Bereitstellung auf den Zielgeräten abgeschlossen. Bei kontinuierlichen Aufträgen wird ein Auftrag für eine Gruppe von Geräten bereitgestellt, sobald diese den Gruppen hinzugefügt werden.

Auftragsausführung

Eine Auftragsausführung ist eine Instance eines Auftrags auf einem Zielgerät. Das Ziel startet eine Ausführung eines Auftrags durch Herunterladen des Auftragsdokuments. Anschließend führt er die im Dokument angegebenen Operationen aus und meldet den Fortschritt an AWS IoT. Eine Ausführungsnummer ist eine eindeutige Kennung einer Auftragsausführung auf einem bestimmten Ziel. Der AWS IoT Jobs-Service stellt Befehle bereit, mit denen Sie den Fortschritt der Ausführung eines Jobs auf einem Ziel und den Fortschritt eines Jobs auf allen Zielen verfolgen können.

## Auftragstypen, Konzepte

Die folgenden Konzepte sollen Ihnen helfen, mehr über die verschiedenen Arten von Jobs zu erfahren, die Sie mit AWS IoT Jobs erstellen können.

Snapshot-Auftrag

Standardmäßig wird ein Auftrag an alle Ziele gesendet, die Sie bei der Erstellung des Auftrags angeben. Wenn diese Ziele den Auftrag abgeschlossen haben (oder melden, dass sie dazu nicht in der Lage sind), ist der Auftrag abgeschlossen.

Kontinuierlicher Auftrag

Kontinuierliche Aufträge werden an alle Ziele gesendet, die Sie bei der Erstellung des Auftrags angeben. Er weiter ausgeführt und an alle neuen Geräten (Objekte) gesendet, die der Zielgruppe hinzugefügt werden. Beispiel: Ein kontinuierlicher Auftrag kann zum Onboarding und zur Aktualisierung von Geräten, die einer Gruppe hinzugefügt werden, verwendet werden. Sie können einen Auftrag kontinuierlich machen, indem Sie bei der Erstellung des Auftrags einen optionalen Parameter setzen.

> **Note**
>
> Wenn Sie Ihre IoT-Flotte mit dynamischen Objektgruppen ins Visier nehmen, empfehlen wir, kontinuierliche Aufträge anstelle von Snapshot-Aufträgen zu verwenden. Durch die Verwendung kontinuierlicher Aufträge erhalten Geräte, die der Gruppe beitreten, die Auftragsausführung auch dann, wenn der Auftrag erstellt wurde.

### Vorsigniert URLs

Für einen sicheren, zeitlich begrenzten Zugriff auf Daten, die nicht im Auftragsdokument enthalten sind, können Sie vorsignierte Amazon S3 verwenden. URLs Platzieren Sie Ihre Daten in einen Amazon S3-Bucket und fügen einen Platzhalterlink zu den Daten in dem Auftragsdokument hinzu. Wenn AWS IoT Jobs eine Anfrage für das Jobdokument erhält, analysiert es das Jobdokument, indem es nach den Platzhalter-Links sucht, und ersetzt dann die Links durch vorsignierte Amazon S3. URLs

Der Platzhalterlink hat das folgende Format:

```
${aws:iot:s3-presigned-url:https://s3.amazonaws.com/bucket/key}
```

wo *`bucket`* ist Ihr Bucket-Name und *`key`* ist das Objekt im Bucket, auf das Sie verlinken.

In den Regionen Peking und Ningxia URLs funktioniert Presigned nur, wenn der Eigentümer der Ressource über eine ICP-Lizenz (Internet Content Provider) verfügt. Weitere Informationen finden Sie unter Amazon Simple Storage Service in der Dokumentation Erste Schritte mit AWS Services in China.

### Auftragskonfigurationskonzepte

Die folgenden Konzepte können Ihnen helfen, die Konfiguration von Aufträgen zu verstehen.

Rollouts

Sie können angeben, wie schnell die Ziele über eine ausstehende Auftragsausführung benachrichtigt werden. Auf diese Weise können Sie einen schrittweisen Rollout erstellen, um Updates, Neustarts und andere Operationen besser zu verwalten. Sie können eine Rolloutkonfiguration erstellen, indem Sie entweder eine statische Rollout-Rate oder eine exponentielle Rollout-Rate verwenden. Verwenden Sie eine statische Rollout-Rate, um die maximale Anzahl von Auftragszielen festzulegen, die pro Minute informiert werden sollen.

Beispiele für die Festlegung von Rollout-Raten und weitere Informationen zur Konfiguration von Auftrags-Rollouts finden Sie unter. Konfigurationen für Auftrags-Rollout, Planung und Abbruch

Planung

Auftragsplanung ermöglicht es Ihnen, den Rollout-Zeitraum eines Auftragsdokuments auf allen Geräten der Zielgruppe für kontinuierliche Aufträge und Snapshot-Aufträge zu planen. Darüber hinaus können Sie ein optionales Wartungsfenster einrichten, das bestimmte Daten und Uhrzeiten enthält, zu denen das Auftragsdokument im Rahmen eines Auftrags auf allen Geräten in der Zielgruppe bereitgestellt wird. Ein Wartungsfenster ist eine wiederkehrende Instance mit einer Häufigkeit von täglichen, wöchentlichen, monatlichen oder benutzerdefinierten Daten und Uhrzeiten, die bei der ersten Erstellung des Auftrags oder der Auftragsvorlage ausgewählt wurden. Nur fortlaufende Aufträge können so geplant werden, dass sie während eines Wartungsfensters einen Rollout durchführen.

Die Planung von Aufträgen ist spezifisch für Ihren Auftrag. Einzelne Auftragsausführungen können nicht geplant werden. Weitere Informationen finden Sie unter Konfigurationen für Auftrags-Rollout, Planung und Abbruch.

Abbrechen

Sie können eine Reihe von Bedingungen für den Abbruch von Rollouts erstellen, wenn bestimmte von Ihnen angegebenen Kriterien erfüllt sind. Weitere Informationen finden Sie unter Konfigurationen für Auftrags-Rollout, Planung und Abbruch.

Timeouts

Auftrags-Timeouts benachrichtigen Sie, wenn eine Auftragsbereitstellung für eine unerwartet lange Zeit im Status `IN_PROGRESS` stecken bleibt. Es gibt zwei Arten von Timern: Timer für „In Bearbeitung“ und Timer für „Schritt“. Wenn der Auftrag `IN_PROGRESS` ist, können Sie den Fortschritt Ihrer Auftragsbereitstellung überwachen und verfolgen.

Rollouts und Abbruchkonfigurationen sind spezifisch für Ihren Auftrag, wohingegen die Timeout-Konfiguration spezifisch für eine Auftragsbereitstellung ist. Weitere Informationen finden Sie unter Timeout bei der Auftragsausführung und Wiederholungskonfigurationen.

Wiederholversuche

Auftragswiederholungen ermöglichen es, die Auftragsausführung erneut zu versuchen, wenn ein Auftrag fehlschlägt, eine Zeitüberschreitung eintritt oder beides auftritt. Sie können über bis zu 10 Wiederholungsversuche für die Auftragsausführung verfügen. Sie können den Fortschritt Ihres Wiederholungsversuchs überwachen und verfolgen, ob die Auftragsausführung erfolgreich war.

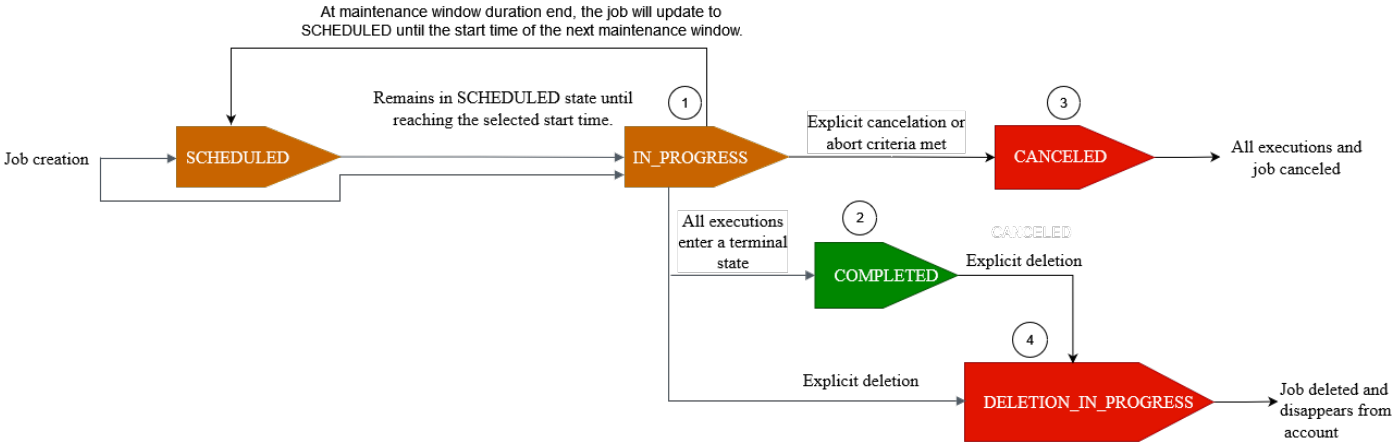
Rollouts und Abbruchkonfigurationen sind spezifisch für Ihren Auftrag, während die Timeout- und Wiederholungs-Konfigurationen spezifisch für eine Auftragsausführung sind. Weitere Informationen finden Sie unter Timeout bei der Auftragsausführung und Wiederholungskonfigurationen.

## Aufträge und Status der Auftragsausführung

In den folgenden Abschnitten werden der Lebenszyklus eines AWS IoT Auftrags und der Lebenszyklus einer Auftragsausführung beschrieben.

### Auftragsstatus

Das folgende Diagramm zeigt die verschiedenen Status eines AWS IoT Jobs.




Ein Job, den Sie mit AWS IoT Jobs erstellen, kann sich in einem der folgenden Status befinden:

- GEPLANT

  Bei der ersten Erstellung eines Jobs oder einer Jobvorlage mithilfe der AWS IoT Konsole, CreateJobCreateJobTemplateAPI oder API können Sie die optionale Planungskonfiguration in der AWS IoT Konsole oder `SchedulingConfig` in der CreateJobAPI oder CreateJobTemplateAPI auswählen. Wenn Sie einen geplanten Auftrag starten, der ein bestimmtes `startTime`, `endTime` und `endBehavior` erhält, wird der Auftragsstatus aktualisiert auf `SCHEDULED`. Wenn der Auftrag das von Ihnen gewählte `startTime` oder `startTime` des nächsten Wartungsfensters erreicht (falls Sie den Auftrags-Rollout während eines Wartungsfensters ausgewählt haben), wird der Status von `SCHEDULED` zu `IN_PROGRESS` aktualisiert und mit dem Rollout des Auftragsdokuments auf allen Geräten in der Zielgruppe begonnen.
- IN_PROGRESS

Wenn Sie einen Job mithilfe der AWS IoT Konsole oder der CreateJobAPI erstellen, wird der Jobstatus auf aktualisiertIN_PROGRESS. Während der Auftragserstellung beginnt AWS IoT Jobs mit der Bereitstellung von Auftragsausführungen auf den Geräten Ihrer Zielgruppe. Nachdem alle Auftragsausführungen eingeführt wurden, wartet AWS IoT Jobs darauf, dass die Geräte die Remote-Aktion abgeschlossen haben.

Informationen zur Parallelität und zu den Beschränkungen, die für laufende Aufträge gelten, finden Sie unter AWS IoT Grenzwerte für Jobs.

> **Note**
>
> Wenn ein IN_PROGRESS-Auftrag das Ende des aktuellen Wartungsfensters erreicht, wird der Rollout des Auftragsdokuments beendet. Der Auftrag wird SCHEDULED bis zum startTime nächsten Wartungsfenster aktualisiert.

- COMPLETED

  Ein kontinuierlicher Auftrag wird auf eine der folgenden Arten behandelt:

  - Bei einem kontinuierlichen Auftrag, bei dem die optionale Planungskonfiguration nicht ausgewählt wurde, ist er immer in Bearbeitung und wird für alle neuen Geräte, die der Zielgruppe hinzugefügt werden, weiterhin ausgeführt. Es wird niemals den Status COMPLETED erreichen.
  - Für einen kontinuierlichen Auftrag mit der ausgewählten optionalen Planungskonfiguration gilt Folgendes:
    - Wenn ein endTime angegeben wurde, erreicht ein kontinuierlicher Auftrag den Status COMPLETED, wenn er endTime bestanden hat und alle Auftragsausführungen den Terminal-Zustand erreicht haben.
    - Wenn in der optionalen Planungskonfiguration kein bereitgestellt *endTime* wurde, führt der fortlaufende Auftrag weiterhin den Rollout des Auftragsdokuments durch.

  Bei einem Snapshot-Auftrag ändert sich der Auftragsstatus in den COMPLETED-Zustand, in dem alle zugehörigen Auftragsausführungen in einen Terminal-Zustand übergehen, z. B. SUCCEEDED, FAILED, TIMED_OUT, REMOVED oder CANCELED.

- CANCELED

  Wenn Sie einen Job mithilfe der AWS IoT Konsole, der CancelJobAPI oder der stornierenKonfiguration des Auftragsabbruchs, ändert sich der Jobstatus aufCANCELED. Während der Auftragsstornierung beginnt AWS IoT Jobs, zuvor erstellte Jobausführungen abzubrechen.

Informationen zur Gleichzeitigkeit und zu den Grenzen, die für abgebrochene Aufträge gelten, finden Sie unter AWS IoT Grenzwerte für Jobs.

- DELETION_IN_PROGRESS

  Wenn Sie einen Job mithilfe der AWS IoT Konsole oder der DeleteJobAPI löschen, ändert sich der Jobstatus in. `DELETION_IN_PROGRESS` Beim Löschen von AWS IoT Jobs beginnt Jobs mit dem Löschen zuvor erstellter Jobausführungen. Nachdem alle Jobausführungen gelöscht wurden, verschwindet der Job aus Ihrem AWS Konto.

## Auftragsausführungsstatus

Die folgende Tabelle zeigt die verschiedenen Status einer AWS IoT Jobausführung und ob die Statusänderung vom Gerät oder von AWS IoT Jobs initiiert wird.

Status und Quelle der Auftragsausführung

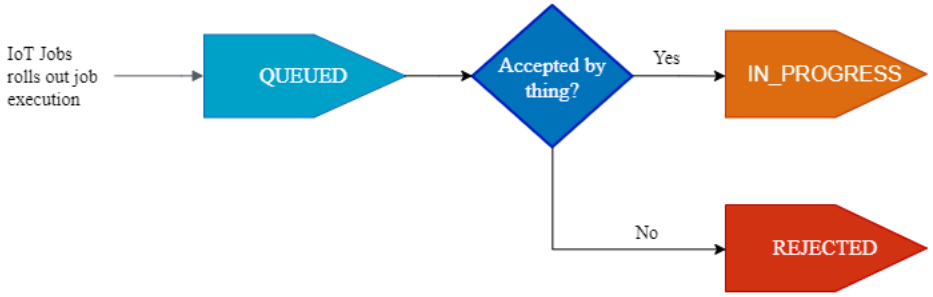
| Auftrags-Ausführungsstatus | Vom Gerät initiiert? | Von AWS IoT Jobs initiiert? | Terminal-Status? | Kann erneut versucht werden? |
|---|---|---|---|---|
| `QUEUED` | Nein | Ja | Nein | Nicht zutreffend |
| `IN_PROGRESS` | Ja | Nein | Nein | Nicht zutreffend |
| `SUCCEEDED` | Ja | Nein | Ja | Nicht zutreffend |
| `FAILED` | Ja | Nein | Ja | Ja |
| `TIMED_OUT` | Nein | Ja | Ja | Ja |
| `REJECTED` | Ja | Nein | Ja | Nein |
| `REMOVED` | Nein | Ja | Ja | Nein |
| `CANCELED` | Nein | Ja | Ja | Nein |

Im folgenden Abschnitt werden die Status einer Jobausführung näher beschrieben, die eingeführt wird, wenn Sie einen Job mit AWS IoT Jobs erstellen.

- IN WARTESCHLANGE

Wenn AWS IoT Jobs eine Jobausführung für ein Zielgerät einführt, wird der Status der Auftragsausführung auf gesetztQUEUED. Die Auftragsausführung bleibt so lange im Status QUEUED, bis:

- Ihr Gerät empfängt die Auftragsausführung und ruft die Jobs API-Operationen auf und meldet den Status als IN_PROGRESS.
- Sie brechen den Auftrag oder die Auftragsausführung ab, oder wenn die von Ihnen angegebenen Abbruchkriterien erfüllt sind und der Status sich auf CANCELED ändert.
- Ihr Gerät wird aus der Zielgruppe entfernt und der Status ändert sich auf REMOVED.




- IN_PROGRESS

  Wenn Ihr IoT-Gerät den reservierten Auftragsthemen $notify und $notify-next abonniert und Ihr Gerät entweder die StartNextPendingJobExecution API oder die UpdateJobExecution API mit dem Status von aufruftIN_PROGRESS, setzt AWS IoT Jobs den Status der Auftragsausführung auf. IN_PROGRESS

  Die UpdateJobExecution-API kann mehrfach mit dem Status IN_PROGRESS aufgerufen werden. Sie können mithilfe des statusDetails-Objekts zusätzliche Details zu den Ausführungsschritten angeben.

  > **Note**
  >
  > Wenn Sie für jedes Gerät mehrere Jobs erstellen, garantieren AWS IoT Jobs und das MQTT-Protokoll nicht die Reihenfolge der Lieferung.

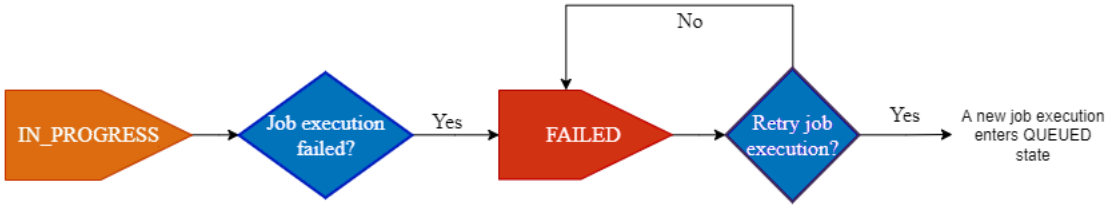
- SUCCEEDED

  Wenn Ihr Gerät den Fernvorgang erfolgreich abgeschlossen hat, muss das Gerät die UpdateJobExecution API mit dem Status von aufrufen, SUCCEEDED um anzuzeigen, dass die

Auftragsausführung erfolgreich war. AWS IoT Jobs wird dann aktualisiert und gibt den Status der Auftragsausführung als `SUCCEEDED` zurück.

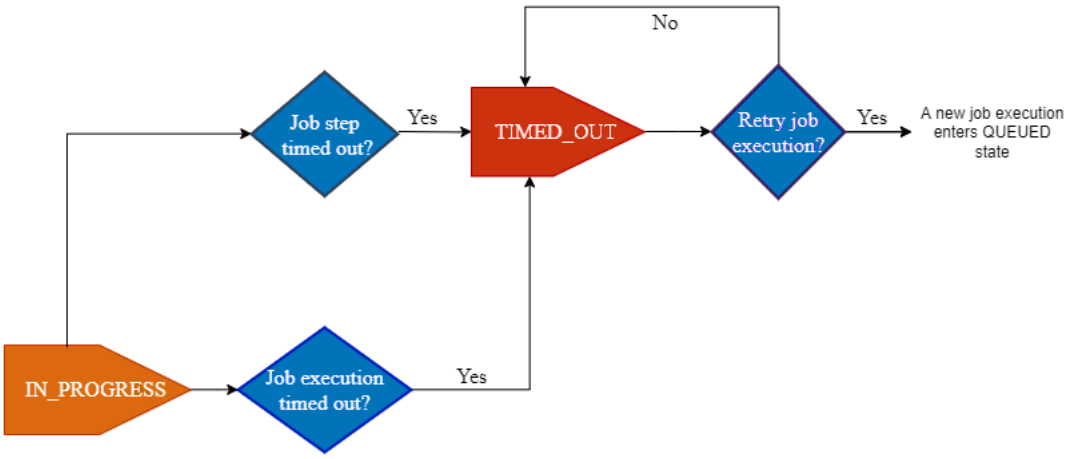
- FEHLGESCHLAGEN

  Wenn Ihr Gerät den Fernvorgang nicht abschließen kann, muss das Gerät die `UpdateJobExecution` API mit dem Status aufrufen, `Failed` um anzuzeigen, dass die Auftragsausführung fehlgeschlagen ist. AWS IoT Jobs wird dann aktualisiert und gibt den Status der Auftragsausführung als `Failed` zurück. Sie können versuchen, diese Auftragsausführung für das Gerät mittels des Auftragsausführung: Konfiguration wiederholen erneut auszuführen.




- TIMED_OUT

  Wenn Ihr Gerät einen Auftragsschritt nicht abschließt, obwohl der Status lautet`IN_PROGRESS`, oder wenn es den Fernvorgang nicht innerhalb der Timeout-Dauer des in Bearbeitung befindlichen Timers abschließt, setzt AWS IoT Jobs den Status der Auftragsausführung auf. `TIMED_OUT` Sie haben außerdem einen Schrittzeitgeber für jeden Auftragsschritt eines laufenden Auftrags, der nur für die Auftragsausführung gilt. Die Dauer des in Bearbeitung befindlichen Timers wird mithilfe der `inProgressTimeoutInMinutes`-Eigenschaft von Timeout-Konfiguration für die Auftragsausführung angegeben. Sie können versuchen, diese Auftragsausführung für das Gerät mittels des Auftragsausführung: Konfiguration wiederholen erneut auszuführen.




- ABGELEHNT

  Wenn Ihr Gerät eine ungültige oder inkompatible Anfrage erhält, muss das Gerät die `UpdateJobExecution` API mit dem Status aufrufen. `REJECTED` AWS IoT Jobs wird dann aktualisiert und gibt den Status der Auftragsausführung als `REJECTED` zurück.

- ENTFERNT

  Wenn Ihr Gerät kein gültiges Ziel für die Auftragsausführung mehr ist, z. B. wenn es von einer dynamischen Objektgruppe getrennt ist, setzt AWS IoT Jobs den Status der Auftragsausführung auf `REMOVED`. Sie können das Objekt wieder an Ihre Zielgruppe anhängen und die Auftragsausführung für das Gerät neu starten.

- CANCELED

  Wenn Sie einen Job oder eine Auftragsausführung mithilfe der Konsole oder der `CancelJobExecution` API abbrechen `CancelJob` oder wenn die mit dem angegebenen Abbruchkriterien erfüllt sind, bricht AWS IoT Jobs den Konfiguration des Auftragsabbruchs Job ab und setzt den Status der Jobausführung auf. `CANCELED`

# Verwalten von Aufträgen

Verwenden Sie Aufträge, um Geräte über ein Software- oder Firmware-Update zu informieren. Sie können die AWS IoT Konsole, dieAPI-Operationen zur Auftragsverwaltung und -steuerung, die oder die verwenden AWS Command Line Interface, um Jobs AWS SDKszu erstellen und zu verwalten.

## Codesignatur für Aufgaben

Wenn Sie Code an Geräte senden, damit Geräte erkennen können, ob der Code während der Übertragung geändert wurde, empfehlen wir, die Codedatei mit dem AWS CLI zu signieren. Anweisungen finden Sie unter Erstellen und Verwalten von Aufträgen mithilfe von AWS CLI.

Weitere Informationen finden Sie unter Wozu dient Codesignatur AWS IoT? .

## Auftragsdokument

Bevor Sie einen Auftrag erstellen, müssen Sie ein Auftragsdokument erstellen. Wenn Sie Code Signing für verwenden AWS IoT, müssen Sie Ihr Auftragsdokument in einen versionierten Amazon S3 S3-Bucket hochladen. Weitere Informationen zum Erstellen eines Amazon S3-Buckets und zum Hochladen von Dateien in diesen Bucket finden Sie unter Erste Schritte mit Amazon Simple Storage Service im Amazon S3 Einführungshandbuch.

> **Tip**
>
> Beispiele für Jobdokumente finden Sie im Beispiel jobs-agent.js im AWS IoT SDK für JavaScript.

## Vorsigniert URLs

Ihr Auftragsdokument kann eine vorsignierte Amazon S3-URL enthalten, die auf Ihre Code-Datei (oder eine andere Datei) verweist. Vorsignierte Amazon S3 URLs sind nur für einen begrenzten Zeitraum gültig und werden generiert, wenn ein Gerät ein Auftragsdokument anfordert. Da die vorsignierte URL nicht erstellt wird, wenn Sie das Auftragsdokument erstellen, setzen Sie stattdessen eine Platzhalter-URL in Ihr Auftragsdokument. Eine Platzhalter-URL sieht wie folgt aus:

```
${aws:iot:s3-presigned-url-v2:https://
s3.region.amazonaws.com/<bucket>/<code file>}
```

Wobei:

- *bucket*ist der Amazon S3 S3-Bucket, der die Codedatei enthält.
- *code file*ist der Amazon S3 S3-Schlüssel der Codedatei.

Wenn ein Gerät das Jobdokument anfordert, AWS IoT generiert es die vorsignierte URL und ersetzt die Platzhalter-URL durch die vorsignierte URL. Ihr Auftragsdokument wird dann an das Gerät gesendet.

IAM-Rolle zur Erteilung der Erlaubnis für den Download von Dateien von S3

Wenn Sie einen Job erstellen, der vorsigniertes Amazon S3 verwendet URLs, müssen Sie eine IAM-Rolle angeben. Die Rolle muss die Berechtigung zum Herunterladen von Dateien aus dem Amazon S3-Bucket gewähren, in dem die Daten oder Updates gespeichert sind. Die Rolle muss auch die Berechtigung für AWS IoT zur Übernahme der Rolle gewähren.

Sie können optional ein Timeout für die vorsignierte URL angeben. Weitere Informationen finden Sie unter CreateJob.

Erteilen Sie AWS IoT Jobs die Erlaubnis, Ihre Rolle anzunehmen

1. Gehen Sie zum Rollen-Hub der IAM-Konsole und wählen Sie Ihre Rolle.
2. Wählen Sie auf der Registerkarte Vertrauensbeziehungen die Option Vertrauensstellung bearbeiten aus und ersetzen Sie das Richtliniendokument durch das folgende JSON-Dokument. Wählen Sie Update Trust Policy (Trust Policy aktualisieren).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "iot.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. Verwenden Sie die globalen Konditionsschlüssel `aws:SourceArn` und `aws:SourceAccount` für die Richtlinie, um vor dem Confused-Deputy-Problem zu schützen.

> **Important**
>
> Ihr `aws:SourceArn` muss das Format einhalten: `arn:aws:iot:`*`region`*`:`*`account-id`*`:*`. Vergewissern Sie sich, dass dies *`region`* mit Ihrer AWS IoT Region und Ihrer Kundenkonto-ID *`account-id`* übereinstimmt. Weitere Informationen finden Sie unter Vermeidung des dienstübergreifenden Confused-Deputy-Problems.

```
{
  "Effect": "Allow",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service":
          "iot.amazonaws.com"
       },
      "Action": "sts:AssumeRole",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "123456789012"
         },
         "ArnLike": {
              "aws:SourceArn": "arn:aws:iot:*:123456789012:job/*"
         }
       }
     }
   ]
}
```

4. Wenn Ihr Auftrag ein Auftragsdokument verwendet, das ein Amazon S3-Objekt ist, wählen Sie Berechtigungen und verwenden Sie das folgende JSON. Dadurch wird eine Richtlinie hinzugefügt, die das Herunterladen von Dateien aus Ihrem Amazon S3-Bucket gestattet:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
```

```
            "Resource": "arn:aws:s3:::your_S3_bucket/*"
        }
    ]
}
```

## Vorsignierte URL für den Datei-Upload

Wenn Ihre Geräte während einer Auftragsbereitstellung Dateien in einen Amazon S3 S3-Bucket hochladen müssen, können Sie den folgenden vorsignierten URL-Platzhalter in Ihr Jobdokument aufnehmen:

```
${aws:iot:s3-presigned-url-upload:https://s3.region.amazonaws.com/<bucket>/<key>}
```

Sie können maximal zwei von jedem von `${thingName}${jobId}`, und `${executionNumber}` als reservierte Schlüsselwörter innerhalb des `key` Attributs in der Platzhalter-URL für den Datei-Upload verwenden, die sich in Ihrem Jobdokument befindet. Der lokale Platzhalter, der diese reservierten Schlüsselwörter im `key` Attribut darstellt, wird analysiert und ersetzt, wenn die Jobausführung erstellt wird. Durch die Verwendung eines lokalen Platzhalters mit reservierten Schlüsselwörtern für jedes Gerät wird sichergestellt, dass jede hochgeladene Datei von einem Gerät spezifisch für dieses Gerät ist und nicht durch eine ähnliche hochgeladene Datei von einem anderen Gerät überschrieben wird, auf das dieselbe Auftragsbereitstellung abzielt. Informationen zur Fehlerbehebung bei lokalen Platzhaltern innerhalb eines vordefinierten URL-Platzhalters für das Hochladen von Dateien während einer Auftragsbereitstellung finden Sie unter. Allgemeine Fehlermeldungen zur Fehlerbehebung

> **Note**
>
> Der Amazon S3 S3-Bucket-Name darf nicht den lokalen Platzhalter enthalten, der die reservierten Schlüsselwörter für die hochgeladene Datei darstellt. Der lokale Platzhalter muss sich im Attribut befinden. `key`

Dieser vorsignierte URL-Platzhalter wird in Ihrem Auftragsdokument in eine vorsignierte Amazon S3 S3-Upload-URL umgewandelt, wenn ein Gerät ihn empfängt. Ihre Geräte verwenden dies, um Dateien in einen Amazon S3 S3-Ziel-Bucket hochzuladen.

> **Note**
>
> Wenn der Amazon S3 S3-Bucket und der Schlüssel nicht in der obigen Platzhalter-URL bereitgestellt werden, generiert AWS IoT Jobs automatisch einen Schlüssel für jedes Gerät, wobei maximal zwei von jeweils `${thingName}${jobId}`, und `${executionNumber}` verwendet werden.

## Vorsignierte URL mit Amazon S3 S3-Versionierung

Der Schutz der Integrität einer Datei, die in einem Amazon S3 S3-Bucket gespeichert ist, ist entscheidend für die Gewährleistung sicherer Auftragsbereitstellungen unter Verwendung dieser Datei für Ihre Geräteflotte. Mithilfe der Amazon S3 S3-Versionierung können Sie für jede Variante der in Ihrem Amazon S3 S3-Bucket gespeicherten Datei eine Versions-ID hinzufügen, um jede Version der Datei zu verfolgen. Dies gibt Aufschluss darüber, welche Version der Datei mithilfe AWS IoT von Jobs für Ihre Geräteflotte bereitgestellt wird. Weitere Informationen zu Amazon S3 S3-Buckets, die Versionierung verwenden, finden Sie unter Verwenden der Versionierung in Amazon S3 S3-Buckets.

Wenn die Datei in Amazon S3 gespeichert ist und das Jobdokument einen vorsignierten URL-Platzhalter enthält, generiert AWS IoT Jobs eine vorsignierte URL im Jobdokument unter Verwendung des Amazon S3 S3-Buckets, des Bucket-Schlüssels und der Version der im Amazon S3 S3-Bucket gespeicherten Datei. Diese im Jobdokument generierte vorsignierte URL ersetzt den vorsignierten URL-Platzhalter, der ursprünglich im Jobdokument enthalten war. Wenn Sie die in Ihrem Amazon S3 S3-Bucket gespeicherte Datei aktualisieren, `versionId` wird eine neue Version der Datei und weitere Versionen erstellt, um die vorgenommenen Aktualisierungen zu signalisieren und die Möglichkeit zu bieten, diese spezifische Datei bei future Auftragsbereitstellungen als Ziel zu verwenden.

In den folgenden Beispielen finden Sie eine Vorher- und Nachbetrachtung des Amazon S3, das URLs in Ihrem Auftragsdokument vorsigniert wurde, mit dem`versionId`:

Platzhalter für vorsignierte Amazon S3 S3-URLs (vor der Auftragsbereitstellung)

```
//Virtual-hosted style URL
${aws:iot:s3-presigned-url-v2:https://bucket-name.s3.region-code.amazonaws.com/key-name%3FversionId%3Dversion-id}

//Path-style URL
```

```
${aws:iot:s3-presigned-url-v2:https://s3.region-code.amazonaws.com/bucket-name/key-name%3FversionId%3Dversion-id}
```

Vorsignierte Amazon S3 S3-URL (während der Auftragsbereitstellung)

```
//Virtual-hosted style URL
${aws:iot:s3-presigned-url-v2:https://sample-bucket-name.s3.us-west-2.amazonaws.com/sample-code-file.png%3FversionId%3Dversion1}

//Path-style
${aws:iot:s3-presigned-url-v2:https://s3.us-west-2.amazonaws.com/sample-bucket-name/sample-code-file.png%3FversionId%3Dversion1}
```

Weitere Informationen zu virtuell gehosteten Objekten und URLs Pfadobjekten in Amazon S3 finden Sie unter Virtual-hosted-style Anfragen und Anfragen im Path-Stil.

> **Note**
>
> Wenn Sie an eine vorsignierte Amazon S3 S3-URL anhängen `versionId` möchten, muss sie der URL-Codierungsunterstützung entsprechen. AWS SDK for Java 2.x Weitere Informationen finden Sie unter Änderungen beim Parsen von Amazon S3 URIs von Version 1 zu Version 2.

Versionsunterschiede für vorsignierte URL-Platzhalter in Amazon S3

In der folgenden Liste werden die Unterschiede zwischen den vorsignierten URL-Platzhaltern von Amazon S3 `${aws:iot:s3-presigned-url-v1` (Version 1) und `${aws:iot:s3-presigned-url-v2` (Version 2) beschrieben:

- Der vorsignierte URL-Platzhalter von Amazon S3 `${aws:iot:s3-presigned-url-v1` wird nicht unterstützt. `version-id`
- Der vorsignierte Amazon S3 S3-Platzhalter `${aws:iot:s3-presigned-url-v1` empfängt die Amazon S3 S3-URL unverschlüsselt. Für den Platzhalter Amazon S3 Presigned URL `${aws:iot:s3-presigned-url-v2` muss die Amazon S3 S3-URL so codiert sein, dass sie dem Amazon S3 S3-SDK-Standard entspricht.

Themen

- Erstellen und Verwalten von Aufträgen mithilfe von AWS Management Console
- Erstellen und verwalten Sie Jobs mit dem AWS CLI

# Erstellen und Verwalten von Aufträgen mithilfe von AWS Management Console

In diesem Abschnitt wird beschrieben, wie Sie Jobs von der Konsole aus erstellen und verwalten können. AWS IoT Nachdem Sie einen Job erstellt haben, können Sie Informationen zu dem Job auf der Detailseite anzeigen und den Job verwalten.

> **Note**
>
> Wenn Sie Codesignaturen für AWS IoT Jobs durchführen möchten, verwenden Sie den AWS CLI. Weitere Informationen finden Sie unter Erstellen und Verwalten von Aufträgen mithilfe von AWS CLI.

Themen

- Erstellen und verwalten Sie Jobs mit dem AWS Management Console
- Sie können Jobs anzeigen und verwalten, indem Sie AWS Management Console

## Erstellen und verwalten Sie Jobs mit dem AWS Management Console

Um einen Job zu erstellen, melden Sie sich bei der AWS IoT Konsole an und wechseln Sie im Bereich Remote Actions zum Hub Jobs. Führen Sie dann die folgenden Schritte aus.

1. Wählen Sie auf der Seite Jobs im Dialogfeld Jobs die Option Job erstellen aus.
2. Je nachdem, welches Gerät Sie verwenden, können Sie einen benutzerdefinierten Job, einen FreeRTOS OTA-Aktualisierungsjob oder einen AWS IoT Greengrass Job erstellen. Wählen Sie für dieses Beispiel Einen benutzerdefinierten Auftragerstellen aus. Wählen Sie Weiter aus.
3. Geben Sie auf der Seite Benutzerdefinierte Auftragseigenschaften im Dialogfeld Auftragseigenschaften Ihre Informationen für die folgenden Felder ein:
   - Name: Geben Sie einen eindeutigen, alphanumerischen Auftragsnamen ein.
   - Beschreibung – optional: Geben Sie optional eine Beschreibung Ihres Auftrags ein.

- Markierungen – optional:

> **Note**
>
> Wir empfehlen, dass Sie in Ihrem Job IDs und Ihrer Beschreibung keine personenbezogenen Daten verwenden.

Wählen Sie Weiter aus.

4. Wählen Sie auf der Seite Dateikonfiguration im Dialogfeld Auftragsziele die Objekte oder Objektgruppen aus, für die Sie diesen Auftrag ausführen möchten.

   Wählen Sie im Dialogfeld Auftragsdokument eine der folgenden Optionen aus:

   - Aus Datei: Eine JSON-Auftragsdatei, die Sie zuvor in einen Amazon S3-Bucket hochgeladen haben
     - Codesignatur

       In dem Auftragsdokument, das sich in Ihrer Amazon S3-URL befindet, ist `${aws:iot:code-sign-signature:s3://region.bucket/code-file@code-file-version-id}` als Platzhalter erforderlich, bis er mithilfe Ihres Codesignaturprofils durch den Pfad der signierten Codedatei ersetzt wird. Die neue signierte Codedatei wird zunächst in einem `SignedImages`-Ordner in Ihrem Amazon S3-Quell-Bucket angezeigt. Es wird ein neues Auftragsdokument mit einem `Codesigned_`-Präfix erstellt, wobei der Pfad der signierten Codedatei den Platzhalter für das Codezeichen ersetzt und in Ihre Amazon S3-URL eingefügt wird, um einen neuen Auftrag zu erstellen.

     - Ressource vor der Unterzeichnung URLs

       Wählen Sie in der Dropdownliste „Rolle vor dem Signieren“ die IAM-Rolle aus, die Sie in Presigned erstellt haben. URLs Die Verwendung `${aws:iot:s3-presigned-url:` der Vorsignierung URLs für Objekte, die sich in Amazon S3 befinden, ist eine bewährte Sicherheitsmethode für Geräte, die Objekte von Amazon S3 herunterladen.

       Wenn Sie den Platzhalter presigned URLs für Codesignaturen verwenden möchten, verwenden Sie die folgende Beispielvorlage:

       ```
       ${aws:iot:s3-presigned-url:${aws:iot:code-sign-signature:<S3 URL>}
       ```

- Aus Vorlage: Eine Auftragsvorlage, die ein Auftragsdokument und Auftragskonfigurationen enthält. Bei der Auftragsvorlage kann es sich um eine von Ihnen erstellte benutzerdefinierte Auftragsvorlage oder um eine AWS verwaltete Vorlage handeln.

  Wenn Sie einen Job für die Durchführung häufig verwendeter Remote-Aktionen wie den Neustart Ihres Geräts erstellen, können Sie eine AWS verwaltete Vorlage verwenden. Diese Vorlagen wurden bereits für die Verwendung vorkonfiguriert. Weitere Informationen erhalten Sie unter Erstellen einer benutzerdefinierten Auftragsvorlage und Erstellen Sie benutzerdefinierte Jobvorlagen aus verwalteten Vorlagen.

5. Wählen Sie auf der Seite Auftragskonfiguration im Dialogfeld Auftragskonfiguration einen der folgenden Auftragstypen aus:

   - Snapshot-Auftrag: Ein Snapshot-Auftrag ist abgeschlossen, wenn er abgeschlossen ist. Er wird auf den Zielgeräten und -gruppen ausgeführt.
   - Kontinuierlicher Auftrag: Ein kontinuierlicher Auftrag gilt für Objektgruppen und wird auf jedem Gerät ausgeführt, das Sie später zu einer bestimmten Zielgruppe hinzufügen.

6. Überprüfen Sie im Dialogfeld Zusätzliche Konfigurationen – optional die folgenden optionalen Auftragskonfigurationen und treffen Sie Ihre Auswahl entsprechend.

   - Rollout-Konfiguration
   - Konfiguration des Zeitplans
   - Konfiguration des Timeouts für Auftragsausführungen
   - Auftragsausführungen: Konfiguration wiederholen – neu
   - Konfiguration abbrechen

   In den folgenden Abschnitten finden Sie weitere Informationen zu Auftragskonfigurationen:

   - Konfigurationen für Auftrags-Rollout, Planung und Abbruch
   - Timeout bei der Auftragsausführung und Wiederholungskonfigurationen

   Überprüfen Sie alle Ihre Auftragsauswahlen und wählen Sie dann Absenden, um Ihren Auftrag zu erstellen.

### Sie können Jobs anzeigen und verwalten, indem Sie AWS Management Console

Nachdem Sie den Auftrag erstellt haben, generiert die Konsole eine JSON-Signatur und setzt sie in Ihr Auftragsdokument. Sie können die AWS IoT -Konsole verwenden, um den Status anzuzeigen, oder um einen Auftrag abzubrechen oder zu löschen.

Wenn Sie den Job auswählen, den Sie erstellt haben, finden Sie:

- Allgemeine Jobdetails, wie Jobname, Beschreibung, Typ, Zeitpunkt der Erstellung, letzte Aktualisierung und geschätzte Startzeit.
- Alle von Ihnen angegebenen Auftragskonfigurationen und deren Status.
- Das Auftragsdokument.
- Die Auftragsausführungen und alle optionalen Tags, die Sie angegeben haben.

Um Jobs zu verwalten, gehen Sie zum Job Hub der Konsole und wählen Sie aus, ob Sie den Job bearbeiten, löschen oder stornieren möchten.

## Erstellen und verwalten Sie Jobs mit dem AWS CLI

In diesem Abschnitt wird beschrieben, wie Sie Aufträge erstellen und verwalten.

### Erstellen von Aufträgen

Verwenden Sie den CreateJob Befehl, um einen AWS IoT Job zu erstellen. Der Auftrag wird in die Warteschlange für die Ausführung auf den Zielen (Objekten oder Objektgruppen) gesetzt, die Sie angeben. Um einen AWS IoT Job zu erstellen, benötigen Sie ein Jobdokument, das in den Hauptteil der Anfrage oder als Link zu einem Amazon S3 S3-Dokument aufgenommen werden kann. Wenn der Job das Herunterladen von Dateien mit vorsigniertem Amazon S3 beinhaltet URLs, benötigen Sie eine IAM-Rolle mit Amazon Resource Name (ARN), die über die Berechtigung zum Herunterladen der Datei verfügt und dem AWS IoT Jobs-Service die Erlaubnis erteilt, die Rolle zu übernehmen.

Weitere Informationen zur Syntax bei der Eingabe von Datum und Uhrzeit mithilfe eines API-Befehls oder des finden Sie unter AWS CLI Timestamp.

#### Codesignatur mit Aufträgen

Wenn Sie Codesignatur für verwenden AWS IoT, müssen Sie einen Codesignaturauftrag starten und die Ausgabe in Ihr Jobdokument aufnehmen. Dadurch wird der Platzhalter für die

Codezeichensignatur in Ihrem Auftragsdokument ersetzt, der als Platzhalter erforderlich ist, bis er mithilfe Ihres Codesignaturprofils durch den Pfad der signierten Codedatei ersetzt wird. Der Platzhalter für die Codesignatur sieht wie folgt aus:

```
    ${aws:iot:code-sign-signature:s3://region.bucket/code-file@code-file-version-id}
```

Verwenden Sie den start-signing-jobBefehl, um einen Codesignaturauftrag zu erstellen. `start-signing-job`gibt eine Job-ID zurück. Verwenden Sie den Befehl describe-signing-job, um den Amazon S3-Ort abzurufen, an dem die Signatur gespeichert ist. Anschließend können Sie die Signatur von Amazon S3 herunterladen. Weitere Informationen zu Codesignaturaufträgen finden Sie unter Codesignatur für AWS IoT.

Ihr Auftragsdokument muss einen vorsignierten URL Platzhalter für Ihre Code-Datei haben, und die JSON-Signaturausgabe muss in einem Amazon S3-Bucket unter Verwendung des start-signing-job-Befehls platziert sein:

```
{
    "presign": "${aws:iot:s3-presigned-url:https://s3.region.amazonaws.com/bucket/
image}",
}
```

Erstellen eines Auftrags mit einem Auftragsdokument

Der folgende Befehl zeigt, wie Sie einen Job mithilfe eines in einem Amazon S3-Bucket (*job-document.json*) gespeicherten Auftragsdokuments (*jobBucket*) und einer Rolle mit der Berechtigung zum Herunterladen von Dateien von Amazon S3 (*S3DownloadRole*) erstellen.

```
aws iot create-job  \
      --job-id 010  \
      --targets arn:aws:iot:us-east-1:123456789012:thing/thingOne  \
      --document-source https://s3.amazonaws.com/amzn-s3-demo-bucket/job-document.json
 \
      --timeout-config inProgressTimeoutInMinutes=100 \
      --job-executions-rollout-config "{ \"exponentialRate\": { \"baseRatePerMinute
\": 50, \"incrementFactor\": 2, \"rateIncreaseCriteria\": { \"numberOfNotifiedThings
\": 1000, \"numberOfSucceededThings\": 1000}}, \"maximumPerMinute\": 1000}" \
      --abort-config "{ \"criteriaList\": [ { \"action\": \"CANCEL\", \"failureType
\": \"FAILED\", \"minNumberOfExecutedThings\": 100, \"thresholdPercentage\": 20},
 { \"action\": \"CANCEL\", \"failureType\": \"TIMED_OUT\", \"minNumberOfExecutedThings
\": 200, \"thresholdPercentage\": 50}]}" \
```

```
      --presigned-url-config "{\"roleArn\":\"arn:aws:iam::123456789012:role/
S3DownloadRole\", \"expiresInSec\":3600}"
```

Der Job wird ausgeführt am*thingOne*.

Der optionale `timeout-config`-Parameter gibt die Dauer an, die jedes Gerät für den Abschluss der Ausführung des Auftrags hat. Der Timer wird gestartet, wenn der Status der Auftragsausführung auf `IN_PROGRESS` gesetzt wird. Wird der Status der Auftragsausführung vor Ablauf der Zeit nicht auf einen anderen Terminal-Zustand festgelegt, wird er automatisch auf `TIMED_OUT` festgelegt.

Der Timer für „In Bearbeitung“ kann nicht aktualisiert werden und gilt für alle Auftragsausführungen für den Auftrag. Immer wenn eine Auftragsausführung länger als dieses Intervall im `IN_PROGRESS` Status verbleibt, schlägt sie fehl und wechselt in den `TIMED_OUT` Terminalstatus. AWS IoT veröffentlicht auch eine MQTT-Benachrichtigung.

Weitere Informationen zum Konfigurieren von Auftragsrollouts und -abbrüchen finden Sie unter Auftragsrollout- und Abbruchkonfiguration.

> **Note**
>
> Auftragsdokumente, die als Amazon S3-Dateien angegeben werden, werden zum Zeitpunkt der Erstellung des Auftrags abgerufen. Wenn Sie den Inhalt der Amazon S3-Datei, die Sie als Quelle Ihres Auftragsdokuments verwendet haben, ändern, nachdem Sie das Auftragsdokument erstellt haben, ändert sich das, was an die Auftragsziele gesendet wird, nicht.

## Aktualisieren eines Auftrags

Um einen Auftrag zu aktualisieren, verwenden Sie den Befehl UpdateJob. Sie können die Felder `description`, `presignedUrlConfig`, `jobExecutionsRolloutConfig`, `abortConfig` und `timeoutConfig` eines Auftrags aktualisieren.

```
aws iot update-job  \
  --job-id 010  \
  --description "updated description" \
  --timeout-config inProgressTimeoutInMinutes=100 \
  --job-executions-rollout-config "{ \"exponentialRate\": { \"baseRatePerMinute\": 50,
 \"incrementFactor\": 2, \"rateIncreaseCriteria\": { \"numberOfNotifiedThings\": 1000,
 \"numberOfSucceededThings\": 1000}, \"maximumPerMinute\": 1000}}" \
```

```
  --abort-config "{ \"criteriaList\": [ { \"action\": \"CANCEL\", \"failureType
\": \"FAILED\", \"minNumberOfExecutedThings\": 100, \"thresholdPercentage\": 20},
 { \"action\": \"CANCEL\", \"failureType\": \"TIMED_OUT\", \"minNumberOfExecutedThings
\": 200, \"thresholdPercentage\": 50}]}" \
  --presigned-url-config "{\"roleArn\":\"arn:aws:iam::123456789012:role/
S3DownloadRole\", \"expiresInSec\":3600}"
```

Weitere Informationen finden Sie unter Rollout von Aufträgen und Abbruchskonfiguration.

## Abbrechen eines Auftrags

Um einen Auftrag abzubrechen, verwenden Sie den Befehl CancelJob. Durch das Abbrechen eines Jobs AWS IoT werden keine neuen Jobausführungen für den Job bereitgestellt. Außerdem werden alle Auftragsausführungen storniert, die sich in einem bestimmten Status befinden. `QUEUED` AWS IoT lässt alle Auftragsausführungen im Terminalstatus unberührt, da das Gerät den Job bereits abgeschlossen hat. Wenn der Status einer Auftragsausführung `IN_PROGRESS` ist, wird sie auch nicht verändert, es sei denn, Sie verwenden den optionalen `--force`-Parameter.

Der folgende Befehl zeigt, wie Sie einen Auftrag mit der ID 010 abbrechen.

```
aws iot cancel-job --job-id 010
```

Die Ausgabe des Befehls sieht wie folgt aus:

```
{
    "jobArn": "string",
    "jobId": "string",
    "description": "string"
}
```

Wenn Sie einen Auftrag abbrechen, werden Auftragsausführungen mit dem Status `QUEUED` abgebrochen. Auftragsausführungen mit dem Status `IN_PROGRESS` werden abgebrochen, aber nur, wenn Sie den optionalen `--force`-Parameter angeben. Auftragsausführungen mit einem Terminal-Zustand werden nicht abgebrochen.

> **Warning**
>
> Der Abbruch eines Auftrags im Status `IN_PROGRESS` (durch Setzen des `--force`-Parameters) bricht alle Auftragsausführungen ab, die sich in Ausführung befinden, was dazu führt, dass das Gerät, das den Auftrag ausführt, den Status der Auftragsausführung nicht

aktualisieren kann. Seien Sie vorsichtig, und stellen Sie sicher, dass jedes Gerät, das einen abgebrochenen Auftrag ausführt, in einen gültigen Status zurückkehren kann.

Der Status eines abgebrochenen Auftrags oder einer seiner Jobausführungen ist letztendlich konsistent. AWS IoT beendet die Planung neuer Auftragsausführungen und `QUEUED` Auftragsausführungen für diesen Job auf Geräten so schnell wie möglich. Die Änderung des Status einer Auftragsausführung zu `CANCELED` kann jedoch je nach der Anzahl der Geräte und anderen Faktoren einige Zeit dauern.

Wenn ein Auftrag abgebrochen wurde, da er die von einem `AbortConfig`-Objekt definierten Kriterien erfüllt hat, fügt der Service automatisch eingegebene Werte für die Felder `comment` und `reasonCode` hinzu. Sie können Ihre eigenen Werte für `reasonCode` erstellen, wenn der Abbruch des Auftrags vom Benutzer gesteuert wird.

## Abbrechen einer Auftragsausführung

Um eine Auftragsausführung auf einem Gerät abzubrechen, verwenden Sie den CancelJobExecution-Befehl. Damit wird eine Auftragsausführung abgebrochen, die sich im Status `QUEUED` befindet. Wenn Sie eine Auftragsausführung abbrechen möchten, die sich in Ausführung befindet, müssen Sie den `--force`-Parameter verwenden.

Der folgende Befehl zeigt, wie die Ausführung von Auftrag 010 auf `myThing` abgebrochen wird.

```
aws iot cancel-job-execution --job-id 010 --thing-name myThing
```

Der Befehl zeigt keine Ausgabe an.

Eine Auftragsausführung, die sich im Status `QUEUED` befindet, wird abgebrochen. Eine Auftragsausführung mit dem Status `IN_PROGRESS` wird abgebrochen, aber nur, wenn Sie den optionalen `--force`-Parameter angeben. Auftragsausführungen mit einem Terminal-Zustand können nicht abgebrochen werden.

> **Warning**
>
> Der Abbruch einer Auftragsausführung mit dem Status `IN_PROGRESS` führt dazu, dass das Gerät den Ausführungsstatus für den Auftrag nicht aktualisieren kann. Seien Sie vorsichtig, und stellen Sie sicher, dass das Gerät in der Lage ist, in einen gültigen Status zurückzukehren.

Wenn sich die Auftragsausführung in einem Terminal-Zustand oder im Status `IN_PROGRESS` befindet und der `--force`-Parameter nicht auf `true` gesetzt ist, führt dieser Befehl zu einer `InvalidStateTransitionException`.

Der Status einer abgebrochenen Auftragsausführungen bleibt schließlich konsistent. Das Ändern des Status einer Auftragsausführung zu `CANCELED` kann aufgrund verschiedener Faktoren einige Zeit in Anspruch nehmen.

## Löschen eines Auftrags

Um einen Auftrag und dessen Auftragsausführungen zu löschen, verwenden Sie den DeleteJob-Befehl. Standardmäßig können Sie nur einen Auftrag löschen, der sich in einem Terminal-Zustand (`SUCCEEDED` oder `CANCELED`) befindet. Andernfalls tritt eine Ausnahme auf. Sie können einen Auftrag im Status `IN_PROGRESS` löschen, jedoch nur, wenn der `force`-Parameter auf `true` gesetzt ist.

Um einen Auftrag zu löschen, führen Sie den folgenden Befehl aus:

```
aws iot delete-job --job-id 010 --force|--no-force
```

Der Befehl zeigt keine Ausgabe an.

> **Warning**
>
> Wenn Sie einen Auftrag löschen, der sich im `IN_PROGRESS`-Status befindet, kann das Gerät, das den Auftrag umsetzt, nicht auf Auftragsinformationen zugreifen oder den Status der Auftragsausführung aktualisieren. Seien Sie vorsichtig, und stellen Sie sicher, dass jedes Gerät, das einen gelöschten Auftrag umsetzt, in einen gültigen Status zurückkehren kann.

Das Löschen eines Auftrags kann einige Zeit in Anspruch nehmen, abhängig von der Anzahl der Auftragsausführungen für den Auftrag und anderen Faktoren. Während der Auftrag gelöscht wird, wird `DELETION_IN_PROGRESS` als Status des Auftrags angezeigt. Es tritt ein Fehler auf, wenn Sie versuchen, einen Auftrag abzubrechen oder zu löschen, dessen Status bereits `DELETION_IN_PROGRESS` ist.

Nur 10 Aufträge können gleichzeitig den Status `DELETION_IN_PROGRESS` haben. Andernfalls tritt eine `LimitExceededException` auf.

## Abrufen eines Auftragsdokuments

Um ein Auftragsdokument für einen Auftrag abzurufen, verwenden Sie den Befehl GetJobDocument. Ein Auftragsdokument ist eine Beschreibung der Remoteoperationen, die von den Geräten ausgeführt werden sollen.

Um ein Auftragsdokument zu erhalten, führen Sie den folgenden Befehl aus:

```
aws iot get-job-document --job-id 010
```

Der Befehl gibt das Auftragsdokument für den angegebenen Auftrag aus:

```
{
    "document": "{\n\t\"operation\":\"install\",\n\t\"url\":\"http://amazon.com/
firmWareUpate-01\",\n\t\"data\":\"${aws:iot:s3-presigned-url:https://s3.amazonaws.com/
amzn-s3-demo-bucket/datafile}\"\n}"
}
```

> **Note**
>
> Wenn Sie diesen Befehl verwenden, um ein Jobdokument abzurufen, werden Platzhalter URLs nicht durch vorsignierte Amazon S3 ersetzt. URLs Wenn ein Gerät den GetPendingJobExecutionsAPI-Vorgang aufruft, URLs werden die Platzhalter URLs im Auftragsdokument durch vorsignierte Amazon S3 ersetzt.

## Auflisten von Aufträgen

Um eine Liste aller Jobs in Ihrem zu erhalten AWS-Konto, verwenden Sie den ListJobs Befehl. Auftragsdaten und Auftragsausführungsdaten werden für eine begrenzte Zeitaufbewahrt. Führen Sie den folgenden Befehl aus, um alle Jobs in Ihrem aufzulisten AWS-Konto:

```
aws iot list-jobs
```

Der Befehl listet alle Aufträge in Ihrem Konto nach Auftragsstatus sortiert auf:

```
{
    "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": "SUCCEEDED",
            "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"
        }
    ]
}
```

## Beschreiben eines Auftrags

Um den Status eines Auftrags abzurufen, führen Sie den Befehl DescribeJob aus. Der folgende Befehl zeigt, wie Sie einen Auftrag beschreiben:

```
$ aws iot describe-job --job-id 010
```

Der Auftrag gibt den Status des angegebenen Auftrags aus. Zum Beispiel:

```
{
    "documentSource": "https://s3.amazonaws.com/amzn-s3-demo-bucket/job-
document.json",
    "job": {
        "status": "IN_PROGRESS",
        "jobArn": "arn:aws:iot:us-east-1:123456789012:job/010",
        "targets": [
            "arn:aws:iot:us-east-1:123456789012:thing/myThing"
```

```
        ],
        "jobProcessDetails": {
            "numberOfCanceledThings": 0,
            "numberOfFailedThings": 0,
            "numberOfInProgressThings": 0,
            "numberOfQueuedThings": 0,
            "numberOfRejectedThings": 0,
            "numberOfRemovedThings": 0,
            "numberOfSucceededThings": 0,
            "numberOfTimedOutThings": 0,
            "processingTargets": [
                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,
                arn:aws:iot:us-east-1:123456789012:thinggroup/thinggroupTwo
            ]
        },
        "presignedUrlConfig": {
            "expiresInSec": 60,
            "roleArn": "arn:aws:iam::123456789012:role/S3DownloadRole"
        },
        "jobId": "010",
        "lastUpdatedAt": 1486593195.006,
        "createdAt": 1486593195.006,
        "targetSelection": "SNAPSHOT",
        "jobExecutionsRolloutConfig": {
            "exponentialRate": {
                "baseRatePerMinute": integer,
                "incrementFactor": integer,
                "rateIncreaseCriteria": {
                    "numberOfNotifiedThings": integer, // Set one or the other
                    "numberOfSucceededThings": integer // of these two values.
                },
            "maximumPerMinute": integer
         }
        },
        "abortConfig": {
            "criteriaList": [
                {
                    "action": "string",
                    "failureType": "string",
                    "minNumberOfExecutedThings": integer,
                    "thresholdPercentage": integer
                }
```

```
            ]
        },
        "timeoutConfig": {
           "inProgressTimeoutInMinutes": number
          }
    }
}
```

## Auflisten von Ausführungen für einen Auftrag

Ein Auftrag, der auf einem bestimmten Gerät ausgeführt wird, wird durch ein Auftragsausführungsobjekt repräsentiert. Mit dem Befehl ListJobExecutionsForJob listen Sie alle Auftragsausführungen für einen Auftrag auf. Nachfolgend sehen Sie, wie Sie die Ausführungen für einen Auftrag auflisten können:

```
aws iot list-job-executions-for-job --job-id 010
```

Der Befehl gibt eine Liste von Auftragsausführungen zurück:

```
{
    "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,
            "queuedAt": 1486593196.378,
            "startedAt": 1486593345.659,
            "executionNumber": 4567890123
        }
    }
    ]
}
```

## Auflisten von Auftragsausführungen für ein Objekt

Mit dem Befehl ListJobExecutionsForThing listen Sie alle Auftragsausführungen auf einem Objekt auf. Nachfolgend sehen Sie, wie Sie die Auftragsausführungen für ein Objekt auflisten können:

```
aws iot list-job-executions-for-thing --thing-name thingOne
```

Der Befehl gibt eine Liste der Auftragsausführungen aus, die auf dem angegebenen Objekt ausgeführt werden oder wurden:


```
{
    "executionSummaries": [
    {
        "jobExecutionSummary": {
            "status": "QUEUED",
            "lastUpdatedAt": 1486687082.071,
            "queuedAt": 1486687082.071,
            "executionNumber": 9876543210
        },
        "jobId": "013"
    },
    {
        "jobExecutionSummary": {
            "status": "IN_PROGRESS",
            "startAt": 1486685870.729,
            "lastUpdatedAt": 1486685870.729,
            "queuedAt": 1486685870.729,
            "executionNumber": 1357924680
        },
        "jobId": "012"
    },
    {
        "jobExecutionSummary": {
            "status": "SUCCEEDED",
            "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"
    }
    ]
}
```

## Beschreiben der Auftragsausführung

Mit dem Befehl DescribeJobExecution rufen Sie den Status einer Auftragsausführung ab. Sie müssen eine Auftrags-ID und den Namen eines Objekts sowie optional eine Ausführungsnummer angeben, um die Auftragsausführung zu identifizieren. Nachfolgend sehen Sie, wie Sie eine Auftragsausführung beschreiben können:

```
aws iot describe-job-execution --job-id 017 --thing-name thingOne
```

Der Befehl gibt den `JobExecution` zurück: Zum Beispiel:

```
{
    "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",
        "approximateSecondsBeforeTimedOut": 100,
        "statusDetails": {
            "status": "IN_PROGRESS",
            "detailsMap": {
                "percentComplete": "10"
            }
        }
    }
}
```

### Löschen einer Auftragsausführung

Mit dem DeleteJobExecution-Befehl löschen Sie eine Auftragsausführung. Sie müssen eine Auftrags-ID und den Namen eines Objekts und eine Ausführungsnummer angeben, um die Auftragsausführung zu identifizieren. Nachfolgend sehen Sie, wie Sie eine Auftragsausführung löschen können:

```
aws iot delete-job-execution --job-id 017 --thing-name thingOne --execution-number
 1234567890 --force|--no-force
```

Der Befehl zeigt keine Ausgabe an.

Standardmäßig muss der Status der Auftragsausführung `QUEUED` oder ein Terminal-Zustand (`SUCCEEDED`, `FAILED`, `REJECTED`, `TIMED_OUT`, `REMOVED` oder `CANCELED`) sein. Andernfalls tritt ein Fehler auf. Um eine Auftragsausführung mit dem Status `IN_PROGRESS` zu löschen, können Sie den `force`-Parameter auf `true` setzen.

> **Warning**
>
> Wenn Sie eine Auftragsausführung löschen, die sich im `IN_PROGRESS`-Status befindet, kann das Gerät, das den Auftrag ausführt, nicht auf Auftragsinformationen zugreifen oder den Status der Auftragsausführung aktualisieren. Seien Sie vorsichtig, und stellen Sie sicher, dass das Gerät in der Lage ist, in einen gültigen Status zurückzukehren.

## Auftragsvorlagen

Verwenden Sie Auftragsvorlagen, um Aufträge vorzukonfigurieren, die Sie auf mehreren Gruppen von Zielgeräten bereitstellen können. Zum Bereitstellen häufig ausgeführter Remote-Aktionen wie das Neustarten oder Installieren einer Anwendung auf Ihren Geräten können Sie Vorlagen verwenden, um Standardkonfigurationen zu definieren. Zum Durchführen von Vorgängen wie die Bereitstellung von Sicherheitspatches und Bugfixes können Sie Vorlagen aus vorhandenen Aufträgen erstellen.

Geben Sie beim Erstellen einer Auftragsvorlage die folgenden zusätzlichen Konfigurationen und Ressourcen an.

- Auftragseigenschaften
- Auftragsunterlagen und Ziele

- Kriterien für Rollout, Planung und Abbrechen
- Kriterien für Zeitüberschreibung und Wiederholung

## Benutzerdefinierte und AWS verwaltete Vorlagen

Abhängig von der Remote-Aktion, die Sie ausführen möchten, können Sie entweder eine benutzerdefinierte Jobvorlage erstellen oder eine AWS verwaltete Vorlage verwenden. Verwenden Sie benutzerdefinierte Auftragsvorlagen, um Ihr eigenes benutzerdefiniertes Auftragsdokument bereitzustellen und wiederverwendbare Jobs zu erstellen, die Sie auf Ihren Geräten bereitstellen können. AWS Verwaltete Vorlagen sind Auftragsvorlagen, die von AWS IoT Jobs für häufig ausgeführte Aktionen bereitgestellt werden. Diese Vorlagen enthalten ein vordefiniertes Auftragsdokument für einige Remote-Aktionen, sodass Sie kein eigenes Auftragsdokument erstellen müssen. Verwaltete Vorlagen helfen Ihnen dabei, wiederverwendbare Aufträge zu erstellen, damit Sie diese Aufträge schneller auf Ihren Geräten starten können.

Themen

- Verwenden Sie AWS verwaltete Vorlagen, um allgemeine Fernoperationen bereitzustellen
- Erstellen von benutzerdefinierten Auftragsvorlagen

## Verwenden Sie AWS verwaltete Vorlagen, um allgemeine Fernoperationen bereitzustellen

AWS Verwaltete Vorlagen sind Auftragsvorlagen, die von bereitgestellt werden AWS. Sie werden für häufig ausgeführte Remote-Aktionen wie den Neustart, das Herunterladen einer Datei oder die Installation einer Anwendung auf Ihren Geräten verwendet. Diese Vorlagen verfügen über ein vordefiniertes Auftragsdokument für jede Remote-Aktion, sodass Sie kein eigenes Auftragsdokument erstellen müssen.

Sie können aus einer Reihe vordefinierter Konfigurationen auswählen und Aufträge mit diesen Vorlagen erstellen, ohne zusätzlichen Code schreiben zu müssen. Mithilfe verwalteter Vorlagen können Sie das Auftragsdokument einsehen, das für Ihre Flotten bereitgestellt wurde. Sie können mithilfe dieser Vorlagen einen Auftrag erstellen und eine benutzerdefinierte Auftragsvorlage erstellen, die Sie für Ihre Remoteoperationen wiederverwenden können.

### Was enthalten verwaltete Vorlagen?

Jede AWS verwaltete Vorlage enthält:

- Die Umgebung, in der die Befehle im Auftragsdokument ausgeführt werden.
- Ein Auftragsdokument, das den Namen und die Parameter der Operation angibt. Wenn Sie beispielsweise eine Vorlage für Download Datei verwenden, lautet der Name der Operation Datei herunterladen und die Parameter können wie folgt lauten:
  - Die URL Datei, die Sie auf Ihr Gerät herunterladen möchten. Dies kann eine Internetressource oder ein öffentlicher oder vorab signierter Amazon Simple Storage Service (Amazon S3) URL sein.
  - Ein lokaler Dateipfad auf dem Gerät zum Speichern der heruntergeladenen Datei.

  Weitere Information zum Auftragsdokument und den Parametern finden Sie unter Verwaltete Vorlagen für Remote-Aktionen und Auftragsdokumente.

## Voraussetzungen

Damit Ihre Geräte die Remote-Aktionen ausführen können, die im verwalteten Auftragsvorlagendokument festgelegt sind, müssen Sie Folgendes tun:

- Installieren Sie die bestimmte Software auf Ihrem Gerät.

  Verwenden Sie Ihre eigene Gerätesoftware und Job-Handler oder den AWS IoT Device Client. Abhängig von Ihrem Geschäftsfall können Sie beide auch so ausführen, dass sie unterschiedliche Funktionen durchführen.

  - Verwenden Sie Ihre eigene Gerätesoftware und Auftragshandler

    Sie können Ihren eigenen Code für Geräte schreiben, indem Sie AWS IoT Device SDK und die zugehörigen Handler-Bibliotheken verwenden, mit denen die Remoteoperationen unterstützt werden. Stellen Sie sicher, dass zum Bereitstellen und Ausführen von Aufträgen die Geräteagent-Bibliotheken korrekt installiert wurden und auf den Geräten ausgeführt werden.

    Sie können auch Ihre eigenen Handler verwenden, mit denen die Remoteoperationen unterstützt werden. Weitere Informationen finden Sie unter Beispiele für Job-Handler im AWS IoT Device GitHub Client-Repository.

  - Verwenden Sie den AWS IoT Geräteclient

    Sie können den AWS IoT Geräteclient auch auf Ihren Geräten installieren und ausführen, da er standardmäßig die Verwendung aller verwalteten Vorlagen direkt von der Konsole aus unterstützt.

Der Device Client ist eine in C++ geschriebene Open-Source-Software, die Sie kompilieren und auf Ihren eingebetteten Linux-basierten IoT-Geräten installieren können. Der Device Client verfügt über einen Basisclient und separate clientseitige Funktionen. Der Basisclient stellt die Konnektivität AWS IoT über MQTT das Protokoll her und kann eine Verbindung zu den verschiedenen clientseitigen Funktionen herstellen.

Verwenden Sie die clientseitige Auftragsfunktion des Geräteclients, um Remoteoperationen auf Ihren Geräten durchzuführen. Diese Funktion enthält einen Parser zum Empfangen des Auftragsdokuments und Auftragshandler, mit denen die im Auftragsdokument angegebenen Remote-Aktionen implementiert sind. Weitere Informationen zum Device Client und dessen zugehörige Funktionen finden unter AWS IoT Device Client.

Bei der Ausführung auf Geräten empfängt der Device Client das Auftragsdokument und verfügt über eine plattformspezifische Implementierung, mit der er Befehle im Dokument ausführt. Weitere Informationen zum Einrichten des Device Client und zur Verwendung der Funktion Aufträge finden Sie unter AWS IoT -Tutorials.

- Verwenden Sie eine unterstützte Umgebung

Für jede verwaltete Vorlage finden Sie Informationen über die Umgebung, in der Sie die Remote-Aktionen ausführen können. Wir empfehlen, dass Sie die Vorlage in einer unterstützten Linux-Umgebung verwenden, so wie das in der Vorlage angegeben ist. Verwenden Sie den AWS IoT Geräteclient, um die verwalteten Template-Remote-Aktionen auszuführen, da er gängige Mikroprozessoren und Linux-Umgebungen wie Debian und Ubuntu unterstützt.

## Verwaltete Vorlagen für Remote-Aktionen und Auftragsdokumente

Der folgende Abschnitt listet die verschiedenen AWS verwalteten Vorlagen für AWS IoT Jobs auf und beschreibt die Remote-Aktionen, die auf den Geräten ausgeführt werden können. Der folgende Abschnitt enthält Informationen zum Auftragsdokument und eine Beschreibung der Parameter für das Auftragsdokument für jede Remote-Aktion. Ihre geräteseitige Software verwendet zum Durchführen der Remote-Aktion den Vorlagennamen und die Parameter.

AWS Verwaltete Vorlagen akzeptieren Eingabeparameter, für die Sie einen Wert angeben, wenn Sie mithilfe der Vorlage einen Job erstellen. Allen verwalteten Vorlagen haben zwei gemeinsame optionale Eingabeparameter: `runAsUser` und `pathToHandler`. Mit Ausnahme der `AWS-Reboot`-Vorlage benötigen die Vorlagen zusätzliche Eingabeparameter, für die Sie einen Wert angeben müssen, wenn Sie einen Auftrag mithilfe der Vorlage erstellen. Die erforderlichen Eingabeparameter

variieren je nach der von Ihnen ausgewählten Vorlage. Wenn Sie beispielsweise die `AWS-Download-File` Vorlage auswählen, müssen Sie eine Liste von Paketen angeben, die installiert werden sollen, und eine, aus der Dateien heruntergeladen werden URL sollen.

Geben Sie einen Wert für die Eingabeparameter an, wenn Sie die AWS IoT Konsole verwenden, oder die AWS Command Line Interface (AWS CLI), um einen Job zu erstellen, der eine verwaltete Vorlage verwendet. Wenn Sie den verwendenCLI, geben Sie diese Werte mithilfe des `document-parameters` Objekts an. Weitere Informationen finden Sie unter documentParameters.

> **Note**
>
> Verwenden Sie `document-parameters` nur beim Erstellen von Aufträgen AWS -verwaltete Vorlagen. Dieser Parameter kann nicht mit benutzerdefinierten Auftragsvorlagen oder zum Erstellen von Aufträgen aus diesen Auftragsvorlagen verwendet werden.

Im Folgenden finden Sie eine Beschreibung der gängigen optionalen Eingabeparameter. Im nächsten Abschnitt finden Sie eine Beschreibung der anderen Eingabeparameter, die für jede verwaltete Vorlage erforderlich sind.

`runAsUser`

Dieser Parameter gibt an, ob der Auftragshandler unter einem anderen Benutzer ausgeführt werden soll. Wird er bei der Auftragserstellung nicht angegeben, wird der Auftragshandler unter demselben Benutzer wie der Device Client ausgeführt. Wenn Sie den Auftragshandler unter einem anderen Benutzer ausführen, geben Sie einen Zeichenkettenwert an, der nicht länger als 256 Zeichen ist.

`pathToHandler`

Der Pfad zum Auftragshandler, der auf dem Gerät ausgeführt wird. Wenn der Pfad bei der Auftragserstellung nicht angegeben wurde, verwendet der Device Client das aktuelle Arbeitsverzeichnis.

Im Folgenden werden die verschiedenen Remote-Aktionen, ihre Auftragsdokumente und die von ihnen akzeptierten Parameter dargestellt. Alle diese Vorlagen unterstützen die Linux-Umgebung für die Ausführung des Remote-Operation auf dem Gerät.

AWS–Download-Datei

Name der Vorlage

`AWS-Download-File`

Vorlagenbeschreibung

Eine verwaltete Vorlage, die von AWS zum Herunterladen einer Datei bereitgestellt wird.

Eingabeparameter

Diese Vorlage verfügt über die folgenden erforderlichen Parameter. Sie können auch die optionalen Parameter `runAsUser` und `pathToHandler` angeben.

`downloadUrl`

DieURL, von der die Datei heruntergeladen werden soll. Dies kann eine Internetressource sein, ein Objekt in Amazon S3, auf das öffentlich zugegriffen werden kann, oder ein Objekt in Amazon S3, auf das Ihr Gerät nur mit einem vorsignierten URL Objekt zugreifen kann. Weitere Informationen zur Verwendung vorsignierter Berechtigungen URLs und zur Erteilung von Berechtigungen finden Sie unter. Vorsigniert URLs

`filePath`

Ein lokaler Dateipfad, der den Speicherort auf dem Gerät anzeigt, an dem die heruntergeladene Datei gespeichert wird.

Geräteverhalten

Das Gerät lädt die Datei vom angegebenen Speicherort herunter, überprüft, ob der Download abgeschlossen ist und speichert sie lokal.

Auftragsdokument

Im Folgenden werden das Auftragsdokument und die zugehörige neueste Version angezeigt. Die Vorlage zeigt den Pfad zum Auftragshandler und zum Shell-Skript `download-file.sh`, die der Auftragshandler ausführen muss, um die Datei herunterzuladen. Es zeigt auch die erforderlichen Parameter `downloadUrl` und `filePath` an.

```
{
  "version": "1.0",
  "steps": [
```

```
    {
      "action": {
        "name": "Download-File",
        "type": "runHandler",
        "input": {
          "handler": "download-file.sh",
          "args": [
            "${aws:iot:parameter:downloadUrl}",
            "${aws:iot:parameter:filePath}"
          ],
          "path": "${aws:iot:parameter:pathToHandler}"
        },
        "runAsUser": "${aws:iot:parameter:runAsUser}"
      }
    }
  ]
}
```

AWS-Install-Application

Name der Vorlage

`AWS-Install-Application`

Vorlagenbeschreibung

Eine verwaltete Vorlage, die von AWS für die Installation einer oder mehrerer Anwendungen bereitgestellt wird.

Eingabeparameter

Diese Vorlage hat den folgenden erforderlichen Parameter, `packages`. Sie können auch die optionalen Parameter `runAsUser` und `pathToHandler` angeben.

`packages`

Eine durch Leerzeichen getrennte Liste mit einer oder mehreren Anwendungen, die installiert werden sollen.

Geräteverhalten

Das Gerät installiert die Anwendungen, wie im Auftragsdokument angegeben.

Auftragsdokument

Im Folgenden werden das Auftragsdokument und die zugehörige neueste Version angezeigt. Die Vorlage zeigt den Pfad zum Auftragshandler und zum Shell-Skript `install-packages.sh`, die der Auftragshandler ausführen muss, um die Datei herunterzuladen. Es zeigt auch den erforderlichen Parameter `packages` an.

```
{
  "version": "1.0",
  "steps": [
    {
      "action": {
        "name": "Install-Application",
        "type": "runHandler",
        "input": {
          "handler": "install-packages.sh",
          "args": [
            "${aws:iot:parameter:packages}"
          ],
          "path": "${aws:iot:parameter:pathToHandler}"
        },
        "runAsUser": "${aws:iot:parameter:runAsUser}"
      }
    }
  ]
}
```

AWS-Neustart

Name der Vorlage

`AWS-Reboot`

Vorlagenbeschreibung

Eine verwaltete Vorlage, die von AWS für den Neustart Ihres Geräts bereitgestellt wird.

Eingabeparameter

Dieser Befehl hat keine erforderlichen Parameter. Sie können die optionalen Parameter `runAsUser` und `pathToHandler` angeben.

Geräteverhalten

Das Gerät wird erfolgreich neu gestartet.

Auftragsdokument

Im Folgenden werden das Auftragsdokument und die zugehörige neueste Version angezeigt. Die Vorlage zeigt den Pfad zum Auftragshandler und zum Shell-Skript `reboot.sh`, die der Auftragshandler ausführen muss, um das Gerät neu zu starten.

```
{
  "version": "1.0",
  "steps": [
    {
      "action": {
        "name": "Reboot",
        "type": "runHandler",
        "input": {
          "handler": "reboot.sh",
          "path": "${aws:iot:parameter:pathToHandler}"
        },
        "runAsUser": "${aws:iot:parameter:runAsUser}"
      }
    }
  ]
}
```

AWS-Remove-Application

Name der Vorlage

`AWS-Remove-Application`

Vorlagenbeschreibung

Eine verwaltete Vorlage, die von AWS für die Deinstallation einer oder mehrerer Anwendungen bereitgestellt wird.

Eingabeparameter

Diese Vorlage hat den folgenden erforderlichen Parameter, `packages`. Sie können auch die optionalen Parameter `runAsUser` und `pathToHandler` angeben.

`packages`

Eine durch Leerzeichen getrennte Liste mit einer oder mehreren Anwendungen, die deinstalliert werden sollen.

Geräteverhalten

Das Gerät deinstalliert die Anwendungen, wie im Jobdokument angegeben.

Auftragsdokument

Im Folgenden werden das Auftragsdokument und die zugehörige neueste Version angezeigt. Die Vorlage zeigt den Pfad zum Auftragshandler und zum Shell-Skript `remove-packages.sh`, die der Auftragshandler ausführen muss, um die Datei herunterzuladen. Es zeigt auch den erforderlichen Parameter `packages` an.

```
{
  "version": "1.0",
  "steps": [
    {
      "action": {
        "name": "Remove-Application",
        "type": "runHandler",
        "input": {
          "handler": "remove-packages.sh",
          "args": [
            "${aws:iot:parameter:packages}"
          ],
          "path": "${aws:iot:parameter:pathToHandler}"
        },
        "runAsUser": "${aws:iot:parameter:runAsUser}"
      }
    }
  ]
}
```

AWS–Restart–Application

Name der Vorlage

`AWS-Restart-Application`

Vorlagenbeschreibung

Eine verwaltete Vorlage, die von AWS zum Beenden und Neustarten eines oder mehrerer Dienste bereitgestellt wird.

Eingabeparameter

Diese Vorlage hat den folgenden erforderlichen Parameter, `services`. Sie können auch die optionalen Parameter `runAsUser` und `pathToHandler` angeben.

Services

Eine durch Leerzeichen getrennte Liste mit einer oder mehreren Anwendungen, die neu gestartet werden sollen.

Geräteverhalten

Die angegebenen Anwendungen werden gestoppt und dann auf dem Gerät neu gestartet.

Auftragsdokument

Im Folgenden werden das Auftragsdokument und die zugehörige neueste Version angezeigt. Die Vorlage zeigt den Pfad zum Auftragshandler und zum Shell-Skript `restart-services.sh`, die der Auftragshandler ausführen muss, um die Systemdienste neu zu starten. Es zeigt auch den erforderlichen Parameter `services` an.

```
{
  "version": "1.0",
  "steps": [
    {
      "action": {
        "name": "Restart-Application",
        "type": "runHandler",
        "input": {
          "handler": "restart-services.sh",
          "args": [
            "${aws:iot:parameter:services}"
          ],
          "path": "${aws:iot:parameter:pathToHandler}"
        },
        "runAsUser": "${aws:iot:parameter:runAsUser}"
      }
    }
  ]
}
```

AWS-Start-Application

Name der Vorlage

`AWS-Start-Application`

Vorlagenbeschreibung

Eine verwaltete Vorlage, die von AWS zum Starten eines oder mehrerer Dienste bereitgestellt wird.

Eingabeparameter

Diese Vorlage hat den folgenden erforderlichen Parameter, `services`. Sie können auch die optionalen Parameter `runAsUser` und `pathToHandler` angeben.

`services`

Eine durch Leerzeichen getrennte Liste mit einer oder mehreren Anwendungen, die gestartet werden sollen.

Geräteverhalten

Die angegebenen Anwendungen werden auf dem Gerät ausgeführt.

Auftragsdokument

Im Folgenden werden das Auftragsdokument und die zugehörige neueste Version angezeigt. Die Vorlage zeigt den Pfad zum Auftragshandler und zum Shell-Skript `start-services.sh`, die der Auftragshandler ausführen muss, um die Systemdienste zu starten. Es zeigt auch den erforderlichen Parameter `services` an.

```
{
  "version": "1.0",
  "steps": [
    {
      "action": {
        "name": "Start-Application",
        "type": "runHandler",
        "input": {
          "handler": "start-services.sh",
          "args": [
            "${aws:iot:parameter:services}"
          ],
          "path": "${aws:iot:parameter:pathToHandler}"
        },
        "runAsUser": "${aws:iot:parameter:runAsUser}"
      }
    }
```

```
  ]
}
```

AWS-Stop-Application

Name der Vorlage

`AWS-Stop-Application`

Vorlagenbeschreibung

Eine verwaltete Vorlage, die von AWS zum Beenden eines oder mehrerer Dienste bereitgestellt wird.

Eingabeparameter

Diese Vorlage hat den folgenden erforderlichen Parameter, `services`. Sie können auch die optionalen Parameter `runAsUser` und `pathToHandler` angeben.

`services`

Eine durch Leerzeichen getrennte Liste mit einer oder mehreren Anwendungen, die beendet werden sollen.

Geräteverhalten

Die angegebenen Anwendungen werden auf dem Gerät nicht mehr ausgeführt.

Auftragsdokument

Im Folgenden werden das Auftragsdokument und die zugehörige neueste Version angezeigt. Die Vorlage zeigt den Pfad zum Auftragshandler und zum Shell-Skript `stop-services.sh`, die der Auftragshandler ausführen muss, um die Systemservices zu beenden. Es zeigt auch den erforderlichen Parameter `services` an.

```
{
  "version": "1.0",
  "steps": [
    {
      "action": {
        "name": "Stop-Application",
        "type": "runHandler",
        "input": {
          "handler": "stop-services.sh",
          "args": [
```

```
            "${aws:iot:parameter:services}"
          ],
          "path": "${aws:iot:parameter:pathToHandler}"
        },
        "runAsUser": "${aws:iot:parameter:runAsUser}"
      }
    }
  ]
}
```

AWS-Run-Command

Name der Vorlage

`AWS-Run-Command`

Vorlagenbeschreibung

Eine verwaltete Vorlage, die von AWS zur Ausführung eines Shell-Befehls bereitgestellt wird.

Eingabeparameter

Diese Vorlage hat den folgenden erforderlichen Parameter, `command`. Sie können auch den anderen optionalen Parameter `runAsUser` angeben.

`command`

Eine durch Kommas getrennte Befehlsfolge. Jedes Komma, das im Befehl selbst enthalten ist, muss maskiert werden.

Geräteverhalten

Das Gerät führt den Shell-Befehl wie im Auftragsdokument angegeben aus.

Auftragsdokument

Im Folgenden werden das Auftragsdokument und die zugehörige neueste Version angezeigt. Die Vorlage zeigt den Pfad zum Auftragsbefehl und den von Ihnen angegebenen Befehl, der auf dem Gerät ausgeführt werden soll.

```
{
  "version": "1.0",
  "steps": [
    {
```

```
      "action": {
        "name": "Run-Command",
        "type": "runCommand",
        "input": {
          "command": "${aws:iot:parameter:command}"
        },
        "runAsUser": "${aws:iot:parameter:runAsUser}"
      }
    }
  ]
}
```

Themen

- Erstellen Sie einen Job aus AWS verwalteten Vorlagen mithilfe von AWS Management Console
- Erstellen Sie einen Job aus AWS verwalteten Vorlagen mithilfe der AWS CLI

## Erstellen Sie einen Job aus AWS verwalteten Vorlagen mithilfe von AWS Management Console

Verwenden Sie die AWS Management Console , um Informationen zu AWS verwalteten Vorlagen abzurufen und mithilfe dieser Vorlagen einen Job zu erstellen. Anschließend können Sie den von Ihnen erstellten Auftrag als Ihre eigene benutzerdefinierte Vorlage speichern.

Abrufen von Details von verwalteten Vorlagen

In der AWS IoT Konsole können Sie Informationen zu den verschiedenen verwalteten Vorlagen abrufen, die verwendet werden können.

1. Um Ihre verfügbaren verwalteten Vorlagen zu sehen, gehen Sie zum Hub Jobvorlagen der AWS IoT Konsole und wählen Sie den Tab Verwaltete Vorlagen.
2. Zum Anzeigen von Details wählen Sie eine verwaltete Vorlage aus.

Die Seite Details enthält die folgenden Informationen:

- Name, Beschreibung und Amazon-Ressourcenname (ARN) der verwalteten Vorlage.
- Die Umgebung, in der die Remote-Operationen ausgeführt werden können, z. B. Linux.
- Das JSON Jobdokument, das den Pfad zum Job-Handler und die Befehle angibt, die auf dem Gerät ausgeführt werden sollen. Im Folgenden wird beispielsweise ein Beispiel-Jobdokument für

die Vorlage AWS-Reboot gezeigt. Die Vorlage zeigt den Pfad zum Auftragshandler und zum Shell-Skript `reboot.sh`, die der Auftragshandler ausführen muss, um das Gerät neu zu starten.

```
{
  "version": "1.0",
  "steps": [
    {
      "action": {
        "name": "Reboot",
        "type": "runHandler",
        "input": {
          "handler": "reboot.sh",
          "path": "${aws:iot:parameter:pathToHandler}"
        },
        "runAsUser": "${aws:iot:parameter:runAsUser}"
      }
    }
  ]
}
```

Weitere Informationen zum Auftragsdokument und den zugehörigen Parametern für verschiedene Remote-Aktionen finden Sie unter Verwaltete Vorlagen für Remote-Aktionen und Auftragsdokumente.

- Die neueste Version des Auftragsdokuments.

### Erstellen Sie einen Auftrag mit verwalteten Vorlagen

Sie können die AWS Managementkonsole verwenden, um eine AWS verwaltete Vorlage für die Erstellung eines Jobs auszuwählen. In diesem Abschnitt erfahren Sie mehr darüber.

Sie können auch den Workflow zur Auftragserstellung starten und dann die AWS verwaltete Vorlage auswählen, die Sie bei der Erstellung des Jobs verwenden möchten. Weitere Informationen zu diesem Workflow finden Sie unter Erstellen und Verwalten von Aufträgen mithilfe von AWS Management Console.

1. Wählen Sie Ihre AWS verwaltete Vorlage

   Gehen Sie in der AWS IoT Konsole zum Hub Jobvorlagen, wählen Sie den Tab Verwaltete Vorlagen und wählen Sie dann Ihre Vorlage aus.

2. Erstellen Sie einen Auftrag mit Ihrer verwalteten Vorlage

    1. Wählen Sie auf der Seite Details Ihrer Vorlage die Option Auftrag erstellen aus.

        Die Konsole wechselt zum Schritt Benutzerdefinierte Auftragseigenschaften des Workflows Auftrag erstellen, in dem Ihre Vorlagenkonfiguration hinzugefügt wurde.

    2. Geben Sie einen eindeutigen alphanumerischen Auftragsnamen sowie optional eine Beschreibung und Tags ein und wählen Sie dann Weiter aus.

    3. Wählen Sie die Objekte oder Objektgruppen als Auftragsziele aus, die Sie in diesem Auftrag ausführen möchten.

    4. Im Bereich Auftragsdokument wird Ihre Vorlage mit ihren Konfigurationseinstellungen und Eingabeparametern angezeigt. Geben Sie Werte für die Eingabeparameter in die von Ihnen ausgewählten Vorlage ein. Wenn Sie beispielsweise die Vorlage AWS-Download-File gewählt haben:

        - Geben Sie für die URL Datei ein downloadUrl, die Sie herunterladen möchten, zum Beispiel:`https://example.com/index.html`.
        - Geben Sie zum filePathBeispiel den Pfad auf dem Gerät ein, in dem die heruntergeladene Datei gespeichert werden soll, z. B.:*path/to/file*.

        Sie können optional auch Werte für die Parameter `runAsUser` und `pathToHandler` eingeben. Weitere Informationen zu den Eingabeparametern für jede Vorlage finden Sie unter Verwaltete Vorlagen für Remote-Aktionen und Auftragsdokumente.

    5. Wählen Sie auf der Seite Auftragskonfiguration den Auftragstyp als kontinuierlichen Auftrag oder Snapshot-Auftrag aus. Ein Snapshot-Auftrag ist abgeschlossen, wenn er seine Ausführung auf den Zielgeräten und Zielgruppen abgeschlossen hat. Ein kontinuierlicher Auftrag gilt für Objektgruppen und wird auf jedem Gerät ausgeführt, das Sie einer bestimmten Zielgruppe hinzufügen.

    6. Fügen Sie weitere Konfigurationen für Ihren Auftrag hinzu und überprüfen und erstellen Sie dann Ihren Auftrag. Weitere Informationen zum Arbeiten mit zusätzlichen Konfigurationen finden Sie unter:

        - Konfigurationen für Auftrags-Rollout, Planung und Abbruch
        - Timeout bei der Auftragsausführung und Wiederholungskonfigurationen

Erstellen Sie benutzerdefinierte Jobvorlagen aus verwalteten Vorlagen

Sie können eine AWS verwaltete Vorlage und einen benutzerdefinierten Job als Ausgangspunkt verwenden, um Ihre eigene benutzerdefinierte Jobvorlage zu erstellen. Um eine benutzerdefinierte Jobvorlage zu erstellen, erstellen Sie zunächst einen Job anhand Ihrer AWS verwalteten Vorlage, wie im vorherigen Abschnitt beschrieben.

Anschließend können Sie den benutzerdefinierten Auftrag als Vorlage speichern, um Ihre eigene benutzerdefinierte Auftragsvorlage zu erstellen. Zum Speichern als Vorlage:

1. Gehen Sie zum Job-Hub der AWS IoT Konsole und wählen Sie den Job aus, der Ihre verwaltete Vorlage enthält.
2. Wählen Sie die Option Als Auftragsvorlage speichern und erstellen Sie dann Ihre benutzerdefinierte Auftragsvorlage. Weitere Informationen zum Erstellen einer benutzerdefinierten Auftragsvorlage finden Sie unter Erstellen einer Auftragsvorlage anhand eines vorhandenen Auftrags.

## Erstellen Sie einen Job aus AWS verwalteten Vorlagen mithilfe der AWS CLI

Verwenden Sie den AWS CLI , um Informationen zu AWS verwalteten Vorlagen abzurufen und mithilfe dieser Vorlagen einen Job zu erstellen. Anschließend können Sie den Auftrag als Vorlage speichern und anschließend Ihre eigene benutzerdefinierte Vorlage erstellen.

Auflisten von verwalteten Vorlagen

Der `list-managed-job-templates` AWS CLI Befehl listet alle Jobvorlagen in Ihrem auf AWS-Konto.

```
aws iot list-managed-job-templates
```

Wenn Sie diesen Befehl ausführen, werden standardmäßig alle verfügbaren AWS verwalteten Vorlagen und deren Details angezeigt.

```
{
    "managedJobTemplates": [
        {
            "templateArn": "arn:aws:iot:region::jobtemplate/AWS-Reboot:1.0",
            "templateName": "AWS-Reboot",
```

```
            "description": "A managed job template for rebooting the device.",
            "environments": [
                "LINUX"
            ],
            "templateVersion": "1.0"
        },
        {
            "templateArn": "arn:aws:iot:region::jobtemplate/AWS-Remove-
Application:1.0",
            "templateName": "AWS-Remove-Application",
            "description": "A managed job template for uninstalling one or more
 applications.",
            "environments": [
                "LINUX"
            ],
            "templateVersion": "1.0"
        },
        {
            "templateArn": "arn:aws:iot:region::jobtemplate/AWS-Stop-Application:1.0",
            "templateName": "AWS-Stop-Application",
            "description": "A managed job template for stopping one or more system
 services.",
            "environments": [
                "LINUX"
            ],
            "templateVersion": "1.0"
        },

        ...

        {
            "templateArn": "arn:aws:iot:us-east-1::jobtemplate/AWS-Restart-
Application:1.0",
            "templateName": "AWS-Restart-Application",
            "description": "A managed job template for restarting one or more system
 services.",
            "environments": [
                "LINUX"
            ],
            "templateVersion": "1.0"
        }
    ]
}
```

Weitere Informationen finden Sie unter ListManagedJobTemplates.

Abrufen von Details über eine verwaltete Vorlage

Der `describe-managed-job-template` AWS CLI Befehl ruft Details zu einer angegebenen Jobvorlage ab. Geben Sie den Namen der Auftragsvorlage und eine optionale Vorlagenversion an. Wenn die Vorlagenversion nicht angegeben ist, wird die vordefinierte Standardversion zurückgegeben. Um beispielsweise Details über die `AWS-Download-File`-Vorlage zu sehen, führen Sie den folgenden Befehl aus.

```
aws iot describe-managed-job-template \
    --template-name AWS-Download-File
```

Der Befehl zeigt die Vorlagendetails und das ARN zugehörige Jobdokument sowie den `documentParameters` Parameter an, bei dem es sich um eine Liste von Schlüssel-Wert-Paaren von Eingabeparametern der Vorlage handelt. Weitere Informationen zu den verschiedenen Vorlagen und Eingabeparametern finden Sie unter Verwaltete Vorlagen für Remote-Aktionen und Auftragsdokumente.

> **Note**
>
> Das bei dieser Verwendung zurückgegebene `documentParameters` Objekt API darf nur verwendet werden, wenn Jobs aus AWS verwalteten Vorlagen erstellt werden. Das Objekt darf nicht für benutzerdefinierte ‚Auftragsvorlagen verwendet werden. Ein Beispiel, das zeigt, wie dieser Parameter verwendet wird, finden Sie unter Erstellen eines Auftrags mithilfe verwalteter Vorlagen.

```
{
    "templateName": "AWS-Download-File",
    "templateArn": "arn:aws:iot:region::jobtemplate/AWS-Download-File:1.0",
    "description": "A managed job template for downloading a file.",
    "templateVersion": "1.0",
    "environments": [
        "LINUX"
    ],
    "documentParameters": [
        {
```

```
            "key": "downloadUrl",
            "description": "URL of file to download.",
            "regex": "(.*?)",
            "example": "http://www.example.com/index.html",
            "optional": false
        },
        {
            "key": "filePath",
            "description": "Path on the device where downloaded file is written.",
            "regex": "(.*?)",
            "example": "/path/to/file",
            "optional": false
        },
        {
            "key": "runAsUser",
            "description": "Execute handler as another user. If not specified, then
 handler is executed as the same user as device client.",
            "regex": "(.){0,256}",
            "example": "user1",
            "optional": true
        },
        {
            "key": "pathToHandler",
            "description": "Path to handler on the device. If not specified, then
 device client will use the current working directory.",
            "regex": "(.){0,4096}",
            "example": "/path/to/handler/script",
            "optional": true
        }
    ],
    "document": "{\"version\":\"1.0\",\"steps\":[{\"action\":{\"name
\":\"Download-File\",\"type\":\"runHandler\",\"input\":{\"handler\":
\"download-file.sh\",\"args\":[\"${aws:iot:parameter:downloadUrl}\",
\"${aws:iot:parameter:filePath}\"],\"path\":\"${aws:iot:parameter:pathToHandler}\"},
\"runAsUser\":\"${aws:iot:parameter:runAsUser}\"}}]}"
}
```

Weitere Informationen finden Sie unter DescribeManagedJobTemplate.

Erstellen eines Auftrags mithilfe verwalteter Vorlagen

Der `create-job` AWS CLI Befehl kann verwendet werden, um einen Job aus einer Jobvorlage zu erstellen. Es zielt auf ein Gerät mit dem Namen `thing0ne` und gibt den Amazon-Ressourcennamen

(ARN) der verwalteten Vorlage an, die als Grundlage für den Job verwendet werden soll. Sie können erweiterte Konfigurationen wie Timeout- und Abbruchkonfigurationen überschreiben, indem Sie die zugehörigen Parameter des Befehls `create-job` übergeben.

Das Beispiel zeigt, wie ein Auftrag erstellt wird, der die Vorlage `AWS-Download-File` verwendet. Außerdem wird gezeigt, wie die Eingabeparameter der Vorlage mithilfe des Parameters `document-parameters` angegeben werden.

> **Note**
>
> Verwenden Sie das `document-parameters` Objekt nur mit AWS verwalteten Vorlagen. Dieses Objekt darf nicht mit benutzerdefinierten Auftragsvorlagen verwendet werden.

```
aws iot create-job \
   --targets arn:aws:iot:region:account-id:thing/thingOne \
   --job-id "new-managed-template-job" \
   --job-template-arn arn:aws:iot:region::jobtemplate/AWS-Download-File:1.0 \
   --document-parameters downloadUrl=https://example.com/index.html,filePath=path/to/
file
```

Wobei:

- *region*ist der AWS-Region.
- *account-id*ist die eindeutige AWS-Konto Zahl.
- *thingOne* ist der Name des IoT-Objekts, für das der Auftrag bestimmt ist.
- *AWS-Download-File:1.0*ist der Name der verwalteten Vorlage.
- `https://`*example.com/index*`.html`ist derURL, von dem die Datei heruntergeladen werden soll.
- `https://`*pathto/file/index* ist der Pfad auf dem Gerät, in dem die heruntergeladene Datei gespeichert werden soll.

Führen Sie den folgenden Befehl aus, um einen Auftrag für die Vorlage *AWS-Download-File* zu erstellen.

```
{
    "jobArn": "arn:aws:iot:region:account-id:job/new-managed-template-job",
    "jobId": "new-managed-template-job",
```

```
    "description": "A managed job template for downloading a file."
}
```

Erstellen Sie eine benutzerdefinierte Auftragsvorlage aus verwalteten Vorlagen

1. Erstellen Sie einen Auftrag mit einer verwalteten Vorlage, wie im vorherigen Abschnitt beschrieben.
2. Erstellen Sie eine benutzerdefinierte Jobvorlage, indem Sie die ARN des Jobs verwenden, den Sie erstellt haben. Weitere Informationen finden Sie unter Erstellen einer Auftragsvorlage anhand eines vorhandenen Auftrags.

## Erstellen von benutzerdefinierten Auftragsvorlagen

Sie können Jobvorlagen mithilfe der Konsole AWS CLI und der AWS IoT Konsole erstellen. Sie können Jobs auch anhand von Jobvorlagen erstellen, indem Sie die Webanwendungen AWS CLI, die AWS IoT Konsole und Fleet Hub for AWS IoT Device Management verwenden. Weitere Informationen zur Arbeit mit Jobvorlagen in Fleet Hub-Anwendungen finden Sie unter Arbeiten mit Jobvorlagen in Fleet Hub for AWS IoT Device Management.

> **Note**
>
> Die Gesamtzahl der Substitutionsmuster in einem Auftragsdokument sollte höchstens zehn betragen.

Themen

- Erstellen von benutzerdefinierten Auftragsvorlagen mit AWS Management Console
- Erstellen von benutzerdefinierten Auftragsvorlagen mit AWS CLI

### Erstellen von benutzerdefinierten Auftragsvorlagen mit AWS Management Console

In diesem Thema wird erklärt, wie Sie Jobvorlagen mithilfe der AWS IoT Konsole erstellen, löschen und Details zu diesen anzeigen können.

Erstellen einer benutzerdefinierten Auftragsvorlage

Sie können entweder eine ursprüngliche benutzerdefinierte Auftragsvorlage oder eine Auftragsvorlage aus einem vorhandenen Auftrag erstellen. Sie können auch eine benutzerdefinierte

Jobvorlage aus einem vorhandenen Job erstellen, der mit einer AWS verwalteten Vorlage erstellt wurde. Weitere Informationen finden Sie unter Erstellen Sie benutzerdefinierte Jobvorlagen aus verwalteten Vorlagen.

Erstellen einer ursprüngliche Auftragsvorlage

1. Beginnen mit der Erstellung Ihrer Jobvorlage

   1. Gehen Sie in der AWS IoT Konsole zum Hub Jobvorlagen und wählen Sie den Tab Benutzerdefinierte Vorlagen aus.
   2. Wählen Sie Auftragsvorlage erstellen.

   > **Note**
   >
   > Sie können auch von der Seite Verwandte Services unter Fleet Hub zur Seite Auftragsvorlagen navigieren.

2. Angeben der Eigenschaften der Auftragsvorlage

   Geben Sie auf der Seite Auftragsvorlage erstellen eine alphanumerische Kennung für Ihren Auftragsnamen und eine alphanumerische Beschreibung ein, um zusätzliche Informationen zur Vorlage bereitzustellen.

   > **Note**
   >
   > Wir raten davon ab, personenbezogene Daten in Ihren Stellenausschreibungen IDs oder Stellenbeschreibungen zu verwenden.

3. Angeben des Auftragsdokuments

   Stellen Sie eine JSON Auftragsdatei bereit, die entweder in einem S3-Bucket oder als Inline-Jobdokument gespeichert ist, das im Job angegeben ist. Diese Auftragsdatei wird zum Auftragsdokument, wenn Sie einen Auftrag mit dieser Vorlage erstellen.

   Wenn die Job-Datei in einem S3-Bucket gespeichert ist, geben Sie S3 ein URL oder wählen Sie Browse S3, navigieren Sie dann zu Ihrem Job-Dokument und wählen Sie es aus.

> **Note**
>
> Sie können nur S3-Buckets in Ihrer aktuellen Region auswählen.

4. Fügen Sie weitere Konfigurationen für Ihren Auftrag hinzu und überprüfen und erstellen Sie dann Ihren Auftrag. Weitere Informationen zu den zusätzlichen optionalen Konfigurationen finden Sie unter den folgenden Links:

   - Konfigurationen für Auftrags-Rollout, Planung und Abbruch
   - Timeout bei der Auftragsausführung und Wiederholungskonfigurationen

Erstellen einer Auftragsvorlage anhand eines vorhandenen Auftrags

1. Wählen Sie Ihren Schlüssel aus.

   1. Gehen Sie zum Job-Hub der AWS IoT Konsole und wählen Sie den Job aus, den Sie als Grundlage für Ihre Jobvorlage verwenden möchten.
   2. Wählen Sie Als Auftragsvorlage speichern aus.

> **Note**
>
> Optional können Sie ein anderes Auftragsdokument auswählen oder die erweiterten Konfigurationen des ursprünglichen Auftrags bearbeiten und dann die Option Jobvorlage erstellen auswählen. Ihre neue Auftragsvorlage wird auf der Seite Auftragsvorlagen angezeigt.

2. Angeben der Eigenschaften der Auftragsvorlage

   Geben Sie auf der Seite Auftragsvorlage erstellen eine alphanumerische Kennung für Ihren Auftragsnamen und eine alphanumerische Beschreibung ein, um zusätzliche Informationen zur Vorlage bereitzustellen.

> **Note**
>
> Das Auftragsdokument ist die Auftragsdatei, die Sie bei der Erstellung der Vorlage angegeben haben. Wenn das Auftragsdokument innerhalb des Auftrags und nicht an

einem S3-Speicherort angegeben ist, können Sie das Auftragsdokument auf der Seite Details für diesen Auftrag sehen.

3. Fügen Sie weitere Konfigurationen für Ihren Auftrag hinzu und überprüfen und erstellen Sie dann Ihren Auftrag. Weitere Informationen zum Arbeiten mit zusätzlichen Konfigurationen finden Sie unter:

   - Konfigurationen für Auftrags-Rollout, Planung und Abbruch
   - Timeout bei der Auftragsausführung und Wiederholungskonfigurationen

Erstellen eines Auftrags anhand einer benutzerdefinierten Auftragsvorlage

Sie können einen Auftrag anhand einer benutzerdefinierten Auftragsvorlage erstellen, indem Sie die Seite Details Ihrer Auftragsvorlage aufrufen, wie in diesem Thema beschrieben. Sie können auch einen Auftrag erstellen oder die Auftragsvorlage auswählen, die Sie bei der Ausführung des Workflows zur Auftragserstellung verwenden möchten. Weitere Informationen finden Sie unter Erstellen und Verwalten von Aufträgen mithilfe von AWS Management Console.

In diesem Thema wird gezeigt, wie Sie einen Auftrag von der Seite Details einer benutzerdefinierten Auftragsvorlage aus erstellen. Sie können einen Job auch aus einer AWS verwalteten Vorlage erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen Auftrag mit verwalteten Vorlagen.

1. Auswählen Ihrer benutzerdefinierten Auftragsvorlage

   Gehen Sie in der AWS IoT Konsole zum Hub Jobvorlagen, wählen Sie den Tab Benutzerdefinierte Vorlagen und wählen Sie dann Ihre Vorlage aus.

2. Erstellen eines Auftrags mit Ihrer benutzerdefinierten Vorlage

   So erstellen Sie einen Auftrag:

   1. Wählen Sie auf der Seite Details Ihrer Vorlage die Option Auftrag erstellen aus.

      Die Konsole wechselt zum Schritt Benutzerdefinierte Auftragseigenschaften des Workflows Auftrag erstellen, in dem Ihre Vorlagenkonfiguration hinzugefügt wurde.

   2. Geben Sie einen eindeutigen alphanumerischen Auftragsnamen sowie optional eine Beschreibung und Tags ein und wählen Sie dann Weiter aus.

3. Wählen Sie die Objekte oder Objektgruppen als Auftragsziele aus, die Sie in diesem Auftrag ausführen möchten.

   Im Bereich Auftragsdokument wird Ihre Vorlage mit ihren Konfigurationseinstellungen angezeigt. Wenn Sie ein anderes Auftragsdokument verwenden möchten, wählen Sie Durchsuchen und wählen Sie einen anderen Bucket und ein anderes Dokument aus. Wählen Sie Weiter aus.

4. Wählen Sie auf der Seite Auftragskonfiguration den Auftragstyp als kontinuierlichen Auftrag oder Snapshot-Auftrag aus. Ein Snapshot-Auftrag ist abgeschlossen, wenn er seine Ausführung auf den Zielgeräten und Zielgruppen abgeschlossen hat. Ein kontinuierlicher Auftrag gilt für Objektgruppen und wird auf jedem Gerät ausgeführt, das Sie einer bestimmten Zielgruppe hinzufügen.

5. Fügen Sie weitere Konfigurationen für Ihren Auftrag hinzu und überprüfen und erstellen Sie dann Ihren Auftrag. Weitere Informationen zum Arbeiten mit zusätzlichen Konfigurationen finden Sie unter:

   - Konfigurationen für Auftrags-Rollout, Planung und Abbruch
   - Timeout bei der Auftragsausführung und Wiederholungskonfigurationen

> **Note**
>
> Wenn ein anhand einer Auftragsvorlage erstellter Auftrag die vorhandenen Parameter aktualisiert, die in der Auftragsvorlage bereitgestellt werden, überschreiben diese aktualisierten Parameter die vorhandenen Parameter, die in der Auftragsvorlage für diesen Auftrag bereitgestellt wurden.

Mit Fleet Hub-Webanwendungen können Sie Aufträge auch anhand von Auftragsvorlagen erstellen. Informationen zum Erstellen von Aufträgen in Fleet Hub finden Sie unter Arbeiten mit Auftragsvorlagen in Fleet Hub for AWS IoT Device Management.

Löschen einer Auftragsvorlage

Um eine Jobvorlage zu löschen, gehen Sie zunächst zum Hub Jobvorlagen der AWS IoT Konsole und wählen Sie den Tab Benutzerdefinierte Vorlagen. Wählen Sie die zu löschende Vorlage aus und klicken Sie auf Löschen.

> **Note**
>
> Eine Löschung ist dauerhaft und die Auftragsvorlage wird nicht mehr auf der Registerkarte Benutzerdefinierte Vorlagen angezeigt.

## Erstellen von benutzerdefinierten Auftragsvorlagen mit AWS CLI

In diesem Thema wird erklärt, wie Sie Details erstellen und löschen können und wie Sie Details zu Auftragsvorlagen mithilfe von AWS CLI abrufen können.

Erstellen einer von Grund auf neuen Auftragsvorlage

Der folgende AWS CLI Befehl zeigt, wie Sie einen Job mithilfe eines in einem S3-Bucket gespeicherten Auftragsdokuments (*job-document.json*) und einer Rolle mit der Berechtigung zum Herunterladen von Dateien von Amazon S3 (*S3DownloadRole*) erstellen.

```
aws iot create-job-template  \
      --job-template-id 010  \
      --description "My custom job template for updating the device firmware"
      --document-source https://s3.amazonaws.com/amzn-s3-demo-bucket/job-document.json
 \
      --timeout-config inProgressTimeoutInMinutes=100 \
      --job-executions-rollout-config "{ \"exponentialRate\": { \"baseRatePerMinute\":
 50, \"incrementFactor\": 2, \"rateIncreaseCriteria\": { \"numberOfNotifiedThings\":
 1000, \"numberOfSucceededThings\": 1000}}, \"maximumPerMinute\": 1000}" \
      --abort-config "{ \"criteriaList\": [ { \"action\": \"CANCEL\", \"failureType
\": \"FAILED\", \"minNumberOfExecutedThings\": 100, \"thresholdPercentage\": 20},
 { \"action\": \"CANCEL\", \"failureType\": \"TIMED_OUT\", \"minNumberOfExecutedThings
\": 200, \"thresholdPercentage\": 50}]}" \
      --presigned-url-config "{\"roleArn\":\"arn:aws:iam::123456789012:role/
S3DownloadRole\", \"expiresInSec\":3600}"
```

Der optionale Parameter `timeout-config` gibt die Dauer an, die jedes Gerät für den Abschluss der Ausführung des Auftrags hat. Der Timer wird gestartet, wenn der Status der Auftragsausführung auf `IN_PROGRESS` gesetzt wird. Wird der Status der Auftragsausführung vor Ablauf der Zeit nicht auf einen anderen abschließenden Status festgelegt, wird er automatisch auf `TIMED_OUT` festgelegt.

Der Timer „In Bearbeitung“ kann nicht aktualisiert werden und gilt für alle Auftragsausführungen für den Auftrag. Immer wenn ein Jobstart länger als dieses Intervall im `IN_PROGRESS` Status verbleibt, schlägt der Jobstart fehl und wechselt in den `TIMED_OUT` Terminalstatus. AWS IoT veröffentlicht auch eine MQTT Benachrichtigung.

Weitere Informationen zum Konfigurieren von Auftragsrollouts und Auftragsabbrüchen finden Sie unter Auftragsrollout- und Abbruchkonfiguration.

> **Note**
>
> Auftragsdokumente, die als Amazon-S3-Dateien angegeben sind, werden zum Zeitpunkt der Erstellung des Auftrags abgerufen. Änderungen der Inhalte der Amazon-S3-Datei, die als Quelle Ihres Auftragsdokuments verwendet werden, nachdem Sie den Auftrag erstellt haben, ändern nicht, was an die Ziele des Auftrags gesendet wird.

Erstellen einer Auftragsvorlage anhand eines vorhandenen Auftrags

Der folgende AWS CLI Befehl erstellt eine Jobvorlage, indem der Amazon-Ressourcenname (ARN) eines vorhandenen Jobs angegeben wird. Die neue Auftragsvorlage verwendet alle im Auftrag angegebenen Konfigurationen. Optional können Sie jede der Konfigurationen im vorhandenen Auftrag ändern, indem Sie einen der optionalen Parameter verwenden.

```
aws iot create-job-template  \
      --job-arn arn:aws:iot:region:123456789012:job/job-name  \
      --timeout-config inProgressTimeoutInMinutes=100
```

Abrufen von Details einer Aufgabenvorlage

Der folgende AWS CLI Befehl ruft Details zu einer angegebenen Jobvorlage ab.

```
aws iot describe-job-template \
      --job-template-id template-id
```

Die Ausgabe des Befehls sieht wie folgt aus:

```
{
   "abortConfig": {
      "criteriaList": [
         {
            "action": "string",
            "failureType": "string",
            "minNumberOfExecutedThings": number,
            "thresholdPercentage": number
         }
      ]
   },
   "createdAt": number,
   "description": "string",
   "document": "string",
   "documentSource": "string",
   "jobExecutionsRolloutConfig": {
      "exponentialRate": {
         "baseRatePerMinute": number,
         "incrementFactor": number,
         "rateIncreaseCriteria": {
            "numberOfNotifiedThings": number,
            "numberOfSucceededThings": number
         }
      },
      "maximumPerMinute": number
   },
   "jobTemplateArn": "string",
   "jobTemplateId": "string",
   "presignedUrlConfig": {
      "expiresInSec": number,
      "roleArn": "string"
   },
   "timeoutConfig": {
      "inProgressTimeoutInMinutes": number
   }
}
```

### Auflisten der Auftragsvorlagen

Der folgende AWS CLI Befehl listet alle Jobvorlagen in Ihrer auf AWS-Konto.

```
aws iot list-job-templates
```

Die Ausgabe des Befehls sieht wie folgt aus:

```
{
   "jobTemplates": [
      {
         "createdAt": number,
         "description": "string",
         "jobTemplateArn": "string",
         "jobTemplateId": "string"
      }
   ],
   "nextToken": "string"
}
```

Verwenden Sie den Wert des Feldes `nextToken`, um weitere Ergebnisseiten abzurufen.

Löschen einer Auftragsvorlage

Der folgende AWS CLI Befehl löscht eine angegebene Jobvorlage.

```
aws iot delete-job-template \
      --job-template-id template-id
```

Der Befehl zeigt keine Ausgabe an.

Erstellen eines Auftrags anhand einer benutzerdefinierten Auftragsvorlage

Der folgende AWS CLI Befehl erstellt einen Job aus einer benutzerdefinierten Jobvorlage. Es zielt auf ein Gerät mit dem Namen `thing0ne` und gibt den Amazon-Ressourcennamen (ARN) der Jobvorlage an, die als Grundlage für den Job verwendet werden soll. Sie können erweiterte Konfigurationen wie Timeout- und Abbruchkonfigurationen überschreiben, indem Sie die zugehörigen Parameter des Befehls `create-job` übergeben.

> **Warning**
>
> Das Objekt `document-parameters` darf nur zusammen mit dem Befehl `create-job` verwendet werden, wenn Aufträge aus AWS -verwalteten Vorlagen erstellt werden. Dieses Objekt darf nicht mit benutzerdefinierten Auftragsvorlagen verwendet werden. Ein Beispiel, das zeigt, wie Aufträge mit diesem Parameter erstellt werden, finden Sie unter Erstellen eines Auftrags mithilfe verwalteter Vorlagen.

```
aws iot create-job \
      --targets arn:aws:iot:region:123456789012:thing/thingOne  \
      --job-template-arn arn:aws:iot:region:123456789012:jobtemplate/template-id
```

# Auftrags--Konfigurationen

Sie können für jeden Auftrag, den Sie für die angegebenen Ziele bereitstellen, die folgenden zusätzlichen Konfigurationen verwenden.

- Rollout: Definiert, wie viele Geräte das Auftragsdokument pro Minute erhalten.
- Planung: Plant einen Auftrag für ein future Datum und eine zukünftige Uhrzeit und verwendet zusätzlich wiederkehrende Wartungsfenster.
- Abbrechen: Bricht einen Auftrag ab, z. B. wenn einige Geräte die Auftragsbenachrichtigung nicht erhalten oder wenn Ihre Geräte bei der Auftragsausführung einen Fehler melden.
- Timeout: Wenn Ihre Auftragsziele innerhalb einer bestimmten Zeit nach Beginn der Auftragsausführung keine Antwort erhalten, kann der Auftrag fehlschlagen.
- Erneut versuchen: Wiederholt die Auftragsausführung, wenn Ihr Gerät beim Versuch, eine Auftragsausführung abzuschließen, einen Fehler meldet oder wenn bei der Auftragsausführung ein Timeout auftritt.

Mithilfe dieser Konfigurationen können Sie den Status Ihrer Auftragsausführung überwachen und verhindern, dass ein fehlerhaftes Update an die gesamte Flotte gesendet wird.

Themen


- Wie funktionieren Auftragskonfigurationen
- Zusätzliche Konfigurationen angeben

# Wie funktionieren Auftragskonfigurationen

Sie verwenden die Rollout- und Abbruchkonfigurationen, wenn Sie einen Auftrag bereitstellen, und die Timeout- und Wiederholungskonfigurationen für die Auftragsausführung. In den folgenden Abschnitten finden Sie weitere Informationen zur Funktionsweise dieser Konfigurationen.

Themen


- Konfigurationen für Auftrags-Rollout, Planung und Abbruch
- Timeout bei der Auftragsausführung und Wiederholungskonfigurationen


## Konfigurationen für Auftrags-Rollout, Planung und Abbruch

Mithilfe der Konfigurationen für Auftrags-Rollout, Planung und Abbruch können Sie festlegen, wie viele Geräte das Auftragsdokument erhalten, einen Auftrags-Rollout planen und die Kriterien für das Abbrechen eines Auftrags festlegen.

Konfiguration des Auftrags-Rollouts

Sie können angeben, wie schnell die Ziele über eine ausstehende Auftragsausführung benachrichtigt werden. Sie können auch ein gestaffeltes Rollout erstellen, um Updates, Neustarts und andere Vorgänge zu verwalten. Um festzulegen, wie Ihre Ziele benachrichtigt werden, verwenden Sie die Auftrags-Rollout-Raten.

Auftragsrolloutraten

Sie können eine Rollout-Konfiguration erstellen, indem Sie entweder eine konstante Rollout-Rate oder eine exponentielle Rollout-Rate verwenden. Verwenden Sie eine konstante Rollout-Rate, um die maximale Anzahl von Auftragszielen festzulegen, die pro Minute informiert werden sollen.

AWS IoT Jobs können mit exponentiellen Rollout-Raten bereitgestellt werden, wenn verschiedene Kriterien und Schwellenwerte erfüllt werden. Wenn die Anzahl der fehlgeschlagenen Aufträge einer Reihe von Kriterien entspricht, die Sie angeben, können Sie den Auftrags-Rollout abbrechen. Sie legen die Kriterien für die Auftrags-Rollout-Rate fest, wenn Sie mithilfe des `JobExecutionsRolloutConfig`-Objekts einen Auftrag erstellen. Sie legen auch die Kriterien für den Auftragsabbruch bei der Auftragserstellung fest, indem Sie das `AbortConfig`-Objekt verwenden.

Das folgende Beispiel zeigt, wie die Rollout-Raten funktionieren. Beispielsweise würde ein Auftrags-Rollout mit einer Basisrate von 50 pro Minute, einem Inkrementfaktor von 2 und einer Anzahl von

jeweils 1.000 Geräten, die benachrichtigt und erfolgreich waren, wie folgt funktionieren: Der Auftrag beginnt mit einer Geschwindigkeit von 50 Auftragsausführungen pro Minute und wird mit dieser Geschwindigkeit fortgesetzt, bis entweder 1.000 Objekte Benachrichtigungen zur Auftragsausführung erhalten haben oder 1.000 erfolgreiche Auftragsausführungen stattgefunden haben.

Die folgende Tabelle zeigt, wie der Rollout über die ersten vier Inkremente verläuft.

| Rolloutrate pro Minute | 50 | 100 | 200 | 400 |
|---|---|---|---|---|
| Anzahl der benachrichtigten Geräte oder der erfolgreichen Auftragsausführungen, um einer erhöhten Rate gerecht zu werden | 1.000 | 2.000 | 3,000 | 4.000 |

> **Note**
>
> Wenn Sie Ihr maximales Limit von 500 Aufträgen (`isConcurrent = True`) erreicht haben, behalten alle aktiven Aufträge den Status `IN-PROGRESS` und führen keine neuen Auftragsausführungen durch, bis die Anzahl der gleichzeitigen Aufträge 499 oder weniger beträgt (`isConcurrent = False`). Dies gilt für Snapshots und kontinuierliche Aufträge. Falls `isConcurrent = True`, führt der Auftrag derzeit Auftragsausführungen auf allen Geräten Ihrer Zielgruppe durch. Falls `isConcurrent = False`, hat der Auftrag den Rollout aller Auftragsausführungen auf allen Geräten in Ihrer Zielgruppe abgeschlossen. Der Status wird aktualisiert, sobald alle Geräte in Ihrer Zielgruppe einen Terminal-Zustand erreicht haben, oder wenn Sie eine Konfiguration für den Auftragsabbruch ausgewählt haben, einen bestimmten Schwellenwert für Ihre Zielgruppe erreicht haben. Der Status auf Auftragsebene `isConcurrent = False` gibt für `isConcurrent = True` und beide `IN_PROGRESS` an. Weitere Informationen zu den Limits für aktive und gleichzeitige Aufträge finden Sie unter Limits für aktive und gleichzeitige Aufträge.

Auftrags-Rollout-Raten für kontinuierliche Aufträge mit dynamischen Objektgruppen

Wenn Sie einen kontinuierlichen Job verwenden, um Fernoperationen in Ihrer Flotte einzuführen, führt AWS IoT Jobs die Ausführung von Jobs für Geräte in Ihrer Zielgruppe durch. Bei neuen Geräten, die der dynamischen Objektgruppe hinzugefügt werden, werden diese

Auftragsausführungen auch nach der Erstellung des Auftrags weiterhin auf diesen Geräten ausgeführt.

Mit der Rollout-Konfiguration können die Rollout-Raten nur für Geräte gesteuert werden, die der Gruppe hinzugefügt werden, bis der Auftrag erstellt wird. Nachdem ein Auftrag erstellt wurde, werden die Auftragsausführungen für alle neuen Geräte nahezu in Echtzeit erstellt, sobald die Geräte der Zielgruppe beitreten.

Konfiguration der Auftragsplanung

Sie können einen kontinuierlichen Auftrag oder einen Snapshot-Auftrag bis zu einem Jahr im Voraus planen und dabei eine vorher festgelegte Startzeit, Endzeit und ein Endverhalten angeben, was mit jeder Auftragsausführung nach Erreichen der Endzeit geschehen soll. Darüber hinaus können Sie ein optionales wiederkehrendes Wartungsfenster mit flexibler Häufigkeit, Startzeit und Dauer für fortlaufende Aufträge einrichten, um ein Auftragsdokument auf allen Geräten innerhalb der Zielgruppe bereitzustellen.

Konfigurationen für die Auftragsplanung

Startzeit

Die Startzeit eines geplanten Auftrags ist das zukünftige Datum und die Uhrzeit, zu der der Auftrag mit der Bereitstellung des Auftragsdokuments auf allen Geräten in der Zielgruppe beginnt. Die Startzeit für einen geplanten Auftrag gilt für fortlaufende Aufträge und Snapshot-Aufträge. Wenn ein geplanter Auftrag zum ersten Mal erstellt wird, behält er den Status `SCHEDULED`. Sobald das von Ihnen gewählte `startTime` erreicht ist, wird es aktualisiert auf `IN_PROGRESS` und der Rollout des Auftragsdokuments wird gestartet. Der Zeitraum zwischen dem ursprünglichen Datum und der Uhrzeit, zu der Sie den geplanten Auftrag erstellt haben, `startTime` darf nicht länger als ein Jahr sein.

Weitere Informationen zur Syntax `startTime` bei der Verwendung eines API-Befehls oder des AWS CLI finden Sie unter Timestamp.

Bei einem Auftrag mit der optionalen Planungskonfiguration, der während eines wiederkehrenden Wartungsfensters an einem Ort mit Sommerzeit ausgeführt wird, ändert sich die Uhrzeit um eine Stunde, wenn von Sommerzeit auf Normalzeit und von Normalzeit auf Sommerzeit umgestellt wird.

> **Note**
>
> Die in der angezeigte Zeitzone AWS Management Console ist Ihre aktuelle Systemzeitzone. Diese Zeitzonen werden jedoch im System in UTC umgerechnet.

Endzeit

Die Endzeit eines geplanten Auftrags ist das zukünftige Datum und die Uhrzeit, zu der der Auftrag das Rollout des Auftragsdokuments an alle verbleibenden Geräte in der Zielgruppe beendet. Die Endzeit für einen geplanten Auftrag gilt für fortlaufende Aufträge und Snapshot-Aufträge. Wenn ein geplanter Auftrag beim ausgewählten `endTime` eintrifft und alle Auftragsausführungen einen Terminal-Zustand erreicht haben, wird sein Status von `IN_PROGRESS` auf `COMPLETED` aktualisiert. Der Zeitraum zwischen dem ursprünglichen Datum und der Uhrzeit, zu der Sie den geplanten Auftrag erstellt haben, `endTime` darf nicht länger als ein Jahr sein. Die Mindestdauer zwischen `startTime` und `endTime` beträgt 30 Minuten. Wiederholungsversuche bei der Auftragsausführung werden durchgeführt, bis der Auftrag den `endTime` erreicht, dann bestimmt der `endBehavior`, wie weiter vorzugehen ist.

Weitere Informationen zur Syntax `endTime` bei der Verwendung eines API-Befehls oder des AWS CLI finden Sie unter Timestamp.

Bei einem Auftrag mit der optionalen Planungskonfiguration, der während eines wiederkehrenden Wartungsfensters an einem Ort mit Sommerzeit ausgeführt wird, ändert sich die Uhrzeit um eine Stunde, wenn von Sommerzeit auf Normalzeit und von Normalzeit auf Sommerzeit umgestellt wird.

> **Note**
>
> Die in der angezeigte Zeitzone AWS Management Console ist Ihre aktuelle Systemzeitzone. Diese Zeitzonen werden jedoch im System in UTC umgerechnet.

Verhalten beenden

Das Endverhalten eines geplanten Auftrags bestimmt, was mit dem Auftrag und allen noch nicht abgeschlossenen Auftragsausführungen passiert, wenn der Auftrag den ausgewählten `endTime` erreicht.

Im Folgenden sind die Endverhaltensweisen aufgeführt, aus denen Sie bei der Erstellung des Auftrags oder der Auftragsvorlage wählen können:

- `STOP_ROLLOUT`
  - `STOP_ROLLOUT` stoppt den Rollout des Auftragsdokuments auf allen verbleibenden Geräten in der Zielgruppe für den Auftrag. Darüber hinaus werden alle `QUEUED`- und `IN_PROGRESS`-Aufträge so lange ausgeführt, bis sie den Terminal-Zustand erreicht haben. Dies ist das standardmäßige Endverhalten, sofern Sie nicht `CANCEL` oder `FORCE_CANCEL` auswählen.
- `CANCEL`
  - `CANCEL` stoppt den Rollout des Auftragsdokuments auf allen verbleibenden Geräten in der Zielgruppe für den Auftrag. Darüber hinaus werden alle `QUEUED` Auftragsausführungen abgebrochen, während alle `IN_PROGRESS` Auftragsausführungen fortgesetzt werden, bis sie einen Terminal-Zustand erreichen.
- `FORCE_CANCEL`
  - `FORCE_CANCEL` stoppt den Rollout des Auftragsdokuments auf allen verbleibenden Geräten in der Zielgruppe für den Auftrag. Darüber hinaus werden alle `QUEUED`- und `IN_PROGRESS`-Auftragsausführungen storniert.

> **Note**
>
> Um eine auszuwählen`endbehavior`, müssen Sie eine auswählen `endtime`

Max. Dauer

Die Höchstdauer eines geplanten Auftrags muss unabhängig von `startTime` und `endTime` unter zwei Jahren liegen.

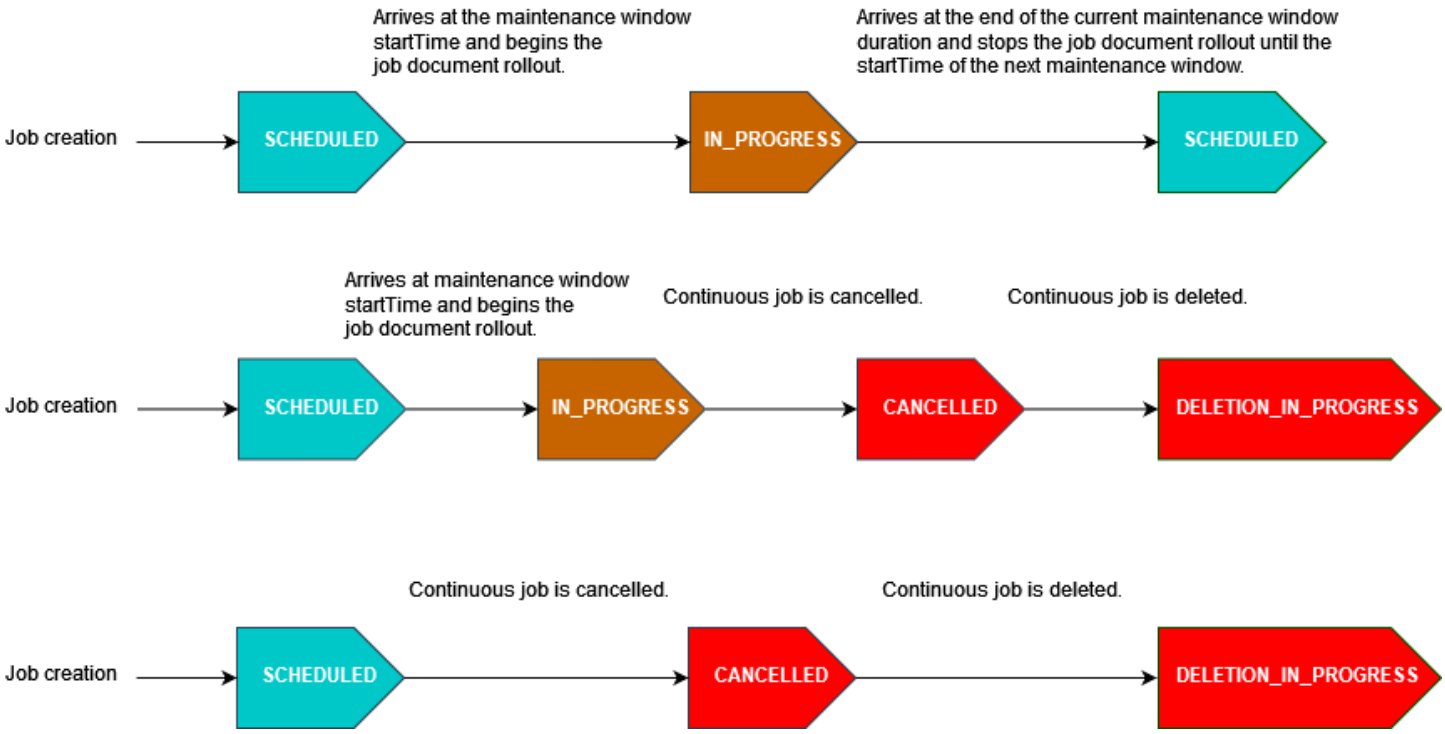
In der folgenden Tabelle sind die häufigsten Dauerszenarien für einen geplanten Auftrag aufgeführt:

| Beispielnummer für einen geplanten Auftrag | startTime | endTime | Max. Dauer |
|---|---|---|---|
| 1 | Unmittelbar nach der ersten Auftragserstellung. | Ein Jahr nach der ersten Auftragserstellung. | Ein Jahr |
| 2 | Ein Monat nach der ersten Schaffung von Arbeitsplätzen. | 13 Monate nach der ersten Schaffung von Arbeitsplätzen. | Ein Jahr |
| 3 | Ein Jahr nach der ersten Auftragserstellung. | Zwei Jahre nach der ersten Auftragserstellung. | Ein Jahr |
| 4 | Unmittelbar nach der ersten Auftragserstellung. | Zwei Jahre nach der ersten Auftragserstellung. | Zwei Jahre |

Wiederkehrendes Wartungsfenster

Das Wartungsfenster ist eine optionale Konfiguration innerhalb der Planungskonfiguration der APIs AWS Management Console und `SchedulingConfig` innerhalb der `CreateJobTemplate` APIs `CreateJob` und. Sie können ein wiederkehrendes Wartungsfenster mit einer festgelegten Startzeit, Dauer und Häufigkeit (täglich, wöchentlich oder monatlich) einrichten. Wartungsfenster gelten nur für fortlaufende Aufträge. Die maximale Dauer eines wiederkehrenden Wartungsfensters beträgt 23 Stunden und 50 Minuten.

Das folgende Diagramm zeigt den Status der Aufträge für verschiedene geplante Auftragsszenarien mit einem optionalen Wartungsfenster:




Weitere Informationen zu Auftragsstatus finden Sie unter [Aufträge und Status der Auftragsausführung](#).

> **Note**
>
> Wenn ein Auftrag `endTime` während eines Wartungsfensters am eingeht, wird er von `IN_PROGRESS` bis `COMPLETED` aktualisiert. Darüber hinaus folgen alle verbleibenden Auftragsausführungen dem `endBehavior` für den Auftrag.

### Cron-Ausdrücke

Bei geplanten Aufträgen, bei denen das Auftragsdokument während eines Wartungsfensters mit einer benutzerdefinierten Häufigkeit ausgeführt wird, wird die benutzerdefinierte Häufigkeit mithilfe eines Cron-Ausdrucks eingegeben. Ein Cron-Ausdruck verfügt über sechs Pflichtfelder, die durch Leerzeichen voneinander getrennt sind.

#### Syntax

```
cron(fields)
```

| Feld | Werte | Platzhalter |
| --- | --- | --- |
| Minuten | 0-59 | , - * / |
| Stunden | 0-23 | , - * / |
| D ay-of-month | 1-31 | , - * ? / L W |
| Monat | 1-12 oder JAN-DEC | , - * / |
| D ay-of-week | 1-7 oder SUN-SAT | , - * ? / L # |
| Jahr | 1970-2199 | , - * / |

Platzhalter

- Das Platzhalterzeichen , (Komma) schließt zusätzliche Werte ein. Im Feld "Monat" steht JAN, FEB, MAR für Januar, Februar und März.
- Das Platzhalterzeichen - (Bindestrich) gibt einen Bereich an. Im Feld "Tag" steht 1-15 für die Tage 1 bis 15 des angegebenen Monats.
- Das Platzhalterzeichen * (Sternchen) steht für alle Werte im Feld. Im Feld für die Stundenangaben steht * für alle Stunden. Sie können * nicht sowohl in den ay-of-week Feldern D als ay-of-month auch in D verwenden. Wenn Sie es in einem der Felder eingeben, müssen Sie im anderen Feld ein ? verwenden.
- Das Platzhalterzeichen / (Schrägstrich) steht für schrittweise Steigerungen. Im Feld "Minuten" können Sie 1/10 eingeben, um einen Bereich von je 10 Minuten beginnend mit der ersten Minute der Stunde anzugeben (z. B. die 11., 21. und 31. Minute usw.).
- Das Platzhalterzeichen ? (Fragezeichen) steht für einen Wert. In das ay-of-month D-Feld könnten Sie 7 eingeben, und wenn es Ihnen egal wäre, welcher Wochentag der 7. ist, könnten Sie eingeben? im ay-of-week D-Feld.
- Der Platzhalter L in den ay-of-week Feldern D ay-of-month oder D gibt den letzten Tag des Monats oder der Woche an.
- Der **`W`** Platzhalter im ay-of-month D-Feld gibt einen Wochentag an. **`3W`**Gibt im ay-of-month Feld D den Wochentag an, der dem dritten Tag des Monats am nächsten liegt.
- Der Platzhalter # im ay-of-week Feld D gibt eine bestimmte Instanz des angegebenen Wochentags innerhalb eines Monats an. Beispiel: 3#2 steht für den zweiten Dienstag des Monats: Die 3 bezieht

sich auf Dienstag, da dies der dritte Tag jeder Woche ist, und die 2 bezieht sich auf den zweiten Tag dieses Typs innerhalb des Monats.

> **Note**
>
> Wenn Sie das Zeichen '#' verwenden, können Sie nur einen Ausdruck in dem day-of-week Feld definieren. Beispiel, `"3#1,6#3"` ist ungültig, da es als zwei Ausdrücke interpretiert wird.

Einschränkungen

- Sie können die ay-of-week Felder D ay-of-month und D nicht in demselben Cron-Ausdruck angeben. Wenn Sie einen Wert (oder einen *) in einem der Felder angeben, müssen Sie in dem anderen Feld ein ? eingeben.

Beispiele

Wenn Sie einen Cron-Ausdruck für ein wiederkehrendes Wartungsfenster verwenden, können Sie sich auf die folgenden Beispiele für `startTime` beziehen.

| Minuten | Stunden | Tag des Monats | Monat | Wochentag | Jahr | Bedeutung |
|---|---|---|---|---|---|---|
| 0 | 10 | * | * | ? | * | Ausführung jeden Tag um 10:00 Uhr (UTC) |
| 15 | 12 | * | * | ? | * | Ausführung jeden Tag um 12:15 Uhr (UTC) |
| 0 | 18 | ? | * | MO-FR | * | Ausführung jeden |

| Minuten | Stunden | Tag des Monats | Monat | Wochentag | Jahr | Bedeutung |
|---|---|---|---|---|---|---|
| | | | | | | Montag bis Freitag um 18:00 Uhr (UTC) |
| 0 | 8 | 1 | * | ? | * | Ausführung jeden 1. Tag des Monats um 08:00 Uhr (UTC) |

Logik für die Dauer des wiederkehrenden Wartungsfensters

Wenn ein Auftrags-Rollout während eines Wartungsfensters das Ende des aktuellen Wartungsfensters erreicht, werden die folgenden Aktionen ausgeführt:

- Der Auftrag beendet alle Rollouts des Auftragsdokuments auf allen verbleibenden Geräten in Ihrer Zielgruppe. Es wird mit dem `startTime` des nächsten Wartungsfensters fortgesetzt.
- Alle Auftragsausführungen mit dem Status `QUEUED` bleiben `QUEUED` bis zum `startTime` des nächsten Wartungsfenster. Im nächsten Fenster können sie zu dem `IN_PROGRESS` wechseln, zu dem das Gerät bereit ist, mit der Ausführung der im Auftragsdokument angegebenen Aktionen zu beginnen.
- Alle Auftragsausführungen mit dem Status `IN_PROGRESS` setzen die Ausführung der im Auftragsdokument angegebenen Aktionen fort, bis sie den Terminal-Zustand erreichen. Alle Wiederholungsversuche, wie unter `JobExecutionsRetryConfig` beschrieben, finden mit dem `startTime` des nächsten Wartungsfensters statt.

Konfiguration des Auftragsabbruchs

Verwenden Sie diese Konfiguration, um Kriterien für das Abbrechen eines Auftrags zu erstellen, wenn ein bestimmter Prozentsatz von Geräten diese Kriterien erfüllt. Mit dieser Konfiguration können Sie beispielsweise einen Auftrag in den folgenden Fällen stornieren:

- Wenn ein bestimmter Prozentsatz von Geräten keine Benachrichtigungen zur Auftragsausführung erhält, z. B. wenn Ihr Gerät für ein Over-The-Air (OTA)-Update nicht kompatibel ist. In diesem Fall kann Ihr Gerät einen `REJECTED`-Status melden.
- Wenn ein bestimmter Prozentsatz von Geräten Fehler bei der Auftragsausführung meldet, z. B. wenn Ihr Gerät beim Versuch, das Auftragsdokument von einer Amazon S3-URL herunterzuladen, auf eine Verbindungsunterbrechung stößt. In solchen Fällen muss Ihr Gerät so programmiert sein, dass es den `FAILURE`-Status an AWS IoT meldet.
- Wenn ein `TIMED_OUT`-Status gemeldet wird, weil die Auftragsausführung nach dem Start der Auftragsausführung für einen bestimmten Prozentsatz von Geräten ein Timeout überschreitet.
- Wenn mehrere Wiederholungsversuche fehlgeschlagen sind. Wenn Sie eine Wiederholungskonfiguration hinzufügen, können für jeden erneuten Versuch zusätzliche Kosten für Ihr AWS-Konto anfallen. In solchen Fällen kann das Abbrechen des Auftrags die Ausführung von Aufträgen in der Warteschlange abbrechen und Wiederholungsversuche für diese Ausführungen verhindern. Weitere Informationen zur Wiederholungskonfiguration und deren Verwendung zusammen mit der Abbruchkonfiguration finden Sie unter Timeout bei der Auftragsausführung und Wiederholungskonfigurationen.

Sie können mithilfe der AWS IoT Konsole oder der Jobs-API eine Abbruchbedingung für einen AWS IoT Job einrichten.

## Timeout bei der Auftragsausführung und Wiederholungskonfigurationen

Verwenden Sie die Timeout-Konfiguration für die Auftragsausführung, um Ihnen eine Auftragsbenachrichtigungen zu senden, wenn eine Auftragsausführung länger als die festgelegte Dauer andauert. Verwenden Sie die Konfiguration für die Wiederholung der Auftragsausführung, um die Ausführung erneut zu versuchen, wenn der Auftrag fehlschlägt oder das Timeout überschritten wird.

### Timeout-Konfiguration für die Auftragsausführung

Verwenden Sie die Konfiguration für die Zeitüberschreitung bei der Auftragsausführung, um Sie zu benachrichtigen, wenn ein Auftrag für einen unerwartet langen Zeitraum im Status `IN_PROGRESS` stecken bleibt. Wenn der Auftrag `IN_PROGRESS` ist, können Sie den Fortschritt Ihrer Auftragsausführung überwachen.

### Timer für Auftrags-Timeouts

Es gibt zwei Arten von Timern: Timer für „In Bearbeitung“ und Timer für „Schritt“.

### Fortschrittstimer

Wenn Sie einen Auftrag oder eine Auftragsvorlage erstellen, können Sie einen Wert für den Timer in Bearbeitung angeben, der zwischen 1 Minute und 7 Tagen liegt. Sie können den Wert dieses Timers bis zum Start der Auftragsausführung aktualisieren. Nachdem Ihr Timer gestartet wurde, kann er nicht mehr aktualisiert werden, und der Timerwert gilt für alle Auftragsausführungen für den Auftrag. Immer wenn eine Auftragsausführung länger als dieses Intervall im `IN_PROGRESS` Status verbleibt, schlägt die Auftragsausführung fehl und wechselt in den `TIMED_OUT` Terminalstatus. AWS IoT veröffentlicht auch eine MQTT-Benachrichtigung.

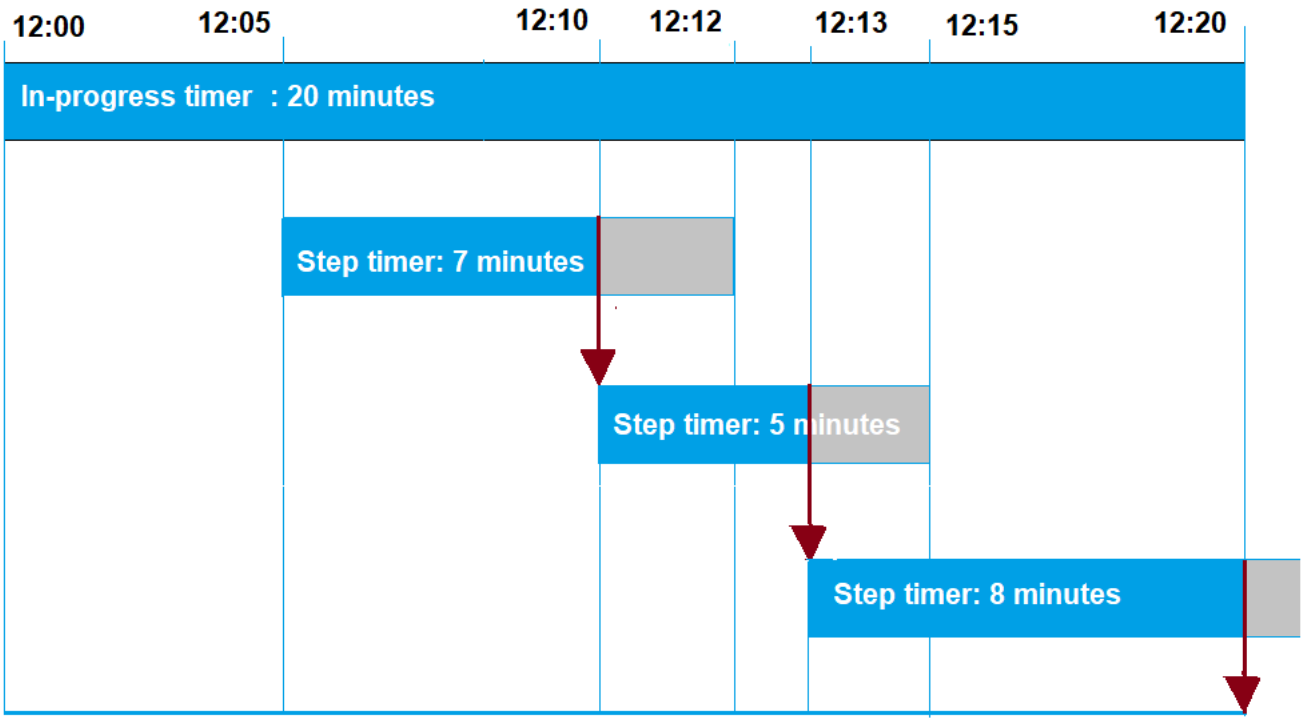
### Schritt-Timer

Sie können auch einen Schritt-Timer festlegen, der nur für die Auftragsausführung gilt, die Sie aktualisieren möchten. Dieser Timer hat keine Auswirklungen auf den Timer, der gerade bearbeitet wird. Jedes Mal, wenn Sie eine Auftragsausführung aktualisieren, können Sie einen neuen Wert für den Schritt-Timer festlegen. Sie können auch einen neuen Schritt-Timer erstellen, wenn Sie die nächste ausstehende Auftragsausführung für ein Objekt starten. Falls die Auftragsausführung länger als das Schritt-Timer-Intervall im Status `IN_PROGRESS` bleibt, schlägt sie fehl und wechselt in den terminalen Status `TIMED_OUT`.

> **Note**
>
> Sie können den Timer für die Bearbeitung festlegen, indem Sie die AWS IoT Konsole oder die AWS IoT Jobs-API verwenden. Verwenden Sie die API, um den Schritt-Timer anzugeben.

### So funktionieren Timer für Auftrags-Timeouts

Nachfolgend sehen Sie, wie die Zeitüberschreitungen während eines 20-minütigen Zeitlimits und die Schrittzeitüberschreitungen miteinander interagieren.




Im Folgenden werden die einzelnen Schritte erläutert:

1. 12:00

   Beim Erstellen eines Auftrags wird ein neuer Auftrag erstellt und ein Timer für die Dauer von 20 Minuten in Bearbeitung gestartet. Der Timer für die Bearbeitung beginnt zu laufen und die Auftragsausführung wechselt in den Status `IN_PROGRESS`.

2. 12:05

   Ein neuer Schritt-Timer mit einem Wert von 7 Minuten wird erstellt. Die Auftragsausführung läuft jetzt um 12:12 Uhr ab.

3. 12:10

   Ein neuer Schritt-Timer mit einem Wert von 5 Minuten wird erstellt. Wenn ein neuer Schritt-Timer erstellt wird, wird der vorherige Step-Timer verworfen und die Auftragsausführung läuft nun um 12:15 Uhr ab.

4. 12:13

   Ein neuer Schritt-Timer mit einem Wert von 9 Minuten wird erstellt. Der vorherige Schritt-Timer wird verworfen und die Auftragsausführung läuft jetzt um 12:20 Uhr ab, da der Timer für die

Bearbeitung des laufenden Timers um 12:20 Uhr abläuft. Der Schritt-Timer kann die absolute Grenze des laufenden Timers nicht überschreiten.

### Auftragsausführung: Konfiguration wiederholen

Sie können die Wiederholungskonfiguration verwenden, um die Ausführung des Auftrags erneut zu versuchen, wenn bestimmte Kriterien erfüllt sind. Ein Wiederholungsversuch kann versucht werden, wenn bei einem Auftrag das Timeout überschritten wird oder wenn das Gerät ausfällt. Um die Ausführung aufgrund eines Timeout-Fehlers erneut zu versuchen, müssen Sie die Timeout-Konfiguration aktivieren.

#### Wie man Konfiguration wiederholen verwendet

Führen Sie die folgenden Schritte aus, um die Konfiguration zu wiederholen:

1. Bestimmen Sie, ob Sie die Wiederholungskonfiguration für `FAILED`, `TIMED_OUT` oder beide Fehlerkriterien verwenden möchten. Was den `TIMED_OUT` Status angeht, versucht AWS IoT Jobs nach der Statusmeldung automatisch erneut, den Job für das Gerät auszuführen.
2. Prüfen Sie für den `FAILED`-Status, ob Ihr Fehler bei der Auftragsausführung erneut versucht werden kann. Wenn ein erneuter Versuch möglich ist, programmieren Sie Ihr Gerät so, dass es einen `FAILURE`-Status an AWS IoT meldet. Im folgenden Abschnitt erfahren Sie mehr über wiederholbare und nicht wiederholbare Fehler.
3. Geben Sie anhand der obigen Informationen die Anzahl der Wiederholungen an, die für jeden Fehlertyp verwendet werden sollen. Für ein einzelnes Gerät können Sie bis zu 10 Wiederholungsversuche für beide Fehlertypen zusammen angeben. Die Wiederholungsversuche werden automatisch beendet, wenn eine Ausführung erfolgreich ist oder wenn die angegebene Anzahl von Versuchen erreicht wird.
4. Fügen Sie eine Abbruchkonfiguration hinzu, um den Auftrag abzubrechen, wenn wiederholte Wiederholungsversuche fehlschlagen, um zu vermeiden, dass bei einer großen Anzahl von Wiederholungsversuchen zusätzliche Kosten anfallen.

> **Note**
>
> Wenn ein Auftrag das Ende eines wiederkehrenden Wartungsfensters erreicht, führen alle `IN_PROGRESS`-Auftragsausführungen weiterhin die im Auftragsdokument angegebenen Aktionen aus, bis sie den Terminal-Zustand erreichen. Wenn die Ausführung eines Auftrags außerhalb eines Wartungsfensters den Terminal-Zustand `FAILED` oder `TIMED_OUT` erreicht,

wird im nächsten Fenster ein erneuter Versuch unternommen, wenn die Versuche nicht erschöpft sind. Beim `startTime` des Wartungsfensters wird eine neue Auftragsausführung erstellt, die in den Status `QUEUED` wechselt, bis das Gerät startbereit ist.

Versuchen Sie es erneut und brechen Sie die Konfiguration ab

Für jeden erneuten Versuch fallen zusätzliche Kosten für Sie an. AWS-Konto Um zu vermeiden, dass zusätzliche Gebühren aufgrund wiederholter Wiederholungsversuche anfallen, empfehlen wir, eine Abbruchkonfiguration hinzuzufügen. Weitere Informationen zu Preisen finden Sie unter AWS IoT Device Management Preise.

Es kann vorkommen, dass mehrere Wiederholungsversuche fehlschlagen, wenn bei einem hohen Prozentsatz Ihrer Geräte ein Timeout auftritt oder ein Fehler gemeldet wird. In diesem Fall können Sie die Abbruchkonfiguration verwenden, um den Auftrag abzubrechen und so zu vermeiden, dass Aufträge in der Warteschlange ausgeführt oder weitere Versuche wiederholt werden.

> **Note**
>
> Wenn die Abbruchkriterien für den Abbruch einer Auftragsausführung erfüllt sind, werden nur `QUEUED`-Auftragsausführungen abgebrochen. Wiederholungen in der Warteschlange für das Gerät werden nicht versucht. Aktuelle Auftragsausführungen, die einen `IN_PROGRESS`-Status haben, werden jedoch nicht abgebrochen.

Bevor Sie eine fehlgeschlagene Auftragsausführung erneut versuchen, empfehlen wir Ihnen außerdem, zu überprüfen, ob die fehlgeschlagene Auftragsausführung erneut versucht werden kann, wie im folgenden Abschnitt beschrieben.

Wiederholungsversuch bei Fehlerart **`FAILED`**

Um Wiederholungsversuche für den Fehlertyp `FAILED` zu versuchen, müssen Ihre Geräte so programmiert sein, dass sie den `FAILURE`.Status einer fehlgeschlagenen Auftragsausführung an AWS IoT melden. Legen Sie die Wiederholungskonfiguration mit den Kriterien fest, nach denen die `FAILED` Auftragsausführung wiederholt werden soll, und geben Sie die Anzahl der auszuführenden Wiederholungen an. Wenn AWS IoT Jobs den `FAILURE` Status erkennt, wird automatisch versucht, die Auftragsausführung für das Gerät erneut zu versuchen. Die Wiederholungsversuche werden fortgesetzt, bis die Auftragsausführung erfolgreich ist oder die maximale Anzahl von Wiederholungsversuchen erreicht ist.

Sie können jeden Wiederholungsversuch und den Auftrag, der auf diesen Geräten ausgeführt wird, verfolgen. Indem Sie den Ausführungsstatus verfolgen, können Sie nach der angegebenen Anzahl von Wiederholungsversuchen Ihr Gerät verwenden, um Fehler zu melden und einen weiteren Wiederholungsversuch einzuleiten.

Fehler, die wiederholt werden können und die nicht wiederholt werden können

Ihr Fehler bei der Auftragsausführung kann wiederholt oder nicht wiederholt werden. Für jeden Wiederholungsversuch können Gebühren für Ihr AWS-Konto anfallen. Um zu vermeiden, dass bei mehreren Wiederholungsversuchen zusätzliche Gebühren anfallen, sollten Sie zunächst prüfen, ob Ihr Fehler bei der Auftragsausführung erneut versucht werden kann. Ein Beispiel für einen erneuten Versuch ist ein Verbindungsfehler, der auf Ihrem Gerät auftritt, wenn versucht wird, das Auftragsdokument von einer Amazon S3-URL herunterzuladen. Wenn Ihr Fehler bei der Auftragsausführung erneut versucht werden kann, programmieren Sie Ihr Gerät so, dass es einen `FAILURE`-Status meldet, falls die Auftragsausführung fehlschlägt. Stellen Sie dann die Wiederholungskonfiguration so ein, dass `FAILED`-Ausführungen erneut versucht werden.

Wenn die Ausführung nicht erneut versucht werden kann, empfehlen wir, das Gerät so zu programmieren, dass es einen `REJECTED`-Status an AWS IoT meldet, um einen erneuten Versuch zu vermeiden und Ihrem Konto möglicherweise zusätzliche Gebühren aufzuerlegen. Ein Fehler, der nicht wiederholt werden kann, ist zum Beispiel, wenn Ihr Gerät keine Auftragsaktualisierung empfangen kann oder wenn bei der Ausführung eines Auftrags ein Speicherfehler auftritt. In diesen Fällen versucht AWS IoT Jobs die Auftragsausführung nicht erneut, da Jobs die Ausführung des Jobs nur dann wiederholt, wenn der Status oder erkannt wird. `FAILED` `TIMED_OUT`

Wenn Sie festgestellt haben, dass ein Fehler bei der Auftragsausführung erneut versucht werden kann, sollten Sie die Geräteprotokolle überprüfen, falls ein erneuter Versuch immer noch fehlschlägt.

> **Note**
>
> Wenn ein Auftrag mit der optionalen Planungskonfiguration seinen `endTime` erreicht, stoppt `endBehavior` die Auswahl die Bereitstellung des Auftragsdokuments auf allen verbleibenden Geräten in der Zielgruppe und bestimmt, wie mit den verbleibenden Auftragsausführungen fortgefahren werden soll. Die Versuche werden wiederholt, wenn sie über die Wiederholungskonfiguration ausgewählt wurden.

Wiederholungsversuch bei Fehlerart **`TIMEOUT`**

Wenn Sie bei der Erstellung eines Jobs das Timeout aktivieren, versucht AWS IoT Jobs, die Auftragsausführung für das Gerät erneut zu versuchen, wenn der Status von zu wechselt. `IN_PROGRESS` `TIMED_OUT` Diese Statusänderung kann auftreten, wenn für den Timer in Bearbeitung eine Zeitüberschreitung eintritt oder wenn ein von Ihnen festgelegter Schritt-Timer in `IN_PROGRESS` ist und dann das Zeitlimit überschritten wird. Die Wiederholungsversuche werden fortgesetzt, bis die Auftragsausführung erfolgreich ist oder bis die maximale Anzahl von Wiederholungsversuchen für diesen Fehlertyp erreicht ist.

Fortlaufende Aktualisierungen von Aufträgen und Mitgliedschaften in Objektgruppen

Bei kontinuierlichen Aufträgen mit dem Auftragsstatus `IN_PROGRESS` wird die Anzahl der Wiederholungsversuche auf Null zurückgesetzt, wenn die Gruppenmitgliedschaft eines Objekts aktualisiert wird. Nehmen wir beispielsweise an, Sie haben fünf Wiederholungsversuche angegeben und drei Wiederholungsversuche wurden bereits durchgeführt. Wenn ein Ding jetzt aus der Objektgruppe entfernt wird und dann wieder der Gruppe beitritt, z. B. bei dynamischen Objektgruppen, wird die Anzahl der Wiederholungsversuche auf Null zurückgesetzt. Sie können jetzt fünf Wiederholungsversuche für Ihre Objektgruppe durchführen, anstatt der beiden verbleibenden Versuche. Wenn ein Objekt aus der Objektgruppe entfernt wird, werden außerdem weitere Wiederholungsversuche abgebrochen.

## Zusätzliche Konfigurationen angeben

Wenn Sie einen Auftrag oder eine Auftragsvorlage erstellen, können Sie diese zusätzlichen Konfigurationen angeben. Im Folgenden wird gezeigt, wann Sie diese Konfigurationen angeben können.

- Wenn Sie eine benutzerdefinierte Auftragsvorlage erstellen. Die zusätzlichen Konfigurationseinstellungen, die Sie angeben, werden gespeichert, wenn Sie einen Auftrag anhand der Vorlage erstellen.
- Beim Erstellen eines benutzerdefinierten Auftrags mithilfe einer Auftragsdatei. Die Auftragsdatei kann eine JSON-Datei sein, die in einen S3-Bucket hochgeladen wird.
- Beim Erstellen eines benutzerdefinierten Auftrags mithilfe einer benutzerdefinierten Auftragsvorlage. Wenn für die Vorlage diese Einstellungen bereits angegeben sind, können Sie sie entweder wiederverwenden oder sie überschreiben, indem Sie neue Konfigurationseinstellungen angeben.
- Beim Erstellen eines benutzerdefinierten Jobs mithilfe einer AWS verwalteten Vorlage.

Themen


- Geben Sie Auftragskonfigurationen mithilfe der AWS Management Console an
- Geben Sie Auftragskonfigurationen mithilfe der AWS IoT Jobs API an


## Geben Sie Auftragskonfigurationen mithilfe der AWS Management Console an

Sie können die verschiedenen Konfigurationen für Ihren Job mithilfe der AWS IoT Konsole hinzufügen. Nachdem Sie einen Auftrag erstellt haben, können Sie die Statusdetails Ihrer Auftrags-Konfigurationen auf der Seite mit den Auftragsdetails sehen. Weitere Informationen über die verschiedenen Konfigurationen und deren Funktionsweise finden Sie unter Wie funktionieren Auftragskonfigurationen.

Fügen Sie die Auftragskonfigurationen hinzu, wenn Sie einen Auftrag oder eine Auftragsvorlage erstellen.

Wenn Sie eine benutzerdefinierte Auftragsvorlage erstellen

Um die Rollout-Konfiguration bei der Erstellung einer benutzerdefinierten Auftragsvorlage anzugeben

1. Gehen Sie in der AWS IoT Konsole zum Hub Jobvorlagen und wählen Sie Jobvorlage erstellen aus.
2. Geben Sie die Eigenschaften der Auftragsvorlage an, stellen Sie das Auftragsdokument bereit, erweitern Sie die Konfiguration, die Sie hinzufügen möchten, und geben Sie dann die Konfigurationsparameter an.

Beim Erstellen eines benutzerdefinierten Auftrags

Um die Rollout-Konfiguration bei der Erstellung eines benutzerdefinierten Auftrags anzugeben

1. Gehen Sie zum Job-Hub der AWS IoT Konsole und wählen Sie Job erstellen aus.
2. Wählen Sie „Benutzerdefinierten Auftrag erstellen“ und geben Sie die Auftragseigenschaften und Ziele an und geben Sie an, ob eine Auftragsdatei oder eine Vorlage für das Auftragsdokument verwendet werden soll. Sie können eine benutzerdefinierte Vorlage oder eine AWS verwaltete Vorlage verwenden.
3. Wählen Sie die Auftragskonfiguration aus und erweitern Sie dann die Rollout-Konfiguration, um anzugeben, ob eine konstante Rate oder eine exponentielle Rate verwendet werden soll. Geben Sie dann die Konfigurationsparameter an.

Der nächste Abschnitt zeigt die Parameter, die Sie für jede Konfiguration angeben können.

Rollout-Konfiguration

Sie können angeben, ob Sie eine konstante Rollout-Rate oder eine exponentielle Rate verwenden möchten.

- Stellen Sie eine konstante Rollout-Rate ein

  Um eine konstante Rate für die Ausführung von Aufträgen festzulegen, wählen Sie Konstante Rate und geben Sie dann das Maximum pro Minute als Obergrenze für die Rate an. Dieser Wert ist optional und reicht von 1 bis 1000. Wenn Sie ihn nicht festlegen, wird 1000 als Standardwert verwendet.
- Legen Sie eine exponentielle Rollout-Rate fest

  Um eine exponentielle Rate festzulegen, wählen Sie Exponentielle Rate und geben Sie dann die folgenden Parameter an:

  - Basistarif pro Minute

    Die Geschwindigkeit, mit der die Aufträge ausgeführt werden, bis der Schwellenwert für die Anzahl der gemeldeten Geräte oder die Anzahl der erfolgreichen Geräte für die Kriterien zur Erhöhung der Rate erreicht ist.
  - Inkrementfaktor

    Der exponentielle Faktor, um den sich die Rollout-Rate erhöht, wenn der Schwellenwert „Anzahl der benachrichtigten Geräte“ oder „Anzahl der erfolgreichen Geräte“ für die Kriterien „Ratenerhöhung“ erreicht ist.
  - Kriterien für die Ratenerhöhung

    Der Schwellenwert für entweder die Anzahl der gemeldeten Geräte oder die Anzahl der erfolgreichen Geräte.

Konfiguration abbrechen

Wählen Sie Neue Konfiguration hinzufügen und geben Sie für jede Konfiguration die folgenden Parameter an:

- Art des Fehlers

Gibt die Fehlertypen an, die einen Auftragsabbruch auslösen. Dazu gehören FAILED, REJECTED, TIMED_OUT oder ALL.

- Inkrementfaktor

  Gibt die Anzahl der abgeschlossenen Auftragsausführungen an, die erfolgen müssen, bevor das Auftragsabbruchkriterium erfüllt ist.

- Schwellenwert-Prozentsatz

  Gibt die Gesamtanzahl der ausgeführten Objekte an, die einen Auftragsabbruch auslöst.

Konfiguration des Zeitplans

Jeder Auftrag kann sofort nach der ersten Erstellung beginnen, zu einem späteren Zeitpunkt beginnen oder während eines wiederkehrenden Wartungsfensters ausgeführt werden.

Wählen Sie Neue Konfiguration hinzufügen und geben Sie für jede Konfiguration die folgenden Parameter an:

- Beginn des Auftrags

  Geben Sie das Datum und die Uhrzeit an, zu der der Auftrag gestartet wird.

- Wiederkehrendes Wartungsfenster

  Ein wiederkehrendes Wartungsfenster definiert das genaue Datum und die Uhrzeit, zu der ein Auftrag das Auftragsdokument auf den Zielgeräten des Auftrags bereitstellen kann. Das Wartungsfenster kann täglich, wöchentlich, monatlich oder mit einer benutzerdefinierten Wiederholung von Tag und Uhrzeit wiederholt werden.

- Ende des Auftrags

  Geben Sie das Datum und die Uhrzeit an, zu der der Auftrag beendet wird.

- Verhalten bei Auftragsende

  Wählen Sie ein Endverhalten für alle noch nicht abgeschlossenen Auftragsausführungen aus, wenn der Auftrag beendet ist.

> **Note**
>
> Wenn ein Auftrag mit der optionalen Zeitplanungskonfiguration und der gewählten Endzeit die Endzeit erreicht, stoppt der Auftrag das Rollout auf alle verbleibenden Geräte in der Zielgruppe. Außerdem wird anhand des ausgewählten Endverhaltens entschieden, wie mit den verbleibenden Auftragsausführungen und deren Wiederholungsversuchen gemäß der Wiederholungskonfiguration fortgefahren werden soll.

Timeout-Konfiguration

Standardmäßig gibt es kein Timeout und Ihr Auftrag wird abgebrochen oder gelöscht. Um Timeouts zu verwenden, wählen Sie Timeout aktivieren und geben Sie dann einen Timeout-Wert zwischen 1 Minute und 7 Tagen an.

Wiederholungs-Konfiguration

> **Note**
>
> Nachdem ein Auftrag erstellt wurde, kann die Anzahl der Wiederholungen nicht aktualisiert werden. Sie können die Wiederholungskonfiguration nur für alle Fehlertypen entfernen. Wenn Sie einen Auftrag erstellen, sollten Sie die entsprechende Anzahl von Wiederholungsversuchen berücksichtigen, die Sie für Ihre Konfiguration verwenden. Fügen Sie eine Abbruchkonfiguration hinzu, um übermäßige Kosten aufgrund potenzieller Wiederholungsfehler zu vermeiden.

Wählen Sie Neue Konfiguration hinzufügen und geben Sie für jede Konfiguration die folgenden Parameter an:

- Art des Fehlers

  Gibt die Fehlertypen an, die einen erneuten Versuch der Auftragsausführung auslösen sollen. Dazu gehören Fehlgeschlagen, Timeout und Alle.
- Anzahl der Wiederholungen

  Gibt die Anzahl der Wiederholungen für den ausgewählten Fehlertyp an. Für beide Fehlertypen zusammen können bis zu 10 Wiederholungsversuche versucht werden.

## Geben Sie Auftragskonfigurationen mithilfe der AWS IoT Jobs API an

Sie können die CreateJoboder die CreateJobTemplateAPI verwenden, um die verschiedenen Jobkonfigurationen anzugeben. In den folgenden Abschnitten wird beschrieben, wie Sie diese Konfigurationen hinzufügen. Nachdem Sie die Konfigurationen hinzugefügt haben, können Sie JobExecutionSummaryund verwenden, JobExecutionSummaryForJobum ihren Status einzusehen.

Weitere Informationen über die verschiedenen Konfigurationen und deren Funktionsweise finden Sie unter Wie funktionieren Auftragskonfigurationen.

Rollout-Konfiguration

Sie können eine konstante Rollout-Rate oder eine exponentielle Rollout-Rate für Ihre Rollout-Konfiguration angeben.

- Stellen Sie eine konstante Rollout-Rate ein

  Um eine konstante Rollout-Rate festzulegen, verwenden Sie das `JobExecutionsRolloutConfig`-Objekt, um den `maximumPerMinute`-Parameter zur `CreateJob`-Anforderung hinzuzufügen. Dieser Parameter gibt die obere Grenze der Rate an, mit der Auftragsausführungen durchgeführt werden können. Dieser Wert ist optional und reicht von 1 bis 1000. Wenn Sie den Wert nicht festlegen, wird 1000 als Standardwert verwendet.

  ```
      "jobExecutionsRolloutConfig": {
          "maximumPerMinute": 1000
      }
  ```

- Legen Sie eine exponentielle Rollout-Rate fest

  Verwenden Sie das `JobExecutionsRolloutConfig`-Objekt, um eine variable Auftrags-Rollout-Rate festzulegen. Sie können die `ExponentialRolloutRate`-Eigenschaft konfigurieren, wenn Sie den `CreateJob`-API-Vorgang ausführen. Im folgenden Beispiel wird eine variable Rolloutrate mit dem Parameter `exponentialRate` eingerichtet. Weitere Informationen zu den Parametern finden Sie unter `ExponentialRolloutRate`.

  ```
  {
  ...
    "jobExecutionsRolloutConfig": {
      "exponentialRate": {
        "baseRatePerMinute": 50,
        "incrementFactor": 2,
  ```

```
      "rateIncreaseCriteria": {
        "numberOfNotifiedThings": 1000,
        "numberOfSucceededThings": 1000
      },
      "maximumPerMinute": 1000
    }
  }
...
}
```

Wo der Parameter:

baseRatePerMinute

Gibt die Rate an, mit der die Aufträge ausgeführt werden, bis der `numberOfNotifiedThings`- oder der `numberOfSucceededThings`-Schwellenwert erreicht wird.

incrementFactor

Gibt den exponentiellen Faktor an, um den die Rolloutrate erhöht wird, nachdem der `numberOfNotifiedThings`- oder der `numberOfSucceededThings`-Schwellenwert erreicht wird.

rateIncreaseCriteria

Gibt entweder den `numberOfNotifiedThings`- oder den `numberOfSucceededThings`-Schwellenwert an.

### Konfiguration abbrechen

Um diese Konfiguration mithilfe der API hinzuzufügen, geben Sie den `AbortConfig`-Parameter an, wenn Sie den `CreateJob` oder den `CreateJobTemplate` API-Vorgang ausführen. Das folgende Beispiel zeigt eine Abbruchkonfiguration für einen Auftrags-Rollout, bei dem es, wie bei der `CreateJob` API-Operation angegeben, zu mehreren fehlgeschlagenen Ausführungen kam.

> **Note**
>
> Das Löschen einer Auftragsausführung wirkt sich auf die Berechnung des Werts der gesamten abgeschlossenen Ausführungen aus. Wenn ein Auftrag abgebrochen wird, erstellt

der Service einen automatisierten `comment` und `reasonCode` zur Differenzierung zwischen eines vom Benutzer ausgelösten Abbruchs und eines automatischen Auftragsabbruchs.

```
  "abortConfig": {
     "criteriaList": [
        {
           "action": "CANCEL",
           "failureType": "FAILED",
           "minNumberOfExecutedThings": 100,
           "thresholdPercentage": 20
        },
        {
           "action": "CANCEL",
           "failureType": "TIMED_OUT",
           "minNumberOfExecutedThings": 200,
           "thresholdPercentage": 50
        }
     ]
   }
```

Wo der Parameter:

Aktion

Gibt die Aktion an, die durchgeführt werden soll, wenn das Abbruchkriterium erfüllt ist. Dieser Parameter ist erforderlich, und `CANCEL` ist der einzige gültige Wert.

failureType

Gibt an, welche Fehlertypen einen Auftragsabbruch auslösen sollen. Gültige Werte sind `FAILED`, `REJECTED`, `TIMED_OUT` und `ALL`.

minNumberOfExecutedThings

Gibt die Anzahl der abgeschlossenen Auftragsausführungen an, die erfolgen müssen, bevor das Auftragsabbruchkriterium erfüllt ist. In diesem Beispiel prüft AWS IoT erst dann, ob ein Auftragsabbruch erfolgen soll, wenn mindestens 100 Geräte Auftragsausführungen abgeschlossen haben.

thresholdPercentage

Gibt die Gesamtzahl der Objekte an, für die Aufträge ausgeführt werden, die einen Auftragsabbruch auslösen können. In diesem Beispiel wird nacheinander AWS IoT geprüft und ein Jobabbruch eingeleitet, wenn der prozentuale Schwellenwert erreicht ist. Wenn mindestens 20 % der vollständigen Ausführungen fehlschlagen, nachdem 100 Ausführungen abgeschlossen sind, wird der Auftrags-Rollout abgebrochen. Wenn dieses Kriterium nicht erfüllt ist, AWS IoT wird geprüft, ob bei mindestens 50% der abgeschlossenen Ausführungen ein Timeout nach 200 Ausführungen erreicht wurde. Wenn dies der Fall ist, wird der Auftrags-Rollout abgebrochen.

Konfiguration des Zeitplans

Um diese Konfiguration mithilfe der API hinzuzufügen, geben Sie den optionalen `SchedulingConfig` an, wenn Sie den `CreateJob` oder den `CreateJobTemplate` API-Vorgang ausführen.

```
  "SchedulingConfig": {
    "endBehavior": string
    "endTime": string
    "maintenanceWindows": string
    "startTime": string
}
```

Wo der Parameter:

startTime

Gibt das Datum und die Uhrzeit an, zu der der Auftrag gestartet wird.

endTime

Gibt das Datum und die Uhrzeit an, zu der der Auftrag beendet wird.

maintenanceWindows

Gibt an, ob für den geplanten Auftrag ein optionales Wartungsfenster ausgewählt wurde, um das Auftragsdokument auf alle Geräte in der Zielgruppe auszurollen. Das Zeichenkettenformat für `maintenanceWindow` ist JJJJ/MM/TT für das Datum und hh:mm für die Uhrzeit.

endBehavior

Gibt das Auftragsverhalten für einen geplanten Auftrag beim Erreichen des `endTime` an.

> **Note**
>
> Die Option `SchedulingConfig` für einen Auftrag ist in den `DescribeJobTemplate`- und `DescribeJob`-APIs einsehbar.

Timeout-Konfiguration

Um diese Konfiguration mithilfe der API hinzuzufügen, geben Sie den `TimeoutConfig`-Parameter an, wenn Sie den `CreateJob` oder den `CreateJobTemplate` API-Vorgang ausführen.

Um die Timeout-Konfiguration zu verwenden

1. Um den Timer für die Bearbeitung festzulegen, wenn Sie einen Job oder eine Jobvorlage erstellen, legen Sie einen Wert für die `inProgressTimeoutInMinutes` Eigenschaft des optionalen Objekts fest. TimeoutConfig

   ```
    "timeoutConfig": {
      "inProgressTimeoutInMinutes": number
   }
   ```

2. Um einen Schrittzeitgeber für die Ausführung eines Jobs anzugeben, legen Sie einen Wert für den `stepTimeoutInMinutes` Zeitpunkt des Aufrufs UpdateJobExecutionfest. Der Schritt Timer gilt nur für die Auftragsausführung, die Sie aktualisieren. Sie können einen neuen Wert für diesen Timer bei jeder Aktualisierung einer Auftragsausführung einrichten.

   > **Note**
   >
   > `UpdateJobExecution` kann einen bereits erstellten Schritt-Timer verwerfen, indem er einen neuen Schritt-Timer mit dem Wert -1 erstellt.

   ```
   {
      ...
       "statusDetails": {
         "string" : "string"
      },
      "stepTimeoutInMinutes": number
   }
   ```

3. Um einen neuen Steptimer zu erstellen, können Sie auch den StartNextPendingJobExecutionAPI-Vorgang aufrufen.

Wiederholungs-Konfiguration

> **Note**
>
> Wenn Sie einen Auftrag erstellen, sollten Sie die entsprechende Anzahl von Wiederholungsversuchen berücksichtigen, die Sie für Ihre Konfiguration verwenden. Fügen Sie eine Abbruchkonfiguration hinzu, um übermäßige Kosten aufgrund potenzieller Wiederholungsfehler zu vermeiden. Nachdem ein Auftrag erstellt wurde, kann die Anzahl der Wiederholungen nicht aktualisiert werden. Sie können die Anzahl der Wiederholungen nur mithilfe der UpdateJobAPI-Operation auf 0 setzen.

Um diese Konfiguration mithilfe der API hinzuzufügen, geben Sie den `jobExecutionsRetryConfig`-Parameter an, wenn Sie den `CreateJob` oder den `CreateJobTemplate` API-Vorgang ausführen.

```
{
...
  "jobExecutionsRetryConfig": {
      "criteriaList": [
         {
            "failureType": "string",
            "numberOfRetries": number
         }
      ]
  }
...
}
```

Wobei criteriaList ein Array ist, das die Kriterienliste angibt, die die Anzahl der zulässigen Wiederholungen für jeden Fehlertyp für einen Auftrag bestimmt.

# Geräte und Aufträge

Geräte können mit AWS IoT Jobs über MQTT, HTTP Signature Version 4 oder HTTP TLS kommunizieren. Führen Sie den Befehl aus, um den Endpunkt zu ermitteln, der verwendet werden

soll, wenn Ihr Gerät mit AWS IoT Jobs kommuniziert. DescribeEndpoint Wenn Sie z. B. den folgenden Befehl ausführen:

```
aws iot describe-endpoint --endpoint-type iot:Data-ATS
```

Das Ergebnis sieht in etwa wie folgt aus:

```
{
    "endpointAddress": "a1b2c3d4e5f6g7-ats.iot.us-west-2.amazonaws.com"
}
```

## Verwendung des MQTT-Protokolls

Geräte können über das MQTT-Protokoll mit AWS IoT Jobs kommunizieren. Geräte abonnieren MQTT-Themen, um über neue Jobs informiert zu werden und Antworten vom AWS IoT Jobs-Service zu erhalten. Geräte veröffentlichen auf MQTT-Themen, um den Status eines Auftrags-Launch abzufragen oder zu aktualisieren. Jedes Gerät verfügt über ein allgemeines MQTT-Thema. Für weitere Informationen zur Veröffentlichung und zum Abonnement von MQTT-Themen vgl. Gerätekommunikationsprotokolle.

Bei dieser Kommunikationsmethode verwendet Ihr Gerät sein gerätespezifisches Zertifikat und seinen privaten Schlüssel, um sich bei Jobs zu authentifizieren. AWS IoT

Ihre Geräte können die folgenden Themen abonnieren. `thing-name` ist der Name des Objekts, das mit dem Gerät verknüpft ist.

- **`$aws/things/thing-name/jobs/notify`**

  Abonnieren Sie dieses Thema, um Sie zu benachrichtigen, wenn ein Auftragsstart zur Liste der ausstehenden Auftragsstarts hinzugefügt oder daraus entfernt wird.

- **`$aws/things/thing-name/jobs/notify-next`**

  Abonnieren Sie dieses Thema, um Sie zu benachrichtigen, wenn sich die nächste ausstehende Auftragsausführung geändert hat.

- **`$aws/things/thing-name/jobs/request-name/accepted`**

  Der AWS IoT Jobs-Service veröffentlicht Erfolgs- und Fehlschlagsmeldungen zu einem MQTT-Thema. Das Thema wird durch Anhängen von `accepted` oder `rejected` an das Thema erstellt,

mit dem die Anforderung getätigt wurde. Hier `request-name` ist der Name einer Anfrage wie `Get` und das Thema kann sein:`$aws/things/myThing/jobs/get`. AWS IoT Jobs veröffentlicht dann Erfolgsmeldungen zum `$aws/things/myThing/jobs/get/accepted` Thema.

- **`$aws/things/`*`thing-name`*`/jobs/`*`request-name`*`/rejected`**

  Hier ist `request-name` der Name Ihrer Region, z. B. `Get`. Wenn die Anfrage fehlgeschlagen ist, veröffentlicht AWS IoT Jobs Fehlermeldungen zu `$aws/things/myThing/jobs/get/rejected` diesem Thema.

Sie können auch die folgenden HTTPS API-Operationen verwenden:

- Den Status einer Auftragsausführung durch Aufruf der `UpdateJobExecution`-API aktualisieren.
- Den Status einer Auftragsausführung durch Aufruf der `DescribeJobExecution`-API abfragen.
- Eine Liste der ausstehenden Auftragsausführung durch Aufruf der `GetPendingJobExecutions`-API abrufen.
- Die nächste ausstehende Auftragsausführung durch Aufruf der `DescribeJobExecution`-API mit `jobId` als `$next` abrufen.
- Die nächste ausstehende Auftragsausführung durch Aufruf der `StartNextPendingJobExecution`-API abrufen und starten.

## Verwendung der HTTP-Signaturversion 4

Geräte können über die AWS IoT HTTP-Signatur Version 4 an Port 443 mit Jobs kommunizieren. Dies ist die Methode, die von der AWS SDKs AND-CLI verwendet wird. Weitere Informationen zu diesen Tools finden Sie unter AWS CLI Befehlsreferenz: iot-jobs-data oder AWS SDKs und Tools sowie im IotJobsDataPlane Abschnitt für Ihre bevorzugte Sprache.

Bei dieser Kommunikationsmethode verwendet Ihr Gerät IAM-Anmeldeinformationen, um sich bei AWS IoT Jobs zu authentifizieren.

Für diese Methode stehen die folgenden Befehle zur Verfügung:

- 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 ...
```

### Verwendung von HTTP TLS

Geräte können über HTTP-TLS auf Port 8443 mit AWS IoT Jobs kommunizieren, indem ein Drittanbieter-Softwareclient verwendet wird, der dieses Protokoll unterstützt.

Bei dieser Methode verwendet Ihr Gerät eine auf dem X.509-Zertifikat basierende Authentifizierung (z. B. unter Verwendung des gerätespezifischen Zertifikats und des privaten Schlüssels).

Für diese Methode stehen die folgenden Befehle zur Verfügung:

- DescribeJobExecution
- GetPendingJobExecutions
- StartNextPendingJobExecution
- UpdateJobExecution

## Programmieren von Geräten zur Arbeit mit Aufträgen

Die Beispiele in diesem Abschnitt verwenden MQTT, um zu veranschaulichen, wie ein Gerät mit dem AWS IoT Jobs-Service zusammenarbeitet. Sie können auch die entsprechenden API- oder CLI-Befehle verwenden. Bei diesen Beispielen wird davon ausgegangen, dass ein Gerät mit der Bezeichnung `MyThing` die folgenden MQTT-Themen abonniert hat:

- `$aws/things/MyThing/jobs/notify` (oder `$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`

Wenn Sie Codesigning für verwenden AWS IoT, muss Ihr Gerätecode die Signatur Ihrer Codedatei verifizieren. Die Signatur befindet sich in dem Auftragsdokument in der `codesign`-Eigenschaft. Weitere Informationen zum Verifizieren einer Codedatei-Signatur finden Sie unter Geräte-Agent-Beispiel.

Themen


- Geräteworkflow
- Arbeitsablauf für Aufträge
- Auftragsbenachrichtigungen


## Geräteworkflow

Ein Gerät kann Aufträge, die es ausführt, auf eine der folgenden Arten verarbeiten.

- Holen Sie sich den nächsten Auftrag

  1. Wenn ein Gerät online geht, sollte es das `notify-next`-Thema des Gerätes abonnieren.
  2. Rufen Sie die DescribeJobExecution-MQTT-API mit jobId `$next` auf, um den nächsten Auftrag, sein Auftragsdokument und andere Details abzurufen, einschließlich eines eventuell in `statusDetails` gespeicherten Status. Wenn das Auftragsdokument eine Codedateisignatur hat, müssen Sie die Signatur verifizieren, bevor Sie mit der Verarbeitung des Auftrags fortfahren.
  3. Rufen Sie die UpdateJobExecution-MQTT-API auf, um den Auftragsstatus zu aktualisieren. Zur Kombination dieses und des vorherigen Schrittes in einem Aufruf kann das Gerät auch StartNextPendingJobExecution aufrufen.
  4. (Optional) Sie können einen Schritt-Timer hinzufügen, indem Sie einen Wert für `stepTimeoutInMinutes` angeben, wenn Sie UpdateJobExecution oder StartNextPendingJobExecution aufrufen.
  5. Führen Sie die in dem Auftragsdokument angegebenen Aktionen mit der UpdateJobExecution-MQTT-API durch, um über den Fortschritt des Auftrags zu berichten.
  6. Überwachen Sie die Auftragsausführung durch Aufruf der DescribeJobExecution MQTT-API mit dieser jobId. Wenn die Auftragsausführung gelöscht wird, gibt ein DescribeJobExecution einen `ResourceNotFoundException` aus.

     Das Gerät sollte in der Lage sein, einen gültigen Zustand wiederherzustellen, wenn die Auftragsausführung abgebrochen oder gelöscht wird, während das Gerät den Auftrag ausführt.

7. Rufen Sie die UpdateJobExecution-MQTT-API erneut auf, wenn Sie den Auftrag abgeschlossen haben, um den Auftragsstatus zu aktualisieren und Erfolg oder Fehlschlag zu melden.
8. Da der Auftragsstatus dieses Auftrags zu einem terminalen Status geändert wurde, ändert sich der nächste zur Ausführung anstehende Auftrag (falls vorhanden). Das Gerät wird benachrichtigt, dass sich die nächste ausstehende Auftragsausführung geändert hat. An diesem Punkt sollte das Gerät wie in Schritt 2 beschrieben fortfahren.

Wenn das Gerät online bleibt, erhält es weiterhin Benachrichtigungen über die nächste ausstehende Auftragsausführung. Dazu gehören auch die Daten zur Auftragsausführung, wenn ein Auftrag abgeschlossen ist oder wenn eine neue ausstehende Auftragsausführung hinzugefügt wird. Wenn dies eintritt, fährt das Gerät wie in Schritt 2 beschrieben fort.

- Wählen Sie aus verfügbaren Aufträgen

1. Wenn ein Gerät online geht, sollte es das `notify`-Thema des Objekts abonnieren.
2. Rufen Sie die GetPendingJobExecutions-MQTT-API auf, um eine Liste der ausstehenden Auftragsausführungen abzurufen.
3. Wenn die Liste eine oder mehrere Auftragsausführungen enthält, wählen Sie eine davon.
4. Rufen Sie die DescribeJobExecution-MQTT-API ab, um das Auftragsdokument und andere Details abzurufen, einschließlich eventueller in `statusDetails` gespeicherter Status.
5. Rufen Sie die UpdateJobExecution-MQTT-API auf, um den Auftragsstatus zu aktualisieren. Wenn das Feld `includeJobDocument` in diesem Befehl auf `true` gesetzt ist, kann das Gerät den vorherigen Schritt übergehen und an diesem Punkt das Auftragsdokument abrufen.
6. Optional können Sie einen Schritt-Timer hinzufügen, indem Sie einen Wert für `stepTimeoutInMinutes` angeben, wenn Sie UpdateJobExecution aufrufen.
7. Führen Sie die in dem Auftragsdokument angegebenen Aktionen mit der UpdateJobExecution-MQTT-API durch, um über den Fortschritt des Auftrags zu berichten.
8. Überwachen Sie die Auftragsausführung durch Aufruf der DescribeJobExecution MQTT-API mit dieser jobId. Wenn die Auftragsausführung abgebrochen oder gelöscht werden, während das Gerät den Auftrag ausführt, sollte das Gerät in der Lage sein, die Wiederherstellung in einen gültigen Zustand durchzuführen.
9. Rufen Sie die UpdateJobExecution-MQTT-API erneut auf, wenn Sie den Auftrag abgeschlossen haben, um den Auftragsstatus zu aktualisieren und Erfolg oder Fehlschlag zu melden.

Wenn das Gerät online bleibt, wird es über alle ausstehenden Auftragsausführungen benachrichtigt, wenn neue ausstehende Auftragsausführungen verfügbar werden. Wenn dies eintritt, kann das Gerät wie in Schritt 2 beschrieben fortfahren.

Wenn das Gerät den Auftrag nicht ausführen kann, sollte es die UpdateJobExecution-MQTT-API aufruft, um den Auftragsstatus zu `REJECTED` aktualisieren.

## Arbeitsablauf für Aufträge

Im Folgenden werden die verschiedenen Schritte des Auftragsworkflows vom Starten eines neuen Auftrags bis hin zur Meldung des Abschlussstatus einer Auftragsausführung dargestellt.

### Starten Sie einen neuen Auftrag

Wenn ein neuer Job erstellt wird, veröffentlicht AWS IoT Jobs für jedes Zielgerät eine Nachricht zu `$aws/things/thing-name/jobs/notify` diesem Thema.

Die Nachricht enthält die folgenden Informationen:

```
{
    "timestamp":1476214217017,
    "jobs":{
        "QUEUED":[{
            "jobId":"0001",
            "queuedAt":1476214216981,
            "lastUpdatedAt":1476214216981,
            "versionNumber" : 1
        }]
    }
}
```

Das Gerät erhält diese Nachricht auf dem `'$aws/things/thingName/jobs/notify'`-Thema, wenn die Auftragsausführung in die Warteschlange gesetzt wird.

> **Note**
>
> Bei Aufträgen mit dem optionalen `SchedulingConfig` behält der Auftrag den ursprünglichen `SCHEDULED`-Status bei. Wenn der Auftrag den ausgewählten `startTime` erreicht, passiert Folgendes:

- Der Status des Auftragsstatus wird auf `IN_PROGRESS` aktualisiert.
- Der Auftrag beginnt mit dem Rollout des Auftragsdokuments auf alle Geräte der Zielgruppe.

## Auftragsinformationen abrufen

Um weitere Informationen zu einer Auftragsausführung abzurufen, ruft das Gerät die DescribeJobExecution-MQTT-API mit dem Wert `true` in dem Feld `includeJobDocument` ab (Standard).

Wenn die Anfrage erfolgreich ist, veröffentlicht der AWS IoT Jobs-Service eine Nachricht zum `$aws/things/MyThing/jobs/0023/get/accepted` Thema:

```
{
    "clientToken" : "client-001",
    "timestamp" : 1489097434407,
    "execution" : {
        "approximateSecondsBeforeTimedOut": number,
        "jobId" : "023",
        "status" : "QUEUED",
        "queuedAt" : 1489097374841,
        "lastUpdatedAt" : 1489097374841,
        "versionNumber" : 1,
        "jobDocument" : {
            < contents of job document >
        }
    }
}
```

Wenn die Anfrage fehlschlägt, veröffentlicht der AWS IoT Jobs-Service eine Nachricht zu dem `$aws/things/MyThing/jobs/0023/get/rejected` Thema.

Das Gerät verfügt jetzt über das Auftragsdokument, das es verwenden kann, um die Remoteoperationen für den Auftrag durchzuführen. Wenn das Auftragsdokument eine vorsignierte Amazon S3-URL enthält, kann das Gerät diese URL zum Download aller für den Auftrag erforderlicher Dateien verwenden.

## Melden des Status der Auftragsausführung

Wenn das Gerät den Auftrag ausführt, kann es die UpdateJobExecution-MQTT-API aufrufen, um den Status der Auftragsausführung zu aktualisieren.

Beispielsweise kann ein Gerät den Status der Auftragsausführung zu `IN_PROGRESS` aktualisieren, indem es die folgende Nachricht auf dem Thema `$aws/things/MyThing/jobs/0023/update` veröffentlicht:

```
{
    "status":"IN_PROGRESS",
    "statusDetails": {
        "progress":"50%"
    },
    "expectedVersion":"1",
    "clientToken":"client001"
}
```

Jobs reagiert mit der Veröffentlichung einer Nachricht auf das Thema `$aws/things/MyThing/jobs/0023/update/accepted` oder `$aws/things/MyThing/jobs/0023/update/rejected`:

```
{
    "clientToken":"client001",
    "timestamp":1476289222841
}
```

Das Gerät kann die beiden vorherigen Anforderungen durch den Aufruf von StartNextPendingJobExecution kombinieren. Dadurch wird die nächste ausstehende Auftragsausführung abgerufen und gestartet, und das Gerät kann den Auftragsausführungsstatus aktualisieren. Diese Anforderung gibt auch das Auftragsdokument aus, wenn eine Auftragsausführung aussteht.

Wenn der Job eine enthält TimeoutConfig, beginnt der Timer in Bearbeitung zu laufen. Sie können auch einen Schrittzeitgeber für die Ausführung eines Jobs festlegen, indem Sie einen Wert für den `stepTimeoutInMinutes` Zeitpunkt des Aufrufs UpdateJobExecutionfestlegen. Der Schritt Timer gilt nur für die Auftragsausführung, die Sie aktualisieren. Sie können einen neuen Wert für diesen Timer bei jeder Aktualisierung einer Auftragsausführung einrichten. Sie können beim Aufrufen auch einen Schritttimer erstellen StartNextPendingJobExecution. Falls die Auftragsausführung länger als das Schritt-Timer-Intervall im Status `IN_PROGRESS` bleibt, schlägt sie fehl und wechselt in den terminalen

Status `TIMED_OUT`. Der Schritt-Timer hat keine Auswirkungen auf den Timer „In Bearbeitung“, den Sie beim Erstellen eines Auftrags festlegen.

Das Feld `status` kann auf `IN_PROGRESS`, `SUCCEEDED` oder `FAILED` gesetzt werden. Der Status einer bereits im Status „Terminal“ befindlichen Auftragsausführung kann nicht aktualisiert werden.

## Meldung des Abschlusses der Ausführung

Wenn das Gerät die Ausführung des Auftrags abgeschlossen hat, ruft es die UpdateJobExecution-MQTT-API ab. Wenn der Auftrag erfolgreich war, setzen Sie `status` auf `SUCCEEDED`, und fügen Sie in `statusDetails` in der Nachrichtnutzlast weitere Informationen zu dem Auftrag als Name/Wert-Paare hinzu. Die Timer „In Bearbeitung“ und „Schritt“ enden, wenn die Auftragsausführung abgeschlossen ist.

Zum Beispiel:

```
{
    "status":"SUCCEEDED",
    "statusDetails": {
        "progress":"100%"
    },
    "expectedVersion":"2",
    "clientToken":"client-001"
}
```

Wenn der Auftrag nicht erfolgreich war, setzen Sie `status` auf `FAILED`, und fügen Sie in `statusDetails`Informationen zu dem aufgetretenen Fehler hinzu:

```
{
    "status":"FAILED",
    "statusDetails": {
        "errorCode":"101",
        "errorMsg":"Unable to install update"
    },
    "expectedVersion":"2",
    "clientToken":"client-001"
}
```

> **Note**
>
> Das Attribut `statusDetails` kann eine beliebige Zahl von Name/Wert-Paaren enthalten.

Wenn der AWS IoT Jobs-Service dieses Update erhält, veröffentlicht er eine Meldung zu diesem `$aws/things/MyThing/jobs/notify` Thema, um darauf hinzuweisen, dass die Jobausführung abgeschlossen ist:

```
{
    "timestamp":1476290692776,
    "jobs":{}
}
```

## Zusätzliche Aufträge

Wenn für das Gerät weitere Auftragsausführungen ausstehen, sind diese in der Nachricht enthalten, die für `$aws/things/MyThing/jobs/notify` veröffentlicht wurde.

Zum Beispiel:

```
{
    "timestamp":1476290692776,
    "jobs":{
        "QUEUED":[{
            "jobId":"0002",
            "queuedAt":1476290646230,
            "lastUpdatedAt":1476290646230
        }],
        "IN_PROGRESS":[{
            "jobId":"0003",
            "queuedAt":1476290646230,
            "lastUpdatedAt":1476290646230
        }]
    }
}
```

# Auftragsbenachrichtigungen

Der AWS IoT Jobs-Service veröffentlicht MQTT-Nachrichten zu reservierten Themen, wenn Jobs ausstehen oder wenn sich die erste Jobausführung in der Liste ändert. Geräte können ausstehende Aufträge verfolgen, indem sie diese Themen abonnieren.

## Auftrag-Benachrichtigungstypen

Auftragsbenachrichtigungen werden als JSON-Nutzlasten in MQTT-Themen veröffentlicht. Es gibt zwei Arten von Benachrichtigungen:

ListNotification

Eine `ListNotification` enthält eine Liste von höchstens 15 ausstehenden Auftragsausführungen. Sie nach Status (`IN_PROGRESS`-Auftragsausführungen vor `QUEUED`-Auftragsausführungen) und dann nach dem Zeitpunkt sortiert, an dem sie in die Warteschlange gestellt wurden.

Eine `ListNotification` wird veröffentlicht, sobald eines der folgenden Kriterien erfüllt ist.

- Eine neue Auftragsausführung wird in die Warteschlange gestellt oder ändert sich in einen Nicht-Endstatus (`IN_PROGRESS` oder `QUEUED`).
- Eine alte Auftragsausführung ändert sich in einen Endstatus (`FAILED`, `SUCCEEDED`, `CANCELED`, `TIMED_OUT`, `REJECTED` oder `REMOVED`).

Weitere Hinweise zu den Grenzwerten mit und ohne Zeitplankonfiguration finden Sie unterGrenzwerte für die Ausführung von Job.

NextNotification

- Eine `NextNotification` enthält zusammenfassende Informationen über die Auftragsausführung, die sich an der nächsten Stelle in der Warteschlange befindet.

  Eine `NextNotification` wird veröffentlicht, sobald sich die erste Auftragsausführung in der Liste ändert.

  - Eine neue Auftragsausführung wird der Liste als `QUEUED` hinzugefügt und ist die erste in der Liste.
  - Der Status einer vorhandenen Auftragsausführung, die nicht die erste in der Liste war, ändert sich von `QUEUED` in `IN_PROGRESS` und wird zur ersten in der Liste. (Dies passiert, wenn

sich in der Liste keine anderen `IN_PROGRESS`-Auftragsausführungen befinden und wenn die Auftragsausführung, deren Status sich von `QUEUED` in `IN_PROGRESS` geändert hat, früher als jede andere `IN_PROGRESS`-Auftragsausführung in der Liste in die Warteschlange gestellt wurde.)

- Der Status der Auftragsausführung, die sich an erster Stelle in der Liste befindet, ändert sich in den Endstatus und wird aus der Liste entfernt.

Für weitere Informationen zur Veröffentlichung und zum Abonnement von MQTT-Themen vgl. the section called “Gerätekommunikationsprotokolle”.

> **Note**
>
> Benachrichtigungen sind nicht verfügbar, wenn Sie die HTTP-Signaturversion 4 oder HTTP TLS für die Kommunikation mit Aufträgen verwenden.

## Ausstehender Auftrag

Der AWS IoT Jobs-Service veröffentlicht eine Nachricht zu einem MQTT-Thema, wenn ein Job zur Liste der ausstehenden Jobausführungen für eine Sache hinzugefügt oder daraus entfernt wird oder wenn sich die erste Jobausführung in der Liste ändert:

- `$aws/things/`*`thingName`*`/jobs/notify`
- `$aws/things/`*`thingName`*`/jobs/notify-next`

Die Nachricht enthält die folgende Beispielnutzlast:

`$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
    } ]
  }
}
```

Wenn die aufgerufene Auftragsausführung `this-job` aus einem Auftrag stammt, für den die optionale Planungskonfiguration ausgewählt wurde und der Rollout des Auftragsdokuments während eines Wartungsfensters geplant ist, wird sie nur in einem wiederkehrenden Wartungsfenster angezeigt. Außerhalb eines Wartungsfensters `this-job` wird der aufgerufene Auftrag aus der Liste der ausstehenden Auftragsausführungen ausgeschlossen, wie im folgenden Beispiel gezeigt.

```
{
  "timestamp" : 10011,
  "jobs" : {
    "IN_PROGRESS" : [ {
      "jobId" : "other-job",
      "queuedAt" : 10003,
      "lastUpdatedAt" : 10009,
      "executionNumber" : 1,
      "versionNumber" : 1
    } ],
    "QUEUED" : []
  }
}
```

`$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"}
```

```
  }
}
```

Wenn die aufgerufene Auftragsausführung `other-job` aus einem Auftrag stammt, für den die optionale Planungskonfiguration ausgewählt wurde und der Rollout des Auftragsdokuments während eines Wartungsfensters geplant ist, wird sie nur in einem wiederkehrenden Wartungsfenster angezeigt. Außerhalb eines Wartungsfensters wird der `other-job` aufgerufene Auftrag nicht als nächste Auftragsausführung aufgeführt, wie im folgenden Beispiel gezeigt.

```
{} //No other pending jobs
```

```
{
  "timestamp" : 10011,
  "execution" : {
      "jobId" : "this-job",
      "queuedAt" : 10011,
      "lastUpdatedAt" : 10011,
      "executionNumber" : 1,
      "versionNumber" : 0,
      "jobDocument" : {"a":"b"}
  }
} // "this-job" is pending next to "other-job"
```

Mögliche Statuswerte für die Auftragsausführungen sind `QUEUED`, `IN_PROGRESS`, `FAILED`, `SUCCEEDED`, `CANCELED`, `TIMED_OUT`, `REJECTED` und `REMOVED`.

Die folgende Reihe von Beispielen zeigt die in jedem Thema veröffentlichten Benachrichtigungen, wenn Auftragsausführungen angelegt und von einem Status in einen anderen geändert werden.

Zuerst wird ein Auftrag mit dem Namen `job1` erstellt. Diese Benachrichtigung wird im `jobs/notify`-Thema veröffentlicht:

```
{
  "timestamp": 1517016948,
  "jobs": {
    "QUEUED": [
      {
        "jobId": "job1",
        "queuedAt": 1517016947,
        "lastUpdatedAt": 1517016947,
```

```
        "executionNumber": 1,
        "versionNumber": 1
      }
    ]
  }
}
```

Diese Benachrichtigung wird im `jobs/notify-next`-Thema veröffentlicht:

```
{
  "timestamp": 1517016948,
  "execution": {
    "jobId": "job1",
    "status": "QUEUED",
    "queuedAt": 1517016947,
    "lastUpdatedAt": 1517016947,
    "versionNumber": 1,
    "executionNumber": 1,
    "jobDocument": {
      "operation": "test"
    }
  }
}
```

Wenn ein weiterer Auftrag erstellt wird (`job2`), wird diese Benachrichtigung im `jobs/notify`-Thema veröffentlicht:

```
{
  "timestamp": 1517017192,
  "jobs": {
    "QUEUED": [
      {
        "jobId": "job1",
        "queuedAt": 1517016947,
        "lastUpdatedAt": 1517016947,
        "executionNumber": 1,
        "versionNumber": 1
      },
      {
        "jobId": "job2",
        "queuedAt": 1517017191,
        "lastUpdatedAt": 1517017191,
        "executionNumber": 1,
```

```
        "versionNumber": 1
      }
    ]
  }
}
```

Es wird keine Benachrichtigung im `jobs/notify-next`-Thema veröffentlicht, da sich der nächste Auftrag in der Warteschlange (`job1`) nicht geändert hat. Wenn die Ausführung von `job1` beginnt, ändert sich der Status zu `IN_PROGRESS`. Es werden keine Benachrichtigungen veröffentlicht, da sich die Liste der Aufträge und der nächste Auftrag in der Warteschlange nicht geändert haben.

Wenn ein dritter Auftrag hinzugefügt wird (`job3`), wird diese Benachrichtigung im `jobs/notify`-Thema veröffentlicht:

```
{
  "timestamp": 1517017906,
  "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
      }
    ]
```

```
  }
}
```

Es wird keine Benachrichtigung im `jobs/notify-next`-Thema veröffentlicht, da der nächste Auftrag in der Warteschlange noch `job1` ist.

Wenn `job1` abgeschlossen ist, ändert sich sein Status zu `SUCCEEDED`. Diese Benachrichtigung wird im `jobs/notify`-Thema veröffentlicht:

```
{
  "timestamp": 1517186269,
  "jobs": {
    "QUEUED": [
      {
        "jobId": "job2",
        "queuedAt": 1517017191,
        "lastUpdatedAt": 1517017191,
        "executionNumber": 1,
        "versionNumber": 1
      },
      {
        "jobId": "job3",
        "queuedAt": 1517017905,
        "lastUpdatedAt": 1517017905,
        "executionNumber": 1,
        "versionNumber": 1
      }
    ]
  }
}
```

Jetzt wurde `job1` aus der Warteschlange entfernt, und die nächste auszuführenden Aufgabe ist `job2`. Diese Benachrichtigung wird im `jobs/notify-next`-Thema veröffentlicht:

```
{
  "timestamp": 1517186269,
  "execution": {
    "jobId": "job2",
    "status": "QUEUED",
    "queuedAt": 1517017191,
    "lastUpdatedAt": 1517017191,
    "versionNumber": 1,
```

```
    "executionNumber": 1,
    "jobDocument": {
      "operation": "test"
    }
  }
}
```

Wenn `job3` vor der Ausführung vor `job2` beginnen muss (was nicht empfehlenswert ist), kann der Status von `job3` zu `IN_PROGRESS` geändert werden. Wenn dies geschieht, ist `job2` nicht mehr der nächste Auftrag in der Warteschlange. Diese Benachrichtigung wird im `jobs/notify-next`-Thema veröffentlicht:

```
{
  "timestamp": 1517186779,
  "execution": {
    "jobId": "job3",
    "status": "IN_PROGRESS",
    "queuedAt": 1517017905,
    "startedAt": 1517186779,
    "lastUpdatedAt": 1517186779,
    "versionNumber": 2,
    "executionNumber": 1,
    "jobDocument": {
      "operation": "test"
    }
  }
}
```

Es wird keine Benachrichtigung im `jobs/notify`-Thema veröffentlicht, da kein Auftrag hinzugefügt oder entfernt wurde.

Wenn das Gerät `job2` ablehnt und seinen Status zu `REJECTED` aktualisiert, wird diese Benachrichtigung im `jobs/notify`-Thema veröffentlicht:

```
{
  "timestamp": 1517189392,
  "jobs": {
    "IN_PROGRESS": [
      {
        "jobId": "job3",
        "queuedAt": 1517017905,
        "lastUpdatedAt": 1517186779,
```

```
        "startedAt": 1517186779,
        "executionNumber": 1,
        "versionNumber": 2
      }
    ]
  }
}
```

Wenn das Löschen von `job3` (der noch ausgeführt wird) erzwungen wird, wird diese Benachrichtigung im `jobs/notify`-Thema veröffentlicht:

```
{
  "timestamp": 1517189551,
  "jobs": {}
}
```

An diesem Punkt ist die Warteschlange leer. Diese Benachrichtigung wird im `jobs/notify-next`-Thema veröffentlicht:

```
{
  "timestamp": 1517189551
}
```

# AWS IoT Jobs API-Operationen

AWS IoT Die Jobs-API kann für eine der folgenden Kategorien verwendet werden:

- Administrative Aufgaben wie die Verwaltung und Kontrolle von Aufträgen. Dies ist die Steuerebene.
- Geräte, die diese Aufgaben ausführen. Dies ist die Datenebene, mit der Sie Daten senden und empfangen können.

Die Auftragsverwaltung und die Auftragssteuerung verwenden eine HTTPS-Protokoll-API. Geräte können eine MQTT- oder eine HTTPS-Protokoll-API verwenden. Die Steuerebenen-API ist für eine geringe Anzahl von Aufrufen ausgelegt, wie sie für die Erstellung und Verfolgung von Aufträgen typisch sind. In der Regel öffnet sie eine Verbindung für eine einzelne Anforderung und schließt diese dann nach dem Eingang der Antwort. Die Datenebene HTTPS und die MQTT-API ermöglichen lange Abfragen. Diese API-Vorgänge sind für große Datenmengen ausgelegt, die auf Millionen von Geräten skaliert werden können.

Jede AWS IoT Jobs-HTTPS-API hat einen entsprechenden Befehl, mit dem Sie die API über AWS Command Line Interface (AWS CLI) aufrufen können. Die Befehle werden in Kleinbuchstaben mit Bindestrichen zwischen den Wörtern, aus denen die API besteht, ausgedrückt. Beispielsweise können Sie die `CreateJob`-API in der CLI aufrufen, indem Sie Folgendes eingeben:

```
aws iot create-job ...
```

Wenn während eines Vorgangs ein Fehler auftritt, erhalten Sie eine Fehlerantwort, die Informationen über den Fehler enthält.

## ErrorResponse

Enthält Informationen zu einem Fehler, der während einer Operation des AWS IoT Jobs-Service aufgetreten ist.

Das folgende Beispiel zeigt die Syntax dieser Operation:

```
{
    "code": "ErrorCode",
    "message": "string",
    "clientToken": "string",
    "timestamp": timestamp,
    "executionState": JobExecutionState
}
```

Im Folgenden finden Sie eine Beschreibung dieser `ErrorResponse`:

`code`

ErrorCode kann wie folgt eingestellt werden:

InvalidTopic

Die Anfrage wurde an ein Thema im AWS IoT Jobs-Namespace gesendet, das keiner API-Operation zugeordnet ist.

InvalidJson

Der Inhalt der Anforderung konnte nicht als gültiger nach UTF-8 kodierter JSON-Inhalt interpretiert werden.

InvalidRequest

Der Inhalt der Anforderung war nicht gültig. Dieser Code wird beispielsweise ausgegeben, wenn eine `UpdateJobExecution`-Anforderung ungültige Statusdetails enthält. Die Mitteilung enthält Einzelheiten zu dem Fehler.

InvalidStateTransition

Bei einem Update wurde versucht, die Auftragsausführung in einen Status zu ändern, der aufgrund des aktuellen Status der Auftragsausführung nicht gültig ist. Beispiel: Ein Versuch, eine Anforderung im Status SUCCEED in den Status IN_PROGRESS zu ändern. In diesem Fall enthält der Text der Fehlermeldung auch das Feld `executionState`.

ResourceNotFound

Die von dem Anforderungsthema angegebene `JobExecution` ist nicht vorhanden.

VersionMismatch

Die in der Anfrage angegebene erwartete Version stimmt nicht mit der Version der Jobausführung im AWS IoT Jobs-Service überein. In diesem Fall enthält der Text der Fehlermeldung auch das Feld `executionState`.

InternalError

Bei der Verarbeitung der Anforderung ist ein interner Fehler aufgetreten.

RequestThrottled

Die Anforderung wurde gedrosselt.

TerminalStateReached

Tritt auf, wenn ein Befehl zum Beschreiben eines Auftrags für einen Auftrag im Status „Terminal“ durchgeführt wird.

`message`

Eine Fehlermeldungszeichenfolge.

`clientToken`

Eine beliebige Zeichenfolge für die Korrelierung einer Anforderung mit der jeweiligen Antwort.

`timestamp`

Die seit der Epoche vergangene Zeit (in Sekunden).

`executionState`

Ein `JobExecutionState`-Objekt. Dieses Feld ist nur enthalten, wenn das Feld `code` den Wert `InvalidStateTransition` oder `VersionMismatch` hat. Dadurch ist es in diesen Fällen nicht erforderlich, eine separate `DescribeJobExecution`-Anforderung durchzuführen, um die Daten zum Status der aktuellen Auftragsausführung abzurufen.

Im Folgenden werden die Operationen und Datentypen der Jobs API aufgeführt.

- Auftragsverwaltung und -steuerung API und Datentypen
- Aufträge, Geräte, MQTT- und HTTPS-API-Operationen und Datentypen

## Auftragsverwaltung und -steuerung API und Datentypen

Die folgenden Befehle sind für die Verwaltung und Steuerung von Aufträgen in der CLI und über das HTTPS-Protokoll verfügbar.

- Datentypen für Auftragsverwaltung und -steuerung
- API-Operationen zur Auftragsverwaltung und -steuerung

Führen Sie diesen Befehl aus, um den *`endpoint-url`* Parameter für Ihre CLI-Befehle zu ermitteln.

```
aws iot describe-endpoint --endpoint-type=iot:Jobs
```

Dieser Befehl gibt die folgende Ausgabe zurück.

```
{
"endpointAddress": "account-specific-prefix.jobs.iot.aws-region.amazonaws.com"
}
```

> **Note**
>
> Der Jobs-Endpunkt unterstützt ALPN `x-amzn-http-ca` nicht.

## Datentypen für Auftragsverwaltung und -steuerung

Die folgenden Datentypen werden von Verwaltungs- und Steuerungsanwendungen für die Kommunikation mit AWS IoT Jobs verwendet.

### Aufgabe

Das Objekt `Job` enthält Details zu einem Auftrag. Im folgenden Beispiel wird die Syntax dargestellt:

```
{
    "jobArn": "string",
    "jobId": "string",
    "status": "IN_PROGRESS|CANCELED|SUCCEEDED",
    "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,
        "numberOfTimedOutThings": long
    },
    "presignedUrlConfig": {
        "expiresInSec": number,
        "roleArn": "string"
    },
    "jobExecutionsRolloutConfig": {
        "exponentialRate": {
           "baseRatePerMinute": integer,
           "incrementFactor": integer,
           "rateIncreaseCriteria": {
              "numberOfNotifiedThings": integer, // Set one or the other
              "numberOfSucceededThings": integer // of these two values.
           },
```

```
            "maximumPerMinute": integer
      }
    },
    "abortConfig": {
       "criteriaList": [
          {
             "action": "string",
             "failureType": "string",
             "minNumberOfExecutedThings": integer,
             "thresholdPercentage": integer
          }
       ]
    },
    "SchedulingConfig": {
      "startTime": string
      "endTime": string
      "timeZone": string


      "endTimeBehavior": string

   },
    "timeoutConfig": {
        "inProgressTimeoutInMinutes": long
    }
}
```

Weitere Informationen finden Sie unter Job oder job.

JobSummary

Das Objekt JobSummary enthält eine Auftragszusammenfassung. Im folgenden Beispiel wird die Syntax dargestellt:

```
{
    "jobArn": "string",
    "jobId": "string",
    "status": "IN_PROGRESS|CANCELED|SUCCEEDED|SCHEDULED",
    "targetSelection": "CONTINUOUS|SNAPSHOT",
    "thingGroupId": "string",
    "createdAt": timestamp,
    "lastUpdatedAt": timestamp,
    "completedAt": timestamp
```

```
}
```

Weitere Informationen finden Sie unter `JobSummary` oder `job-summary`.

JobExecution

Das Objekt `JobExecution` repräsentiert die Ausführung eines Auftrags auf einem Gerät. Im folgenden Beispiel wird die Syntax dargestellt:

> **Note**
>
> Wenn Sie die API-Operationen der Steuerebene verwenden, enthält der Datentyp `JobExecution` kein `JobDocument`-Feld. Um diese Informationen zu erhalten, können Sie die `GetJobDocument` API-Operation oder den `get-job-document` CLI-Befehl verwenden.

```
{
    "approximateSecondsBeforeTimedOut": 50,
    "executionNumber": 1234567890,
    "forceCanceled": true|false,
    "jobId": "string",
    "lastUpdatedAt": timestamp,
    "queuedAt": timestamp,
    "startedAt": timestamp,
    "status": "QUEUED|IN_PROGRESS|FAILED|SUCCEEDED|CANCELED|TIMED_OUT|REJECTED|
REMOVED",
    "forceCanceled": boolean,
    "statusDetails": {
        "detailsMap": {
            "string": "string" ...
        },
        "status": "string"
    },
    "thingArn": "string",
    "versionNumber": 123
}
```

Weitere Informationen finden Sie unter `JobExecution` oder `job-execution`.

JobExecutionSummary

Das `JobExecutionSummary`-Objekt enthält zusammenfassende Informationen zur Auftragsausführung. Im folgenden Beispiel wird die Syntax dargestellt:

```
{
    "executionNumber": 1234567890,
    "queuedAt": timestamp,
    "lastUpdatedAt": timestamp,
    "startedAt": timestamp,
    "status": "QUEUED|IN_PROGRESS|FAILED|SUCCEEDED|CANCELED|TIMED_OUT|REJECTED|REMOVED"
}
```

Weitere Informationen finden Sie unter `JobExecutionSummary` oder `job-execution-summary`.

JobExecutionSummaryForJob

Das Objekt `JobExecutionSummaryForJob` enthält eine Zusammenfassung der Informationen zu Auftragsausführungen für einen bestimmten Auftrag. Im folgenden Beispiel wird die Syntax dargestellt:

```
{
    "executionSummaries": [
        {
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyThing",
            "jobExecutionSummary": {
                "status": "IN_PROGRESS",
                "lastUpdatedAt": 1549395301.389,
                "queuedAt": 1541526002.609,
                "executionNumber": 1
            }
        },
        ...
    ]
}
```

Weitere Informationen finden Sie unter `JobExecutionSummaryForJob` oder `job-execution-summary-for-job`.

JobExecutionSummaryForThing

Das `JobExecutionSummaryForThing` Objekt enthält eine Zusammenfassung von Informationen über die Ausführung eines Jobs an einem bestimmten Objekt. FThe Das folgende Beispiel zeigt die Syntax:

```
{
    "executionSummaries": [
        {
            "jobExecutionSummary": {
                "status": "IN_PROGRESS",
                "lastUpdatedAt": 1549395301.389,
                "queuedAt": 1541526002.609,
                "executionNumber": 1
            },
            "jobId": "MyThingJob"
        },
        ...
    ]
}
```

Weitere Informationen finden Sie unter `JobExecutionSummaryForThing` oder `job-execution-summary-for-thing`.

## API-Operationen zur Auftragsverwaltung und -steuerung

Verwenden Sie die folgenden API-Vorgänge oder CLI-Befehle:

AssociateTargetsWithJob

Weist eine Gruppe einem kontinuierlichen Auftrag zu. Die folgenden Kriterien müssen erfüllt sein:

- Der Auftrag muss mit der Einstellung des Feldes `targetSelection` auf `CONTINUOUS` erstellt worden sein.
- Der Auftrag muss den Status `IN_PROGRESS` haben.
- Die Gesamtzahl der mit einem Auftrag verbundenen Ziele darf 100 nicht überschreiten.

HTTPS request

```
POST /jobs/jobId/targets
```

```
{
"targets": [ "string" ],
"comment": "string"
}
```

Weitere Informationen finden Sie unter AssociateTargetsWithJob.

CLI syntax

```
aws iot  associate-targets-with-job \
--targets <value> \
--job-id <value> \
[--comment <value>]  \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

`cli-input-json` format:

```
{
"targets": [
"string"
],
"jobId": "string",
"comment": "string"
}
```

Weitere Informationen finden Sie unter associate-targets-with-job.

CancelJob

Bricht einen Auftrag ab.

HTTPS request

```
PUT /jobs/jobId/cancel

{
"force": boolean,
"comment": "string",
"reasonCode": "string"
```

```
}
```

Weitere Informationen finden Sie unter CancelJob.

CLI syntax

```
aws iot cancel-job \
    --job-id <value> \
    [--force <value>]  \
    [--comment <value>]  \
    [--reasonCode <value>]  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` format:

```
{
    "jobId": "string",
    "force": boolean,
    "comment": "string"
}
```

Weitere Informationen finden Sie unter cancel-job.

CancelJobExecution

Bricht eine Auftragsausführung auf einem Gerät ab.

HTTPS request

```
PUT /things/thingName/jobs/jobId/cancel

{
"force": boolean,
"expectedVersion": "string",
"statusDetails": {
    "string": "string"
    ...
}
}
```

Weitere Informationen finden Sie unter CancelJobExecution.

CLI syntax

```
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"
}
}
```

Weitere Informationen finden Sie unter `cancel-job-execution`.

CreateJob

Erstellt einen Auftrag. Sie können das Auftragsdokument als Link zu einer Datei in einem Amazon S3-Bucket (Parameter `documentSource`) oder im Text der Anfrage (Parameter `document`) bereitstellen.

Ein Auftrag kann kontinuierlich gemacht werden, indem Sie den optionalen Parameter `targetSelection` auf `CONTINUOUS` setzen (der Standard ist `SNAPSHOT`). Ein kontinuierlicher Auftrag kann verwendet werden, um Geräte zu integrieren oder zu aktualisieren, wenn sie zu einer Gruppe hinzugefügt werden, da er weiterhin ausgeführt wird und für neu hinzugefügte Objekte gestartet wird. Dies kann auch dann der Fall sein, wenn die Objekte, die sich zum Zeitpunkt der Auftragserstellung in der Gruppe befanden, den Auftrag abgeschlossen haben.

Ein Job kann einen optionalen Wert haben TimeoutConfig, der den Wert des Timers für die Bearbeitung festlegt. Der Timer für „In Bearbeitung“ kann nicht aktualisiert werden und gilt für alle Ausführungen des Auftrags.

Die folgenden Validierungen werden auf Argumenten der `CreateJob`-API durchgeführt:

- Das `targets` Argument muss eine Liste gültiger Dinge oder Dinggruppen ARNs sein. Alle Dinge und Dinggruppen müssen in Ihrer sein AWS-Konto.
- Das Argument `documentSource` muss eine gültige Amazon S3-URL zu einem Auftragsdokument sein. Amazon S3 URLs haben das Format:`https://s3.amazonaws.com/`*`bucketName`*`/`*`objectName`*.
- Das in der vom Argument `documentSource` angegebenen URL gespeicherte Dokument muss ein nach UTF-8 kodiertes JSON-Dokument sein.
- Die Größe eines Auftragsdokuments ist aufgrund der Größenbeschränkung für eine MQTT-Nachricht (128 KB) und die Verschlüsselung auf 32 KB begrenzt.
- Das `jobId` muss in Ihrem einzigartig sein AWS-Konto.

HTTPS request

```
PUT /jobs/jobId

{
"targets": [ "string" ],
"document": "string",
"documentSource": "string",
"description": "string",
"jobTemplateArn": "string",
"presignedUrlConfigData": {
    "roleArn": "string",
    "expiresInSec": "integer"
},
"targetSelection": "CONTINUOUS|SNAPSHOT",
"jobExecutionsRolloutConfig": {
    "exponentialRate": {
       "baseRatePerMinute": integer,
       "incrementFactor": integer,
       "rateIncreaseCriteria": {
          "numberOfNotifiedThings": integer, // Set one or the other
          "numberOfSucceededThings": integer // of these two values.
       },
       "maximumPerMinute": integer
  }
},
"abortConfig": {
```

```
   "criteriaList": [
      {
         "action": "string",
         "failureType": "string",
         "minNumberOfExecutedThings": integer,
         "thresholdPercentage": integer
      }
   ]
},
"SchedulingConfig": {
    "startTime": string
    "endTime": string
    "timeZone": string


    "endTimeBehavior": string

   }
"timeoutConfig": {
  "inProgressTimeoutInMinutes": long
}
}
```

Weitere Informationen finden Sie unter [CreateJob](#).

CLI syntax

```
aws iot create-job \
    --job-id <value> \
    --targets <value> \
    [--document-source <value>] \
    [--document <value>] \
    [--description <value>] \
    [--job-template-arn <value>] \
    [--presigned-url-config <value>] \
    [--target-selection <value>] \
    [--job-executions-rollout-config <value>] \
    [--abort-config <value>] \
    [--timeout-config <value>] \
    [--document-parameters <value>]  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` format:

```
{
    "jobId": "string",
    "targets": [ "string" ],
    "documentSource": "string",
    "document": "string",
    "description": "string",
    "jobTemplateArn": "string",
    "presignedUrlConfig": {
        "roleArn": "string",
        "expiresInSec": long
     },
    "targetSelection": "string",
    "jobExecutionsRolloutConfig": {
          "exponentialRate": {
              "baseRatePerMinute": integer,
              "incrementFactor": integer,
              "rateIncreaseCriteria": {
                 "numberOfNotifiedThings": integer, // Set one or the other
                 "numberOfSucceededThings": integer // of these two values.
              },
      "maximumPerMinute": integer
      }
    },
    "abortConfig": {
    "criteriaList": [
        {
           "action": "string",
           "failureType": "string",
           "minNumberOfExecutedThings": integer,
           "thresholdPercentage": integer
         }
      ]
    },
    "timeoutConfig": {
          "inProgressTimeoutInMinutes": long
    },
    "documentParameters": {
    "string": "string"
    }
}
```

Weitere Informationen finden Sie unter [create-job](#).

DeleteJob

Löscht einen Auftrag und die damit verbundenen Auftragsausführungen.

Das Löschen eines Auftrags kann einige Zeit in Anspruch nehmen, abhängig von der Anzahl der Auftragsausführungen für den Auftrag und verschiedenen anderen Faktoren. Während der Auftrag gelöscht wird, wird der Status des Auftrags als „DELETION_IN_PROGRESS“ angezeigt. Der Versuch, einen Auftrag zu löschen oder abzubrechen, dessen Status bereits „DELETION_IN_PROGRESS“ ist, führt zu einem Fehler.

HTTPS request

```
DELETE /jobs/jobId?force=force
```

Weitere Informationen finden Sie unter DeleteJob.

CLI syntax

```
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
}
```

Weitere Informationen finden Sie unter delete-job.

DeleteJobExecution

Löscht eine Auftragsausführung.

HTTPS request

```
DELETE /things/thingName/jobs/jobId/executionNumber/executionNumber?force=force
```

Weitere Informationen finden Sie unter DeleteJobExecution.

CLI syntax

```
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:

```
{
"jobId": "string",
"thingName": "string",
"executionNumber": long,
"force": boolean
}
```

Weitere Informationen finden Sie unter delete-job-execution.

DescribeJob

Ruft die Details der Auftragsausführung ab.

HTTPS request

```
GET /jobs/jobId
```

Weitere Informationen finden Sie unter DescribeJob.

CLI syntax

```
aws iot describe-job \
--job-id <value>  \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

`cli-input-json` format:

```
{
"jobId": "string"
}
```

Weitere Informationen finden Sie unter describe-job.

DescribeJobExecution

Ruft Details einer Auftragsausführung ab. Der Ausführungsstatus des Auftrags muss SUCCEEDED oder FAILED sein.

HTTPS request

```
GET /things/thingName/jobs/jobId?executionNumber=executionNumber
```

Weitere Informationen finden Sie unter DescribeJobExecution.

CLI syntax

```
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
}
```

Weitere Informationen finden Sie unter describe-job-execution.

GetJobDocument

Ruft das Auftragsdokument für einen Auftrag ab.

> **Note**
>
> Platzhalter URLs werden in dem zurückgesandten Dokument nicht durch vorsignierte Amazon S3 URLs ersetzt. Vorsignierte URLs werden nur generiert, wenn der AWS IoT Jobs-Service eine Anfrage über MQTT erhält.

HTTPS request

```
GET /jobs/jobId/job-document
```

Weitere Informationen finden Sie unter GetJobDocument.

CLI syntax

```
aws iot get-job-document \
--job-id <value>  \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

`cli-input-json` format:

```
{
"jobId": "string"
}
```

Weitere Informationen finden Sie unter get-job-document.

ListJobExecutionsForJob

Ruft eine Liste der Auftragsausführungen für einen Auftrag ab.

HTTPS request

```
GET /jobs/jobId/things?status=status&maxResults=maxResults&nextToken=nextToken
```

Weitere Informationen finden Sie unter ListJobExecutionsForJob.

CLI syntax

```
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"
}
```

Weitere Informationen finden Sie unter `list-job-executions-for-job`.

### ListJobExecutionsForThing

Ruft eine Liste der Auftragsausführungen für ein Objekt ab.

HTTPS request

```
GET /things/thingName/jobs?status=status&maxResults=maxResults&nextToken=nextToken
```

Weitere Informationen finden Sie unter `ListJobExecutionsForThing`.

CLI syntax

```
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"
}
```

Weitere Informationen finden Sie unter list-job-executions-for-thing.

ListJobs

Ruft eine Liste der Jobs in Ihrem ab. AWS-Konto

HTTPS request

```
GET /jobs?
status=status&targetSelection=targetSelection&thingGroupName=thingGroupName&thingGroupId=thi
```

Weitere Informationen finden Sie unter ListJobs.

CLI syntax

```
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"
}
```

Weitere Informationen finden Sie unter `list-jobs`.

### UpdateJob

Aktualisiert unterstützte Felder des angegebenen Auftrags. Aktualisierte Werte für `timeoutConfig` werden nur für neu begonnen Launches wirksam. Derzeit werden laufende Starts weiterhin mit der vorherigen Timeout-Konfiguration gestartet.

#### HTTPS request

```
PATCH /jobs/jobId
{
"description": "string",
"presignedUrlConfig": {
  "expiresInSec": number,
  "roleArn": "string"
},
"jobExecutionsRolloutConfig": {
  "exponentialRate": {
     "baseRatePerMinute": number,
     "incrementFactor": number,
     "rateIncreaseCriteria": {
        "numberOfNotifiedThings": number,
        "numberOfSucceededThings": number
     },
  "maximumPerMinute": number
  },
"abortConfig": {
  "criteriaList": [
     {
        "action": "string",
        "failureType": "string",
        "minNumberOfExecutedThings": number,
        "thresholdPercentage": number
     }
  ]
},
"timeoutConfig": {
  "inProgressTimeoutInMinutes": number
}
}
```

Weitere Informationen finden Sie unter `UpdateJob`.

CLI syntax

```
aws iot  update-job \
--job-id <value> \
[--description <value>] \
[--presigned-url-config <value>] \
[--job-executions-rollout-config <value>] \
[--abort-config <value>] \
[--timeout-config <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

`cli-input-json` format:

```
{
"description": "string",
"presignedUrlConfig": {
  "expiresInSec": number,
  "roleArn": "string"
},
"jobExecutionsRolloutConfig": {
  "exponentialRate": {
     "baseRatePerMinute": number,
     "incrementFactor": number,
     "rateIncreaseCriteria": {
        "numberOfNotifiedThings": number,
        "numberOfSucceededThings": number
     }
  },
  "maximumPerMinute": number
},
"abortConfig": {
  "criteriaList": [
     {
        "action": "string",
        "failureType": "string",
        "minNumberOfExecutedThings": number,
        "thresholdPercentage": number
     }
  ]
},
"timeoutConfig": {
```

```
  "inProgressTimeoutInMinutes": number
}
}
```

Weitere Informationen finden Sie unter [update-job](#).

## Aufträge, Geräte, MQTT- und HTTPS-API-Operationen und Datentypen

Die folgenden Befehle stehen über die Protokolle MQTT und HTTPS zur Verfügung. Verwenden Sie diese API-Operationen auf der Datenebene für Geräte, die die Aufträge ausführen.

### Geräte, MQTT- und HTTPS-Datentypen

Die folgenden Datentypen werden für die Kommunikation mit dem AWS IoT Jobs-Dienst über die Protokolle MQTT und HTTPS verwendet.

JobExecution

Das Objekt `JobExecution` repräsentiert die Ausführung eines Auftrags auf einem Gerät. Im folgenden Beispiel wird die Syntax dargestellt:

> **Note**
>
> Wenn Sie die API-Operationen MQTT und HTTP für die Datenebene verwenden, enthält der Datentyp `JobExecution` ein `JobDocument`-Feld. Ihre Geräte können diese Informationen verwenden, um das Auftragsdokument aus einer Auftragsausführung abzurufen.

```
{
    "jobId" : "string",
    "thingName" : "string",
    "jobDocument" : "string",
    "status": "QUEUED|IN_PROGRESS|FAILED|SUCCEEDED|CANCELED|TIMED_OUT|REJECTED|
REMOVED",
    "statusDetails": {
        "string": "string"
    },
    "queuedAt" : "timestamp",
    "startedAt" : "timestamp",
    "lastUpdatedAt" : "timestamp",
```

```
    "versionNumber" : "number",
    "executionNumber": long
}
```

Weitere Informationen finden Sie unter JobExecution oder job-execution.

JobExecutionState

Das JobExecutionState enthält Informationen über den Status einer Auftragsausführung. Im folgenden Beispiel wird die Syntax dargestellt:

```
{
    "status": "QUEUED|IN_PROGRESS|FAILED|SUCCEEDED|CANCELED|TIMED_OUT|REJECTED|
REMOVED",
    "statusDetails": {
        "string": "string"
        ...
    }
    "versionNumber": "number"
}
```

Weitere Informationen finden Sie unter JobExecutionState oder job-execution-state.

JobExecutionSummary

Enthält einen Teil der Informationen zu einer Auftragsausführung. Im folgenden Beispiel wird die Syntax dargestellt:

```
{
    "jobId": "string",
    "queuedAt": timestamp,
    "startedAt": timestamp,
    "lastUpdatedAt": timestamp,
    "versionNumber": "number",
    "executionNumber": long
}
```

Weitere Informationen finden Sie unter JobExecutionSummary oder job-execution-summary.

In den folgenden Abschnitten erfahren Sie mehr über die MQTT- und HTTPS-API-Operationen:

- Führt MQTT-API-Operationen auf dem Gerät aus

- HTTP-API für Aufträge-Geräte

## Führt MQTT-API-Operationen auf dem Gerät aus

Sie können Gerätebefehle für Aufträge ausgeben, indem Sie MQTT-Nachrichten in den für Auftragsbefehle verwendeten reservierten Themen veröffentlichen.

Ihr geräteseitiger Client muss die Antwortnachrichten-Themen dieser Befehle abonniert haben. Wenn Sie den AWS IoT Geräteclient verwenden, abonniert Ihr Gerät automatisch die Antwortthemen. Das bedeutet, dass der Message Broker die Themen der Antwortnachricht auf dem Client veröffentlicht, der die Befehlsnachricht veröffentlicht hat, unabhängig davon, ob Ihr Client die Themen der Antwortnachricht abonniert hat oder nicht. Diese Antwortnachrichten werden nicht durch den Message Broker weitergeleitet und können auch nicht von anderen Clients oder Regeln abonniert werden.

Wenn Sie den Auftrag und die `jobExecution` Ereignisthemen für Ihre Flottenüberwachungslösung abonnieren, aktivieren Sie zunächst die Aufgaben- und Auftragsausführungsereignisse, um alle Ereignisse auf der Cloud-Seite zu empfangen. Auftragsfortschrittsnachrichten, die über den Message Broker verarbeitet werden und von AWS IoT -Regeln verwendet werden können, werden veröffentlicht als Auftragsereignisse. Da der Message Broker Antwortnachrichten auch ohne ausdrückliches Abonnement veröffentlicht, muss Ihr Client so konfiguriert sein, dass er die empfangenen Nachrichten empfängt und identifiziert. Ihr Kunde muss außerdem bestätigen, dass das Thema *`thingName`* in der eingehenden Nachricht für den Dingnamen des Kunden gilt, bevor der Client auf die Nachricht reagiert.

> **Note**
>
> Nachrichten, die als Antwort auf MQTT Jobs API-Befehlsnachrichten AWS IoT gesendet werden, werden Ihrem Konto in Rechnung gestellt, unabhängig davon, ob Sie sie explizit abonniert haben oder nicht.

Im Folgenden werden die MQTT-API-Operationen und ihre Anfrage- und Antwortsyntax gezeigt. Alle MQTT-API-Operationen haben die folgenden Parameter:

clientToken

Ein optionaler Client-Token zur Korrelierung von Anforderungen und Antworten. Geben Sie hier einen beliebigen Wert ein, und dieser wird in der Antwort reflektiert.

`timestamp`

Die Zeit in Sekunden seit der Epoche, in der die Nachricht gesendet wurde, vergangene Zeit.

GetPendingJobExecutions

Ruft die Liste aller Aufträge für ein bestimmtes Objekt ab, die sich nicht in einem Terminal-Zustand befinden.

Veröffentlichen Sie zum Aufruf dieser API eine Nachricht auf `$aws/things/thingName/jobs/get`.

Anforderungsnutzlast:

```
{ "clientToken": "string" }
```

Der Message Broker veröffentlicht `$aws/things/thingName/jobs/get/accepted` und `$aws/things/thingName/jobs/get/rejected` auch ohne ein bestimmtes Abonnement. Damit Ihr Kunde die Nachrichten empfangen kann, muss er sie jedoch abhören. Weitere Informationen finden Sie in der Anmerkung zu Jobs API-Nachrichten.

Antwortnutzlast:

```
{
"inProgressJobs" : [ JobExecutionSummary ... ],
"queuedJobs" : [ JobExecutionSummary ... ],
"timestamp" : 1489096425069,
"clientToken" : "client-001"
}
```

Wenn `inProgressJobs` und `queuedJobs` eine Liste von JobExecutionSummary Objekten zurückgibt, die den Status `IN_PROGRESS` oder `QUEUED` haben.

StartNextPendingJobExecution

Ruft die nächste anstehende Auftragsausführung für ein Objekt ab und startet sie (Status `IN_PROGRESS` oder `QUEUED`).

- Alle Auftragsausführungen mit dem Status `IN_PROGRESS` werden zuerst zurückgegeben.
- Auftragsausführungen werden in der Reihenfolge zurückgegeben, in der sie zur Warteschlange hinzugefügt wurden. Wenn der Zielgruppe für Ihren Auftrag etwas hinzugefügt oder daraus entfernt

wird, überprüfen Sie die Rollout-Reihenfolge aller neuen Auftragsausführungen im Vergleich zu bestehenden Auftragsausführungen.

- Wenn die nächste ausstehende Auftragsausführung den Status `QUEUED` hat, wechselt ihr Status zu `IN_PROGRESS`, und die Statusdetails der Auftragsausführung werden wie angegeben eingerichtet.
- Wenn die nächste ausstehende Auftragsausführung bereits den Status `IN_PROGRESS` hat, werden ihre Statusdetails nicht geändert.
- Wenn keine Auftragsausführungen ausstehen, enthält die Antwort das Feld `execution` nicht.
- Optional können Sie einen Schritt-Timer erstellen, indem Sie einen Wert für die `stepTimeoutInMinutes`-Eigenschaft angeben. Falls Sie den Wert dieser Eigenschaft nicht aktualisieren, indem Sie `UpdateJobExecution` ausführen, läuft die Auftragsausführung ab, wenn der Schritt-Timer abläuft.

Veröffentlichen Sie zum Aufruf dieser API eine Nachricht auf `$aws/things/`*`thingName`*`/jobs/start-next`.

Anforderungsnutzlast:

```
{
"statusDetails": {
    "string": "job-execution-state"
    ...
},
"stepTimeoutInMinutes": long,
"clientToken": "string"
}
```

`statusDetails`

Eine Sammlung von Name/Wert-Paaren, die den Status der Auftragsausführung beschreiben. Wenn nicht angegeben, sind die `statusDetails` nicht geändert.

`stepTimeOutInMinutes`

Gibt die Dauer an, die dieses Gerät für den Abschluss der Ausführung dieses Auftrags hat. Wenn der Status der Auftragsausführung vor Ablauf oder Zurücksetzen des Timers (durch Aufrufen von `UpdateJobExecution`, Setzen des Status auf `IN_PROGRESS` und Angeben eines neuen Zeitüberschreitungswerts im Feld `stepTimeoutInMinutes`) auf keinen Terminal-Zustand gesetzt wird, wird der Status der Auftragsausführung auf `TIMED_OUT` gesetzt. Das Festlegen dieser Zeitüberschreitung hat keinen Einfluss auf die Zeitüberschreitung für

die Auftragsausführung, die möglicherweise beim Erstellen des Auftrags festgelegt wurde (`CreateJob` mithilfe des Feldes `timeoutConfig`).

Gültige Werte für diesen Parameter liegen im Bereich von 1 bis 10 080 (1 Minute bis 7 Tage). Ein Wert von -1 ist ebenfalls gültig und beendet den aktuellen Step-Timer (der durch eine frühere Verwendung von UpdateJobExecutionRequest erstellt wurde).

Der Message Broker veröffentlicht `$aws/things/`*`thingName`*`/jobs/start-next/accepted` und `$aws/things/`*`thingName`*`/jobs/start-next/rejected` auch ohne ein bestimmtes Abonnement. Damit Ihr Kunde die Nachrichten empfangen kann, muss er sie jedoch abhören. Weitere Informationen finden Sie in der Anmerkung zu Jobs API-Nachrichten.

Antwortnutzlast:

```
{
"execution" : JobExecutionData,
"timestamp" : timestamp,
"clientToken" : "string"
}
```

Wo `execution` ein JobExecution-Objekt ist. Zum Beispiel:

```
{
"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,
}
```

DescribeJobExecution

Ruft detaillierte Informationen zu einer Auftragsausführung ab.

Sie können die `jobId` auf `$next` setzen, um die nächste ausstehende Auftragsausführung für ein Objekt (mit Status `IN_PROGRESS` oder `QUEUED`) zurückzugeben.

Veröffentlichen Sie zum Aufruf dieser API eine Nachricht auf `$aws/things/`*`thingName`*`/jobs/`*`jobId`*`/get`.

Anforderungsnutzlast:

```
{
"jobId" : "022",
"thingName" : "MyThing",
"executionNumber": long,
"includeJobDocument": boolean,
"clientToken": "string"
}
```

`thingName`

Der Name des dem Gerät zugeordneten Objekts.

`jobId`

Die eindeutige Kennung, die diesem Auftrag bei seiner Erstellung zugewiesen wurde.

Sie können `$next` verwenden, um die nächste ausstehende Auftragsausführung für ein Objekt (mit Status `IN_PROGRESS` oder `QUEUED`) zurückzugeben. In diesem Fall werden alle Auftragsausführungen mit dem Status `IN_PROGRESS` zuerst zurückgegeben. Auftragsausführungen werden in der Reihenfolge zurückgegeben, in der sie erstellt wurden.

`executionNumber`

(Optional) Eine Nummer, die eine Auftragsausführung auf einem Gerät identifiziert. Wenn nicht angegeben, wird die letzte Auftragsausführung zurückgegeben.

`includeJobDocument`

(Optional) Sofern nicht auf `false` gesetzt, enthält die Antwort das Auftragsdokument. Der Standardwert ist `true`.

Der Message Broker veröffentlicht `$aws/things/`*`thingName`*`/jobs/`*`jobId`*`/get/accepted` und `$aws/things/`*`thingName`*`/jobs/`*`jobId`*`/get/rejected` auch ohne ein bestimmtes Abonnement. Damit Ihr Kunde die Nachrichten empfangen kann, muss er sie jedoch abhören. Weitere Informationen finden Sie in der Anmerkung zu Jobs API-Nachrichten.

Antwortnutzlast:

```
{
"execution" : JobExecutionData,
"timestamp": "timestamp",
"clientToken": "string"
}
```

Wo `execution` ein JobExecution-Objekt ist.

UpdateJobExecution

Aktualisiert den Status einer Auftragsausführung. Sie können optional einen Schritt-Timer erstellen, indem Sie einen Wert für die `stepTimeoutInMinutes`-Eigenschaft angeben. Falls Sie den Wert dieser Eigenschaft nicht aktualisieren, indem Sie `UpdateJobExecution` erneut ausführen, läuft die Auftragsausführung ab, wenn der Schritt-Timer abläuft.

Veröffentlichen Sie zum Aufruf dieser API eine Nachricht auf `$aws/things/`*`thingName`*`/jobs/`*`jobId`*`/update`.

Anforderungsnutzlast:

```
{
"status": "job-execution-state",
"statusDetails": {
    "string": "string"
    ...
},
"expectedVersion": "number",
"executionNumber": long,
"includeJobExecutionState": boolean,
"includeJobDocument": boolean,
"stepTimeoutInMinutes": long,
"clientToken": "string"
}
```

`status`

Der neue Status für die Auftragsausführung (`IN_PROGRESS`, `FAILED`, `SUCCEEDED` oder `REJECTED`). Dieser muss bei jeder Aktualisierung angegeben werden.

`statusDetails`

Eine Sammlung von Name/Wert-Paaren, die den Status der Auftragsausführung beschreiben. Wenn nicht angegeben, sind die `statusDetails` nicht geändert.

`expectedVersion`

Die erwartete aktuelle Version der Auftragsausführung. Bei jeder Aktualisierung der Auftragsausführung wird die Version erhöht. Wenn die im Jobs-Service gespeicherte Version der AWS IoT Auftragsausführung nicht übereinstimmt, wird die Aktualisierung mit einem `VersionMismatch` Fehler abgelehnt. Eine ErrorResponse, die den aktuellen Status der Auftragsausführung enthält, wird ebenfalls zurückgegeben. (Dadurch ist es nicht erforderlich, eine separate `DescribeJobExecution`-Anforderung durchzuführen, um die Daten zum Status der Auftragsausführung abzurufen.)

`executionNumber`

(Optional) Eine Nummer, die eine Auftragsausführung auf einem Gerät identifiziert. Wenn nicht angegeben, wird die letzte Auftragsausführung verwendet.

`includeJobExecutionState`

(Optional) Wenn enthalten und auf `true` gesetzt, enthält die Antwort das Feld `JobExecutionState`. Der Standardwert ist `false`.

`includeJobDocument`

(Optional) Wenn enthalten und auf `true` gesetzt, enthält die Antwort das `JobDocument`. Der Standardwert ist `false`.

`stepTimeoutInMinutes`

Gibt die Dauer an, die dieses Gerät für den Abschluss der Ausführung dieses Auftrags hat. Wenn der Status der Auftragsausführung nicht in einen Terminal-Zustand gesetzt wird, bevor dieser Timer abläuft oder bevor der Timer zurückgesetzt wird, wird der Status der Auftragsausführung auf `TIMED_OUT` gesetzt. Das Festlegen oder Zurücksetzen dieser Zeitüberschreitung hat keinen Einfluss auf die Zeitüberschreitung der Auftragsausführung, die möglicherweise beim Erstellen des Auftrags festgelegt wurde.

Der Message Broker veröffentlicht `$aws/things/`*`thingName`*`/jobs/`*`jobId`*`/update/accepted` und `$aws/things/`*`thingName`*`/jobs/`*`jobId`*`/update/rejected` auch ohne ein bestimmtes Abonnement. Damit Ihr Kunde die Nachrichten empfangen kann, muss er sie jedoch abhören. Weitere Informationen finden Sie in der Anmerkung zu Jobs API-Nachrichten.

Antwortnutzlast:

```
{
"executionState": JobExecutionState,
"jobDocument": "string",
"timestamp": timestamp,
"clientToken": "string"
}
```

`executionState`

Ein JobExecutionState-Objekt.

`jobDocument`

Ein -Auftragsdokument-Objekt.

> **Note**
>
> In MQTT-Antworten ist das `jobDocument` Feld ein JSON-Objekt. In HTTP-Antworten ist es eine Zeichenkettendarstellung des JSON-Objekts.

`timestamp`

Die Zeit in Sekunden seit der Epoche, in der die Nachricht gesendet wurde, vergangene Zeit.

`clientToken`

Ein Client-Token zur Korrelierung von Anforderungen und Antworten.

Wenn Sie das MQTT-Protokoll verwenden, können Sie auch die folgenden Updates durchführen:

JobExecutionsChanged

Wird gesendet, wenn eine Auftragsausführung der Liste ausstehender Auftragsausführungen für ein Objekt hinzugefügt oder daraus entfernt wird.

Verwenden Sie das -Thema:

`$aws/things/thingName/jobs/notify`

Nachrichtennutzlast:

```
{
"jobs" : {
    "JobExecutionState": [ JobExecutionSummary ... ]
         },
    "timestamp": timestamp
}
```

NextJobExecutionChanged

Wird gesendet, wenn sich ändert, welche Auftragsausführung die nächste auf der Liste der ausstehenden Auftragsausführungen für ein Objekt ist, wie für `DescribeJobExecution` mit `jobId` `$next` definiert. Diese Nachricht wird nicht gesendet, wenn sich die Details der nächsten Auftragsausführung ändern, sondern nur, wenn sich der nächste Auftrag geändert hat, der von `DescribeJobExecution` mit `jobId` `$next` ausgegeben würde. Nehmen wir als Beispiel die Auftragsausführungen J1 und J2 mit dem Status `QUEUED`. J1 ist die nächste ausstehende Auftragsausführung auf der Liste. Wenn sich der Status von J2 zu `IN_PROGRESS` ändert und der Status von J1 unverändert bleibt, wird diese Benachrichtigung gesendet und enthält Details von J2.

Verwenden Sie das -Thema:

`$aws/things/`*`thingName`*`/jobs/notify-next`

Nachrichtennutzlast:

```
{
"execution" : JobExecution,
"timestamp": timestamp,
}
```

## HTTP-API für Aufträge-Geräte

Geräte können mithilfe der HTTP-Signaturversion 4 an Port 443 mit AWS IoT Jobs kommunizieren. Dies ist die Methode, die von der AWS SDKs AND-CLI verwendet wird. Weitere Informationen zu diesen Tools finden Sie unter AWS CLI Befehlsreferenz: iot-jobs-data oder AWS SDKs und Tools.

Für Geräte, die die Aufträge ausführen, sind die folgenden Befehle verfügbar. Hinweise zur Verwendung von API-Operationen mit dem MQTT-Protokoll finden Sie unter Führt MQTT-API-Operationen auf dem Gerät aus.

GetPendingJobExecutions

Ruft die Liste aller Aufträge für ein bestimmtes Objekt ab, die sich nicht in einem Terminal-Zustand befinden.

HTTPS request

```
GET /things/thingName/jobs
```

Antwort:

```
{
"inProgressJobs" : [ JobExecutionSummary ... ],
"queuedJobs" : [ JobExecutionSummary ... ]
}
```

Weitere Informationen finden Sie unter GetPendingJobExecutions.

CLI syntax

```
aws iot-jobs-data get-pending-job-executions \
--thing-name <value>  \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

`cli-input-json` format:

```
{
"thingName": "string"
}
```

Weitere Informationen finden Sie unter get-pending-job-executions.

StartNextPendingJobExecution

Ruft die nächste anstehende Auftragsausführung für ein Objekt ab und startet sie (mit Status `IN_PROGRESS` oder `QUEUED`).

- Alle Auftragsausführungen mit dem Status `IN_PROGRESS` werden zuerst zurückgegeben.
- Auftragsausführungen werden in der Reihenfolge zurückgegeben, in der sie erstellt wurden.

- Wenn die nächste ausstehende Auftragsausführung den Status `QUEUED` hat, wechselt ihr Status zu `IN_PROGRESS`, und die Statusdetails der Auftragsausführung werden wie angegeben eingerichtet.
- Wenn die nächste ausstehende Auftragsausführung bereits den Status `IN_PROGRESS` hat, ändern sich ihre Statusdetails nicht.
- Wenn keine Auftragsausführungen ausstehen, enthält die Antwort das Feld `execution` nicht.
- Optional können Sie einen Schritt-Timer erstellen, indem Sie einen Wert für die `stepTimeoutInMinutes`-Eigenschaft angeben. Falls Sie den Wert dieser Eigenschaft nicht aktualisieren, indem Sie `UpdateJobExecution` ausführen, läuft die Auftragsausführung ab, wenn der Schritt-Timer abläuft.

HTTPS request

Im folgenden Beispiel wird die Anfragesyntax dargestellt:

```
PUT /things/thingName/jobs/$next
{
"statusDetails": {
    "string": "string"
    ...
},
"stepTimeoutInMinutes": long
}
```

Weitere Informationen finden Sie unter [StartNextPendingJobExecution].

CLI syntax

Syntax:

```
aws iot-jobs-data  start-next-pending-job-execution \
--thing-name <value> \
{--step-timeout-in-minutes <value>] \
[--status-details <value>]  \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

`cli-input-json` format:

```
{
```

```
"thingName": "string",
"statusDetails": {
"string": "string"
},
"stepTimeoutInMinutes": long
}
```

Weitere Informationen finden Sie unter start-next-pending-job-execution.

DescribeJobExecution

Ruft detaillierte Informationen zu einer Auftragsausführung ab.

Sie können die `jobId` auf `$next` setzen, um die nächste ausstehende Auftragsausführung für ein Objekt zurückzugeben. Der Ausführungsstatus des Auftrags muss `QUEUED` oder `IN_PROGRESS` sein.

HTTPS request

Anforderung:

```
GET /things/thingName/jobs/jobId?
executionNumber=executionNumber&includeJobDocument=includeJobDocument
```

Antwort:

```
{
"execution" : JobExecution,
}
```

Weitere Informationen finden Sie unter DescribeJobExecution.

CLI syntax

Syntax:

```
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
}
```

Weitere Informationen finden Sie unter `describe-job-execution`.

UpdateJobExecution

Aktualisiert den Status einer Auftragsausführung. Optional können Sie einen Schritt-Timer erstellen, indem Sie einen Wert für die `stepTimeoutInMinutes`-Eigenschaft angeben. Falls Sie den Wert dieser Eigenschaft nicht aktualisieren, indem Sie `UpdateJobExecution` erneut ausführen, läuft die Auftragsausführung ab, wenn der Schritt-Timer abläuft.

HTTPS request

Anforderung:

```
POST /things/thingName/jobs/jobId
{
"status": "job-execution-state",
"statusDetails": {
    "string": "string"
    ...
},
"expectedVersion": "number",
"includeJobExecutionState": boolean,
"includeJobDocument": boolean,
"stepTimeoutInMinutes": long,
"executionNumber": long
}
```

Weitere Informationen finden Sie unter `UpdateJobExecution`.

CLI syntax

Syntax:

```
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>] \
[--step-timeout-in-minutes <value>] \
[--generate-cli-skeleton]
```

`cli-input-json` format:

```
{
"jobId": "string",
"thingName": "string",
"status": "string",
"statusDetails": {
"string": "string"
},
"stepTimeoutInMinutes": number,
"expectedVersion": long,
"includeJobExecutionState": boolean,
"includeJobDocument": boolean,
"executionNumber": long
}
```

Weitere Informationen finden Sie unter update-job-execution.

# Benutzer und Geräte mit AWS IoT Jobs schützen

Um Benutzer zur Verwendung von AWS IoT Jobs mit ihren Geräten zu autorisieren, müssen Sie ihnen mithilfe von IAM Richtlinien Berechtigungen gewähren. Die Geräte müssen dann mithilfe von AWS IoT Core Richtlinien autorisiert werden, um eine sichere Verbindung herzustellen AWS IoT, Auftragsausführungen zu empfangen und den Ausführungsstatus zu aktualisieren.

# Erforderlicher Richtlinientyp für Jobs AWS IoT

Die folgende Tabelle zeigt die verschiedenen Richtlinientypen, die Sie für die Autorisierung verwenden müssen. Weitere Informationen über die erforderliche Richtlinie finden Sie unter Autorisierung.

Erforderlicher Richtlinientyp

| Anwendungsfall | Protokoll | Authentifizierung | Steuerebene/Datenebene | Identitätstyp | Erforderlicher Richtlinientyp |
|---|---|---|---|---|---|
| Autorisieren Sie einen Administrator, Operator oder Cloud-Service, um sicher mit Aufträgen zu arbeiten | HTTPS | AWS Authentifizierung mit Signaturversion 4 (Port 443) | Sowohl Steuerebene als auch Datenebene | Amazon Cognito Identity oder Verbundbenutzer IAM | IAMRichtlinie |
| Autorisieren Sie Ihr IoT-Gerät, um sicher mit Aufträgen zu arbeiten | MQTT/HTTPS | TCPoder TLS gegenseitige Authentifizierung (Port 8883 oder 443) | Datenebene | X.509-Zertifikate | AWS IoT Core Richtlinie |

Um AWS IoT Jobs-Operationen zu autorisieren, die sowohl auf der Steuerungsebene als auch auf der Datenebene ausgeführt werden können, müssen Sie IAM Richtlinien verwenden. Die Identitäten müssen für AWS IoT authentifiziert sein, um diese Operationen ausführen zu können. Dabei muss es sich um Amazon-Cognito-Identitäten oder IAM-Benutzer, -Gruppen und -Rollen handeln. Weitere Informationen über die Authentifizierung finden Sie unter Authentifizierung.

Die Geräte müssen jetzt auf der Datenebene mithilfe von AWS IoT Core Richtlinien autorisiert werden, um eine sichere Verbindung zum Geräte-Gateway herzustellen. Das Device Gateway ermöglicht es Geräten, sicher mit ihnen zu kommunizieren AWS IoT, Auftragsausführungen zu empfangen und den Status der Auftragsausführung zu aktualisieren. Die Gerätekommunikation

wird mithilfe von sicheren MQTT- oder HTTPS-Kommunikationsprotokollen gesichert. Diese Protokolle verwenden X.509-Clientzertifikate die, die von bereitgestellt werden, AWS IoT um die Geräteverbindungen zu authentifizieren.

Im Folgenden wird gezeigt, wie Sie Ihre Benutzer, Cloud-Dienste und Geräte zur Verwendung AWS IoT von Jobs autorisieren. Informationen zu den API Vorgängen auf der Steuerungsebene und der Datenebene finden Sie unterAWS IoT Jobs API-Operationen.

Themen

- Autorisieren von Benutzern und Cloud-Services zur Nutzung von AWS IoT -Aufträgen
- Autorisieren Sie Ihre Geräte für die sichere Verwendung von AWS IoT Jobs auf der Datenebene

## Autorisieren von Benutzern und Cloud-Services zur Nutzung von AWS IoT -Aufträgen

Um Ihre Benutzer und Cloud-Dienste zu autorisieren, müssen Sie IAM Richtlinien sowohl auf der Steuerungsebene als auch auf der Datenebene verwenden. Die Richtlinien müssen mit dem HTTPS Protokoll verwendet werden und müssen die AWS Signature Version 4-Authentifizierung (Port 443) verwenden, um Benutzer zu authentifizieren.

> **Note**
>
> AWS IoT Core Richtlinien dürfen nicht auf der Steuerungsebene verwendet werden. Für die Autorisierung von Benutzern oder Cloud-Diensten werden nur IAM Richtlinien verwendet. Weitere Informationen über die Verwendung der erforderlichen Richtlinie finden Sie unter Erforderlicher Richtlinientyp für Jobs AWS IoT.

IAMRichtlinien sind JSON Dokumente, die Richtlinienerklärungen enthalten. Richtlinienanweisungen verwenden die Elemente Effekt, Aktion und Ressource, um Ressourcen festzulegen, Aktionen zuzulassen oder abzulehnen und Bedingungen, bei denen Aktionen zugelassen oder abgelehnt werden. Weitere Informationen finden Sie unter IAMJSONPolicy Elements Reference im IAMBenutzerhandbuch.

> **Warning**
>
> Wir empfehlen, dass Sie keine Platzhalterberechtigungen verwenden, z. B. `"Action": ["iot:*"]` in Ihren IAM Richtlinien oder AWS IoT Core Richtlinien. Die Verwendung von Platzhalterberechtigungen ist keine empfohlene, bewährte Sicherheitsmethode. Weitere Informationen finden Sie unter Zu AWS IoT freizügige Richtlinie.

## IAMRichtlinien auf der Kontrollebene

Auf der Steuerungsebene verwenden IAM Richtlinien das `iot:` Präfix mit der Aktion, um den entsprechenden API Auftragsvorgang zu autorisieren. Die `iot:CreateJob` Richtlinienaktion gewährt dem Benutzer beispielsweise die Erlaubnis, den `CreateJob`APIzu verwenden.

Richtlinienaktionen

Die folgende Tabelle enthält eine Liste der IAM Richtlinienaktionen und der Berechtigungen zur Verwendung der API Aktionen. Informationen zu Ressourcentypen finden Sie unter Ressourcentypen, definiert von AWS IoT. Weitere Informationen zu AWS IoT Aktionen finden Sie unter Aktionen definiert von AWS IoT.

IAMpolitische Aktionen auf der Kontrollebene

| Richtlinienaktionen | APIBetrieb | Ressourcentypen | Beschreibung |
|---|---|---|---|
| `iot:AssociateTargetsWithJob` | `AssociateTargetsWithJob` | • Auftrag<br>• Objekt<br>• thinggroup | Steht für die Erlaubnis zum Verknüpfen einer Gruppe mit einem kontinuierlichen Auftrag. Die Berechtigung `iot:AssociateTargetsWithJob` wird jedes Mal überprüft, wenn eine Anforderung zur Verknüpfung eines Auftrags gestellt wird. |
| `iot:CancelJob` | `CancelJob` | Auftrag | Stellt die Berechtigung zum Abbrechen eines Auftrags dar. Die Berechtigung `iot:CancelJob` wird jedes Mal überprüft, wenn eine Anforderung zum Abbrechen eines Auftrags gestellt wird. |

| Richtlinienaktionen | APIBetrieb | Ressourcentypen | Beschreibung |
| --- | --- | --- | --- |
| `iot:CancelJobExecution` | `CancelJobExecution` | • Auftrag<br>• Objekt | Stellt die Berechtigung zum Abbruch einer Auftragsausführung dar. Die Berechtigung `iot: CancelJobExecution` wird jedes Mal überprüft, wenn eine Anforderung zum Abbrechen einer Auftragsausführung gestellt wird. |
| `iot:CreateJob` | `CreateJob` | • Auftrag<br>• Objekt<br>• thinggroup<br>• jobtemplate<br>• package | Stellt die Berechtigung zum Erstellen eines Auftrags dar. Die Berechtigung `iot: CreateJob` wird jedes Mal überprüft, wenn eine Anforderung zum Erstellen eines Auftrags gestellt wird. |
| `iot:CreateJobTemplate` | `CreateJobTemplate` | • Auftrag<br>• jobtemplate<br>• package | Stellt die Berechtigung zum Erstellen einer Auftragsvorlage dar. Die Berechtigung `iot: CreateJobTemplate` wird jedes Mal überprüft, wenn eine Anforderung zum Erstellen einer Auftragsvorlage gestellt wird. |
| `iot:DeleteJob` | `DeleteJob` | Auftrag | Stellt die Berechtigung zum Löschen eines Auftrags dar. Die Berechtigung `iot: DeleteJob` wird jedes Mal überprüft, wenn eine Anforderung zum Löschen eines Auftrags gestellt wird. |

| Richtlinienaktionen | APIBetrieb | Ressourcentypen | Beschreibung |
| --- | --- | --- | --- |
| `iot:DeleteJobTemplate` | DeleteJobTemplate | jobtemplate | Stellt die Berechtigung zum Löschen einer Auftragsvorlage dar. Die Berechtigung `iot: CreateJobTemplate` wird jedes Mal überprüft, wenn eine Anforderung zum Löschen einer Auftragsvorlage gestellt wird. |
| `iot:DeleteJobExecution` | DeleteJobTemplate | • Auftrag<br>• Objekt | Stellt die Berechtigung zum Löschen einer Auftragsausführung dar. Die Berechtigung `iot: DeleteJobExecution` wird jedes Mal überprüft, wenn eine Anforderung zum Löschen eines Auftragsausführung gestellt wird. |
| `iot:DescribeJob` | DescribeJob | Auftrag | Stellt die Berechtigung zum Beschreiben eines Auftrags dar. Die Berechtigung `iot: DescribeJob` wird jedes Mal überprüft, wenn eine Anforderung zum Beschreiben eines Auftrags gestellt wird. |
| `iot:DescribeJobExecution` | DescribeJobExecution | • Auftrag<br>• Objekt | Stellt die Berechtigung zum Beschreiben einer Auftragsausführung dar. Die Berechtigung `iot: DescribeJobExecution` wird jedes Mal überprüft, wenn eine Anforderung zum Beschreiben einer Auftragsausführung gestellt wird. |
| `iot:DescribeJobTemplate` | DescribeJobTemplate | jobtemplate | Stellt die Berechtigung zum Beschreiben einer Auftragsvorlage dar. Die Berechtigung `iot: DescribeJobTemplate` wird jedes Mal überprüft, wenn eine Anforderung zum Beschreiben einer Auftragsvorlage gestellt wird. |

| Richtlinienaktionen | APIBetrieb | Ressourcentypen | Beschreibung |
| --- | --- | --- | --- |
| `iot:DescribeManagedJobTemplate` | DescribeManagedJobTemplate | jobtemplate | Stellt die Berechtigung zum Beschreiben einer verwalteten Auftragsvorlage dar. Die Berechtigung `iot: DescribeManagedJobTemplate` wird jedes Mal überprüft, wenn eine Anfrage zur Beschreibung einer verwalteten Auftragsvorlage gestellt wird. |
| `iot:GetJobDocument` | GetJobDocument | Auftrag | Stellt die Berechtigung zum Abrufen eines Auftragsdokuments für einen Auftrag dar. Die Berechtigung `iot:GetJobDocument` wird jedes Mal überprüft, wenn eine Anforderung zum Abrufen eines Auftragsdokuments gestellt wird. |
| `iot:ListJobExecutionsForJob` | ListJobExecutionsForJob | Auftrag | Stellt die Berechtigung zum Auflisten von Auftragsausführungen für einen Auftrag dar. Die Berechtigung `iot:ListJobExecutionsForJob` wird jedes Mal überprüft, wenn eine Anforderung zum Auflisten der Auftragsausführungen für einen Auftrag gestellt wird. |
| `iot:ListJobExecutionsForThing` | ListJobExecutionsForThing | Objekt | Stellt die Berechtigung zum Auflisten von Auftragsausführungen für einen Auftrag dar. Die Berechtigung `iot:ListJobExecutionsForThing` wird jedes Mal überprüft, wenn eine Anforderung zum Auflisten der Auftragsausführungen für ein Objekt gestellt wird. |

| Richtlinienaktionen | APIBetrieb | Ressourcentypen | Beschreibung |
| --- | --- | --- | --- |
| `iot:ListJobs` | ListJobs | Keine | Stellt die Berechtigung zum Auflisten der Aufträge dar. Die Berechtigung `iot:ListJobs` wird jedes Mal überprüft, wenn eine Anforderung zum Auflisten der Aufträge gestellt wird. |
| `iot:ListJobTemplates` | ListJobTemplates | Keine | Stellt die Berechtigung zum Auflisten der Auftragsvorlagen dar. Die Berechtigung `iot:ListJobTemplates` wird jedes Mal überprüft, wenn eine Anforderung zum Auflisten der Auftragsvorlagen gestellt wird. |
| `iot:ListManagedJobTemplates` | ListManagedJobTemplates | Keine | Stellt die Berechtigung zum Auflisten der verwalteten Jobvorlagen dar. Die Berechtigung `iot:ListManagedJobTemplates` wird jedes Mal überprüft, wenn eine Anforderung zum Auflisten der verwalteten Auftragsvorlagen gestellt wird. |
| `iot:UpdateJob` | UpdateJob | Auftrag | Stellt die Berechtigung zum Aktualisieren eines Auftrags dar. Die Berechtigung `iot:UpdateJob` wird jedes Mal überprüft, wenn eine Anforderung zum Aktualisieren des Auftrags gestellt wird. |
| `iot:TagResource` | TagResource | • Auftrag<br>• jobtemplate<br>• Objekt | Gewährt die Berechtigung zum Markieren einer bestimmten Ressource. |
| `iot:UntagResource` | UntagResource | • Auftrag<br>• jobtemplate<br>• Objekt | Gewährt die Berechtigung zum Aufheben der Markierung einer bestimmten Ressource. |

### Grundlegendes Beispiel IAM für eine Richtlinie

Das folgende Beispiel zeigt eine IAM Richtlinie, die dem Benutzer die Erlaubnis gibt, die folgenden Aktionen für Ihr IoT-Ding und Ihre IoT-Dinggruppe auszuführen.

Ersetzen Sie im Beispiel:

- *region* mit Ihrem AWS-Region, wie`us-east-1`.
- *account-id* mit deiner AWS-Konto Nummer, wie`57EXAMPLE833`.
- *thing-group-name* mit dem Namen Ihrer IoT-Dinggruppe, für die Sie Jobs anstreben, wie `FirmwareUpdateGroup` z.
- *thing-name* mit dem Namen Ihres IoT-Dings, für das Sie Jobs anstreben, wie `MyIoTThing` z.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iot:CreateJobTemplate",
                "iot:CreateJob",
                ],
            "Effect": "Allow",
            "Resource": "arn:aws:iot:region:account-id:thinggroup/thing-group-name"
        },
        {
            "Action": [
                "iot:DescribeJob",
                "iot:CancelJob",
                "iot:DeleteJob",
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iot:region:account-id:job/*"
        },
        {
            "Action": [
                "iot:DescribeJobExecution",
                "iot:CancelJobExecution",
                "iot:DeleteJobExecution",
            ],
            "Effect": "Allow",
            "Resource": [
```

```
                "arn:aws:iot:region:account-id:thing/thing-name"
                "arn:aws:iot:region:account-id:job/*"
            ]
        }
    ]
}
```

IAMRichtlinienbeispiel für IP-basierte Autorisierung

Sie können verhindern, dass Principals von bestimmten IP-Adressen aus API Anrufe an Ihren Kontrollebenen-Endpunkt tätigen. Um die IP-Adressen anzugeben, die zugelassen werden können, verwenden Sie im Element Bedingung Ihrer IAM Richtlinie den `aws:SourceIp`globalen Bedingungsschlüssel.

Die Verwendung dieses Bedingungsschlüssels kann auch dazu führen, dass andere AWS-Service Benutzer diese API Anrufe nicht in Ihrem Namen tätigen können, z. AWS CloudFormation B. Um den Zugriff auf diese Dienste zu ermöglichen, verwenden Sie den `aws:ViaAWSService`globalen Bedingungsschlüssel mit dem SourceIp Schlüssel aws:. Dadurch wird sichergestellt, dass die Zugriffsbeschränkung für die Quell-IP-Adresse nur für Anforderungen gilt, die direkt von einem Prinzipal stammen. Weitere Informationen finden Sie unter AWS: Verweigert den Zugriff auf AWS basierend auf der Quell-IP.

Das folgende Beispiel zeigt, wie nur eine bestimmte IP-Adresse zugelassen wird, die API Anrufe an den Endpunkt der Steuerungsebene tätigen kann. Der `aws:ViaAWSService` Schlüssel ist auf eingestellt`true`, sodass andere Dienste in Ihrem Namen API Anrufe tätigen können.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
            "Effect": "Allow",
            "Action": [
                "iot:CreateJobTemplate",
                "iot:CreateJob"
             ],
            "Resource": ["*"],
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "123.45.167.89"
                }
            },
```

```
            "Bool": {"aws:ViaAWSService": "true"}
        }
    ],
}
```

## IAMRichtlinien auf der Datenebene

IAMRichtlinien auf der Datenebene verwenden das `iotjobsdata:` Präfix, um API Jobvorgänge zu autorisieren, die Benutzer ausführen können. Auf der Datenebene können Sie einem Benutzer mithilfe der `iotjobsdata:DescribeJobExecution` Richtlinienaktion die Berechtigung zur Verwendung `DescribeJobExecution`APIvon erteilen.

> **Warning**
>
> Die Verwendung von IAM Richtlinien auf der Datenebene wird nicht empfohlen, wenn Sie AWS IoT Jobs auf Ihre Geräte ausrichten möchten. Wir empfehlen, dass Sie IAM Richtlinien auf der Steuerungsebene verwenden, damit Benutzer Jobs erstellen und verwalten können. Verwenden Sie auf der Datenebene AWS IoT Core Richtlinien für HTTPS das Protokoll, um Geräte zum Abrufen von Auftragsausführungen und zum Aktualisieren des Ausführungsstatus zu autorisieren.

### Beispiel IAM für eine grundlegende Richtlinie

Die API Operationen, die autorisiert werden müssen, werden normalerweise ausgeführt, indem Sie CLI Befehle eingeben. Nachfolgend wird ein Beispiel für einen Benutzer gezeigt, der eine Operation `DescribeJobExecution` ausführt.

Ersetzen Sie im Beispiel:

- *`region`* mit deinem AWS-Region, wie`us-east-1`.
- *`account-id`* mit deiner AWS-Konto Nummer, wie`57EXAMPLE833`.
- *`thing-name`* mit dem Namen Ihres IoT-Dings, für das Sie Jobs anstreben, wie `myRegisteredThing` z.
- *`job-id`*ist die eindeutige Kennung für den Job, auf den Sie mithilfe von abzielenAPI.

```
aws iot-jobs-data describe-job-execution \
    --endpoint-url "https://account-id.jobs.iot.region.amazonaws.com" \
```

```
    --job-id jobID --thing-name thing-name
```

Im Folgenden wird ein Beispiel IAM für eine Richtlinie gezeigt, die diese Aktion autorisiert:

```
{
    "Version": "2012-10-17",
    "Statement":
    {
        "Action": ["iotjobsdata:DescribeJobExecution"],
        "Effect": "Allow",
        "Resource": "arn:aws:iot:region:account-id:thing/thing-name",
    }
   }
```

IAMRichtlinienbeispiele für IP-basierte Autorisierung

Sie können verhindern, dass Prinzipale von bestimmten IP-Adressen aus API Anrufe an Ihren Datenebenen-Endpunkt tätigen. Um die IP-Adressen anzugeben, die zugelassen werden können, verwenden Sie im Element Condition Ihrer IAM Richtlinie den `aws:SourceIp`globalen Bedingungsschlüssel.

Die Verwendung dieses Bedingungsschlüssels kann auch dazu führen, dass andere AWS-Service Benutzer diese API Anrufe nicht in Ihrem Namen tätigen können, z. AWS CloudFormation B. Um den Zugriff auf diese Services zu ermöglichen, verwenden Sie den globalen Bedingungsschlüssel `aws:ViaAWSService` zusammen mit dem Bedingungsschlüssel `aws:SourceIp`. Dadurch wird sichergestellt, dass die Zugriffsbeschränkung für IP-Adressen nur für Anfragen gilt, die direkt vom Prinzipal gestellt werden. Weitere Informationen finden Sie unter AWS: Verweigert den Zugriff auf AWS basierend auf der Quell-IP.

Das folgende Beispiel zeigt, wie nur eine bestimmte IP-Adresse zugelassen wird, die API Anrufe an den Endpunkt der Datenebene tätigen kann.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
            "Effect": "Allow",
            "Action": ["iotjobsdata:*"],
            "Resource": ["*"],
            "Condition": {
```

```
                "IpAddress": {
                    "aws:SourceIp": "123.45.167.89"
                }
            },
            "Bool": {"aws:ViaAWSService": "false"}
        }
    ],
}
```

Das folgende Beispiel zeigt, wie Sie verhindern können, dass bestimmte IP-Adressen oder Adressbereiche API Anrufe an den Endpunkt der Datenebene tätigen.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
            "Effect": "Deny",
            "Action": ["iotjobsdata:*"],
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
                        "123.45.167.89",
                        "192.0.2.0/24",
                        "203.0.113.0/24"
                    ]
                }
            },
            "Resource": ["*"],
        }
    ],
}
```

IAMBeispiel für eine Richtlinie sowohl für die Steuerungsebene als auch für die Datenebene

Wenn Sie einen API Vorgang sowohl auf der Steuerungsebene als auch auf der Datenebene ausführen, muss Ihre Richtlinienaktion auf der Kontrollebene das `iot:` Präfix verwenden, und Ihre Richtlinienaktion auf der Datenebene muss das `iotjobsdata:` Präfix verwenden.

Beispielsweise `DescribeJobExecution` API kann das sowohl auf der Steuerungsebene als auch auf der Datenebene verwendet werden. Auf der Steuerungsebene DescribeJobExecutionAPIwird der verwendet, um die Ausführung eines Jobs zu beschreiben. Auf der Datenebene DescribeJobExecutionAPIwird der verwendet, um Details einer Auftragsausführung abzurufen.

Mit der folgenden IAM Richtlinie wird einem Benutzer die Erlaubnis erteilt, den sowohl `DescribeJobExecution` API auf der Steuerungsebene als auch auf der Datenebene zu verwenden.

Ersetzen Sie im Beispiel:

- *`region`* mit deinem AWS-Region, wie`us-east-1`.
- *`account-id`* mit deiner AWS-Konto Nummer, wie`57EXAMPLE833`.
- *`thing-name`* mit dem Namen Ihres IoT-Dings, für das Sie Jobs anstreben, wie `MyIoTThing` z.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": ["iotjobsdata:DescribeJobExecution"],
            "Effect": "Allow",
            "Resource": "arn:aws:iot:region:account-id:thing/thing-name"
        },
        {
            "Action": [
                "iot:DescribeJobExecution",
                "iot:CancelJobExecution",
                "iot:DeleteJobExecution",
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:iot:region:account-id:thing/thing-name"
                "arn:aws:iot:region:account-id:job/*"
            ]
        }
    ]
}
```

## Das Markieren von IoT-Ressourcen autorisieren

Um eine bessere Kontrolle über Aufträge und Auftragsvorlagen zu erhalten, die Sie erstellen, ändern oder verwenden können, haben Sie die Möglichkeit, Markierungen an die Aufträge oder Auftragsvorlagen anzuhängen. Markierungen helfen Ihnen außerdem bei der Unterscheidung von Eigentumsrechten, der Zuweisung und Zuordnung von Kosten, indem Sie diese Abrechnungsgruppen zuordnen und mit Markierungen versehen.

Wenn ein Benutzer seine Jobs oder Jobvorlagen, die er mithilfe von oder dem erstellt hat, taggen AWS Management Console möchte AWS CLI, muss Ihre IAM Richtlinie dem Benutzer die Erlaubnis gewähren, sie zu taggen. Um Berechtigungen zu gewähren, muss Ihre IAM Richtlinie die `iot:TagResource` Aktion verwenden.

> **Note**
>
> Wenn Ihre IAM Richtlinie die `iot:TagResource` Aktion nicht beinhaltet, wird bei jeder Aktion `CreateJob`oder `CreateJobTemplate`mit einem Tag ein `AccessDeniedException` Fehler zurückgegeben.

Wenn Sie Ihre Jobs oder Jobvorlagen, die Sie mithilfe von oder dem erstellt haben, taggen AWS Management Console möchten AWS CLI, muss Ihre IAM Richtlinie die Erlaubnis gewähren, sie zu taggen. Um Berechtigungen zu gewähren, muss Ihre IAM Richtlinie die `iot:TagResource` Aktion verwenden.

Allgemeine Informationen zum Tagging von Ressourcen finden Sie unter Verschlagworten Sie Ihre Ressourcen AWS IoT.

IAMBeispiel für eine Richtlinie

Sehen Sie sich die folgenden IAM Richtlinienbeispiele zur Gewährung von Tagging-Berechtigungen an:

Beispiel 1

Ein Benutzer, der den folgenden Befehl ausführt, um einen Auftrag zu erstellen und ihn einer bestimmten Umgebung zuzuordnen.

Ersetzen Sie in diesem Beispiel:

- *`region`* mit Ihrem AWS-Region, wie`us-east-1`.
- *`account-id`* mit deiner AWS-Konto Nummer, wie`57EXAMPLE833`.
- *`thing-name`* mit dem Namen Ihres IoT-Dings, für das Sie Jobs anstreben, wie `MyIoTThing` z.

```
aws iot create-job
    --job-id test_job
    --targets "arn:aws:iot:region:account-id:thing/thingOne"
    --document-source "https://s3.amazonaws.com/amzn-s3-demo-bucket/job-document.json"
```

```
    --description "test job description"
    --tags Key=environment,Value=beta
```

Für dieses Beispiel müssen Sie die folgende IAM Richtlinie verwenden:

```
{
    "Version": "2012-10-17",
    "Statement":
    {
        "Action": [ "iot:CreateJob", "iot:CreateJobTemplate", "iot:TagResource" ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:iot:aws-region:account-id:job/*",
            "arn:aws:iot:aws-region:account-id:jobtemplate/*"
        ]
    }
}
```

## Autorisieren Sie Ihre Geräte für die sichere Verwendung von AWS IoT Jobs auf der Datenebene

Um Ihre Geräte für die sichere Interaktion mit AWS IoT Jobs auf der Datenebene zu autorisieren, müssen Sie Richtlinien verwenden AWS IoT Core . AWS IoT Core Richtlinien für Jobs sind JSON Dokumente, die Grundsatzerklärungen enthalten. Diese Richtlinien verwenden auch die Elemente Wirkung, Aktion und Ressource und folgen einer ähnlichen Konvention wie IAM Richtlinien. Weitere Informationen zu diesen Elementen finden Sie unter IAMJSONPolicy Elements Reference im IAMBenutzerhandbuch.

Die Richtlinien können mit beiden MQTT HTTPS Protokollen verwendet werden und müssen für die Authentifizierung der Geräte eine TLS gegenseitige Authentifizierung verwendenTCP. Im Folgenden wird gezeigt, wie diese Richtlinien in den verschiedenen Kommunikationsprotokollen verwendet werden.

> **Warning**
>
> Wir empfehlen, dass Sie keine Platzhalterberechtigungen verwenden, z. B. `"Action": ["iot:*"]` in Ihren IAM Richtlinien oder AWS IoT Core Richtlinien. Die Verwendung von Platzhalterberechtigungen ist keine empfohlene, bewährte Sicherheitsmethode. Weitere Informationen finden Sie unter Zu AWS IoT freizügige Richtlinie.

## AWS IoT Core Richtlinien für das Protokoll MQTT

AWS IoT Core Richtlinien für MQTT das Protokoll gewähren Ihnen Berechtigungen zur Verwendung der MQTT API Geräteaktionen für Jobs. Die MQTT API Operationen werden verwendet, um mit MQTT Themen zu arbeiten, die Jobs-Befehlen vorbehalten sind. Weitere Informationen zu diesen API Vorgängen finden Sie unterFührt MQTT-API-Operationen auf dem Gerät aus.

MQTTIn Richtlinien werden politische Aktionen wie`iot:Connect`,`iot:Publish`, und verwendet`iot:Subscribe`, `iot:Receieve` um mit den Berufsthemen zu arbeiten. Diese Richtlinien ermöglichen es Ihnen, eine Verbindung zum Message Broker herzustellen, die MQTT Jobthemen zu abonnieren und MQTT Nachrichten zwischen Ihren Geräten und der Cloud zu senden und zu empfangen. Weitere Informationen zu diesen Aktionen finden Sie unter AWS IoT Core politische Maßnahmen.

Informationen zu Themen für AWS IoT Jobs finden Sie unterAuftragsthemen.

Grundlegendes Beispiel MQTT für eine Richtlinie

Das folgende Beispiel zeigt, wie Sie `iot:Publish` und `iot:Subscribe` zum Veröffentlichen und Abonnieren von Aufträgen und Auftragsausführungen verwenden können.

Ersetzen Sie im Beispiel:

- *`region`* mit deinem AWS-Region, wie`us-east-1`.
- *`account-id`* mit deiner AWS-Konto Nummer, wie`57EXAMPLE833`.
- *`thing-name`* mit dem Namen Ihres IoT-Dings, für das Sie Jobs anstreben, wie `MyIoTThing` z.

```
{
    "Statement": [
        {
           "Effect": "Allow",
           "Action": [
                "iot:Publish",
                "iot:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:region:account-id:topic/$aws/events/job/*",
                "arn:aws:iot:region:account-id:topic/$aws/events/jobExecution/*",
                "arn:aws:iot:region:account-id:topic/$aws/things/thing-name/jobs/*"
```

```
            ]
        }
    ],
    "Version": "2012-10-17"
}
```

## AWS IoT Core Richtlinien für HTTPS das Protokoll

AWS IoT Core Richtlinien auf der Datenebene können auch HTTPS das Protokoll mit dem TLS Authentifizierungsmechanismus verwenden, um Ihre Geräte zu autorisieren. Auf der Datenebene verwenden Richtlinien das `iotjobsdata:` Präfix, um Jobs und API Operationen zu autorisieren, die Ihre Geräte ausführen können. Beispielsweise gewährt die `iotjobsdata:DescribeJobExecution` Richtlinienaktion dem Benutzer die Erlaubnis, den `DescribeJobExecution`APIzu verwenden.

> **Note**
>
> Die Richtlinienaktionen auf der Datenebene müssen das Präfix `iotjobsdata:` verwenden. Auf der Steuerebene müssen die Aktionen das Präfix `iot:` verwenden. Ein Beispiel für eine IAM Richtlinie, bei der sowohl Richtlinienaktionen auf der Steuerungsebene als auch auf der Datenebene verwendet werden, finden Sie unterIAMBeispiel für eine Richtlinie sowohl für die Steuerungsebene als auch für die Datenebene.

### Richtlinienaktionen

Die folgende Tabelle enthält eine Liste der AWS IoT Core Richtlinienaktionen und der Berechtigungen für die Autorisierung von Geräten zur Verwendung der API Aktionen. Eine Liste der API Operationen, die Sie auf der Datenebene ausführen können, finden Sie unterHTTP-API für Aufträge-Geräte.

> **Note**
>
> Diese Richtlinienaktionen zur Auftragsausführung gelten nur für den HTTP TLS Endpunkt. Wenn Sie den MQTT Endpunkt verwenden, müssen Sie die zuvor definierten MQTT Richtlinienaktionen verwenden.

AWS IoT Core Richtlinienaktionen auf Datenebene

| Richtlinienaktionen | APIBetrieb | Ressou ntypen | Beschreibung |
|---|---|---|---|
| `iotjobsdata:DescribeJobExecution` | `DescribeJobExecution` | • Auftra<br>• Objek | Stellt die Berechtigung für den Abruf einer Auftragsausführung dar. Die Berechtigung `iotjobsdata:DescribeJobExecution` wird jedes Mal überprüft, wenn eine Anforderung zum Abruf einer Auftragsausführung gestellt wird. |
| `iotjobsdata:GetPendingJobExecutions` | `GetPendingJobExecutions` | Objekt | Stellt die Berechtigung zum Abrufen der Liste der Aufträge dar, die sich nicht in einem Endstatus für ein Objekt befinden. Die Berechtigung `iotjobsdata:GetPendingJobExecutions` wird jedes Mal überprüft, wenn eine Anforderung zum Abrufen der Liste gestellt wird. |
| `iotjobsdata:StartNextPendingJobExecution` | `StartNextPendingJobExecution` | Objekt | Stellt die Berechtigung zum Abrufen und Starten der nächsten ausstehen den Auftragsausführung für ein Objekt dar. Das heißt, um eine Auftragsausführung mit dem Status `QUEUED` auf `IN_PROGRESS` zu aktualisieren. Die Berechtigung `iotjobsdata:StartNextPendingJobExecution` wird jedes Mal überprüft, wenn eine Anforderung zum Starten der nächsten ausstehenden Auftragsausführung gestellt wird. |

| Richtlinienaktionen | APIBetrieb | Ressourcentypen | Beschreibung |
| --- | --- | --- | --- |
| `iotjobsdata:UpdateJobExecution` | UpdateJobExecution | Objekt | Stellt die Berechtigung zum Aktualisieren einer Auftragsausführung dar. Die Berechtigung `iotjobsdata:UpdateJobExecution` wird jedes Mal überprüft, wenn eine Anforderung zum Aktualisieren des Status einer Auftragsausführung gestellt wird. |

Grundlegende Beispiele für Richtlinien

Im Folgenden wird ein Beispiel AWS IoT Core für eine Richtlinie gezeigt, die die Erlaubnis erteilt, die Aktionen auf der Datenebene API für jede Ressource auszuführen. Sie können Ihre Richtlinie auf eine bestimmte Ressource beschränken, wie z. B. auf ein IoT-Objekt. Ersetzen Sie in Ihrem Beispiel:

- *region* mit Ihrem AWS-Region wie`us-east-1`.
- *account-id* mit deiner AWS-Konto Nummer, wie`57EXAMPLE833`.
- *thing-name* mit dem Namen der IoT-Sache, wie zum Beispiel`MyIoTthing`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "iotjobsdata:GetPendingJobExecutions",
                "iotjobsdata:StartNextPendingJobExecution",
                "iotjobsdata:DescribeJobExecution",
                "iotjobsdata:UpdateJobExecution"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iot:region:account-id:thing/thing-name"
        }
    ]
}
```

Ein Beispiel dafür, wann Sie diese Richtlinien verwenden müssen, kann sein, wenn Ihre IoT-Geräte eine AWS IoT Core Richtlinie für den Zugriff auf einen dieser API Vorgänge verwenden, z. B. das folgende Beispiel für `DescribeJobExecution`API:

```
GET /things/thingName/jobs/jobId?
executionNumber=executionNumber&includeJobDocument=includeJobDocument&namespaceId=namespaceId
 HTTP/1.1
```

# AWS IoT Grenzwerte für Jobs

AWS IoT Jobs hat Dienstkontingente oder -limits, die der maximalen Anzahl von Serviceressourcen oder Vorgängen für Sie entsprechen AWS-Konto.

Themen

- Grenzwerte für die Ausführung von Job
- Limits für aktive und gleichzeitige Aufträge

## Grenzwerte für die Ausführung von Job

Dieser Abschnitt enthält Informationen zu den Grenzwerten für AWS IoT Device Management die Auftragsausführung.

> **Note**
>
> Diese Beschränkungen sind nicht Teil der Servicekontingente, die Sie in der Dokumentation zu den AWS IoT Device Management Service Quotas finden.

Um Informationen über die Anzahl der ausstehenden Jobausführungen zu erhalten, können Sie entweder die `GetPendingJobExecutions` API verwenden oder die reservierten MQTT-Themen für AWS IoT Jobs and Receive abonnieren. Auftrag-Benachrichtigungstypen

Die Anzahl der ausstehenden Jobausführungen in Ihrem Konto kann variieren, je nachdem, ob Sie die Planungskonfiguration aktiviert haben und ein wiederkehrendes Wartungsfenster verwenden.

Maximale Anzahl ausstehender Auftragsausführungen

| Name der API/Benachrichtigung | Beschreibung | Ohne Planungskonfiguration | Mit Planungskonfiguration |
|---|---|---|---|
| `ListNotification` | A `ListNotification` wird veröffentlicht, wenn eine alte Auftragsausführung in einen Terminalstatus übergeht oder wenn eine neue Auftragsausführung in die Warteschlange gestellt wird oder in einen Nicht-Terminal-Status wechselt. Es können bis zu 15 ausstehende Auftragsausführungen angezeigt werden, bei denen es sich entweder um oder handelt. `QUEUED` `IN_PROGRESS` | 10 | 15 (Bis zu 5 Auftragsausführungen werden nur im Fenster „`ListNotification` Während einer Wartung“ angezeigt). |
| `GetPendingJobExecutions` | Wenn Sie die `GetPendingJobExecutions` API aufrufen, gibt sie eine Liste der Jobausführungen zurück, die noch nicht gestartet wurden und nach dem API-Aufruf gestartet werden können. Die API kann bis zu 10 ausstehende Auftragsausführungen zurückgeben.<br>• Von den 10 ausstehenden Auftragsausführungen werden `IN_PROGRESS` die Ausführungen, die bereits ausgeführt wurden, aus dem Ergebnis herausgefiltert.<br>• Von den 10 ausstehenden Jobausführungen werden ihre Jobs, sofern sie sich im `SCHEDULED` Status befinden, aus dem Ergebnis gefiltert. | 10 | 15 |

# Limits für aktive und gleichzeitige Aufträge

In diesem Abschnitt erfahren Sie mehr über aktive und gleichzeitige Aufträge und die für sie geltenden Beschränkungen.

Aktive Aufträge und Limit für aktive Aufträge

Wenn Sie einen Job mithilfe der AWS IoT Konsole oder der `CreateJob` API erstellen, ändert sich der Jobstatus auf`IN_PROGRESS`. Alle laufenden Aufträge sind aktive Aufträge und werden auf das Limit für aktive Aufträge angerechnet. Dazu gehören Aufträge, bei denen entweder neue Auftragsausführungen eingeführt werden, oder Aufträge, die darauf warten, dass Geräte ihre Auftragsausführungen abschließen. Dieses Limit gilt sowohl für kontinuierliche als auch für Snapshot-Aufträge.

Gleichzeitige Aufträge und Limit für die gleichzeitige Ausführung von Aufträgen

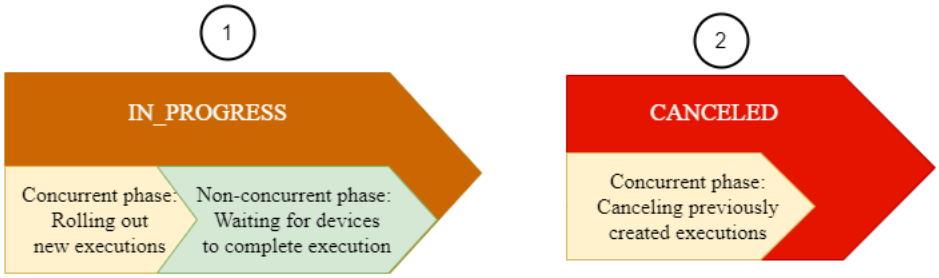
In Bearbeitung befindliche Jobs, bei denen entweder neue Jobausführungen eingeführt werden, oder Jobs, bei denen zuvor erstellte Jobausführungen abgebrochen werden, sind gleichzeitige Jobs und werden auf das Limit für die gleichzeitige Ausführung von Jobs angerechnet. AWS IoT Jobs können schnell bereitgestellt und Auftragsausführungen mit einer Geschwindigkeit von 1000 Geräten pro Minute abgebrochen werden. Jeder Auftrag ist `concurrent` und wird nur für kurze Zeit auf das Limit für die gleichzeitige Ausführung von Aufträgen angerechnet. Nachdem die Auftragsausführungen eingeführt oder abgebrochen wurden, ist der Auftrag nicht mehr gleichzeitig und wird nicht auf das Limit für die gleichzeitige Ausführung von Aufträgen angerechnet. Sie können die Auftragsparallelität verwenden, um eine große Anzahl von Aufträgen zu erstellen und gleichzeitig darauf zu warten, dass die Geräte die Auftragsausführung abschließen.

> **Note**
>
> Wenn ein Auftrag mit der optionalen Planungskonfiguration und dem Rollout des Auftragsdokuments, der während eines Wartungsfensters stattfinden soll, den ausgewählten `startTime` erreicht und Sie Ihr maximales Limit für die gleichzeitige Ausführung von Aufträgen erreicht haben, wechselt dieser geplante Auftrag in den Statusstatus `CANCELED`.

Um festzustellen, ob ein Job gleichzeitig ausgeführt wird, können Sie die `IsConcurrent` Eigenschaft eines Jobs in der AWS IoT Konsole oder mithilfe der OR-API verwenden. `DescribeJob` `ListJob` Dieses Limit gilt sowohl für kontinuierliche als auch für Snapshot-Aufträge.

Unter Endpunkte und Kontingente für Geräteverwaltung AWS IoT finden Sie unter Endpunkte AWS-Konto und Kontingente für die AWS IoT Geräteverwaltung im. Allgemeine AWS-Referenz

Das folgende Diagramm zeigt, wie sich die gleichzeitige Ausführung von Aufträgen auf Aufträge bezieht, die gerade bearbeitet werden, und auf Aufträge, die gerade storniert werden.




> **Note**
>
> Neue Aufträge mit dem optionalen `SchedulingConfig` behalten ihren ursprünglichen Status bei `SCHEDULED` und werden bei Erreichen des ausgewählten `startTime` auf `IN_PROGRESS` aktualisiert. Sobald der neue Auftrag mit der Option `SchedulingConfig` den ausgewählten `startTime` erreicht und auf `IN_PROGRESS` aktualisiert wird, wird er auf das Limit für aktive Aufträge und das Limit für die gleichzeitige Ausführung von Aufträgen angerechnet. Aufträge mit einem Status von `SCHEDULED` werden auf das Limit für aktive Aufträge angerechnet, nicht aber auf das Limit für die gleichzeitige Ausführung von Aufträgen.

Die folgende Tabelle zeigt die Grenzwerte, die für aktive und gleichzeitige Aufträge gelten, sowie die gleichzeitigen und nicht gleichzeitigen Phasen der Auftragsstatus.

Limits für aktive und gleichzeitige Aufträge

| Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können. | Phase | Limit für aktive Aufträge | Grenzwert für die Auftrags-Gleichzeitigkeit |
|---|---|---|---|
| `SCHEDULED` | Phase „Nicht gleichzeitig“: AWS IoT Jobs wartet auf den Zeitplan `startTime` des Auftrags, um mit der Auftragsausführung zu beginnen. Auf Ihren Geräten werden Benachrichtigungen zur Auftragsausführung gesendet. Aufträge in dieser Phase werden nur auf das Limit für aktive Aufträge angerechnet und die `IsConcurrent` -Eigenschaft ist auf „Falsch“ gesetzt. | Trifft zu | Trifft nicht zu |
| `IN_PROGRESS` | Gleichzeitige Phase: AWS IoT Jobs akzeptiert die Anfrage zur Erstellung des Jobs und beginnt mit der Bereitstellung von Benachrichtigungen zur Auftragsausführung auf Ihren Geräten. Aufträge in dieser Phase sind parallel, wie durch die `IsConcurrent` -Eigenschaft angegeben, die auf „true“ gesetzt ist, und werden sowohl auf die aktiven Aufträgen als auch auf die Grenzwerte für die gleichzeitige Ausführung von Aufträgen angerechnet. | Trifft zu | Trifft zu |

| Sobald Ihr Auftrag erstellt ist, wird das Auftrags-Dashboard geöffnet, wo Sie Ihre Aufträge anzeigen und verwalten können. | Phase | Limit für aktive Aufträge | Grenzwert für die Auftrags-Gleichzeitigkeit |
|---|---|---|---|
| | Nicht gleichzeitige Phase: AWS IoT Jobs wartet darauf, dass Geräte die Ergebnisse ihrer Jobausführungen melden. Aufträge in dieser Phase werden nur auf das Limit für aktive Aufträge angerechnet und die `IsConcurrent` -Eigenschaft ist auf „Falsch“ gesetzt. | Trifft zu | Trifft nicht zu |
| `Canceled` | Gleichzeitige Phase: AWS IoT Jobs akzeptiert die Anfrage zum Abbrechen des Jobs und beginnt mit dem Abbrechen von Jobausführungen, die zuvor für Ihre Geräte erstellt wurden. Jobs in dieser Phase sind gleichzeitig und die Eigenschaft `IsConcurrent` wird auf „true“ gesetzt. Sobald der Auftrag und die Auftragsausführungen abgebrochen wurden, ist der Auftrag nicht mehr gleichzeitig und wird nicht auf das Limit für die gleichzeitige Ausführung von Aufträgen angerechnet. | Trifft nicht zu | Trifft zu |

> **Note**
>
> Die maximale Dauer eines wiederkehrenden Wartungsfensters beträgt 23 Stunden und 50 Minuten.

# AWS IoT Device Management Befehle

> **Important**
>
> In dieser Dokumentation wird beschrieben, wie Sie die Befehlsfunktion in verwenden können AWS IoT Device Management. Informationen zur Verwendung dieser Funktion für finden Sie AWS IoT FleetWise unter Fernbefehle.
> Sie sind allein dafür verantwortlich, Befehle auf sichere und gesetzeskonforme Weise bereitzustellen. Weitere Informationen zu Ihren Pflichten finden Sie in den AWS Nutzungsbedingungen für AWS IoT Dienste.

Verwenden Sie AWS IoT Device Management Befehle, um eine Anweisung aus der Cloud an ein Gerät zu senden, mit dem eine Verbindung besteht AWS IoT. Befehle zielen jeweils auf ein Gerät ab und können für Anwendungen mit niedriger Latenz und hohem Durchsatz verwendet werden, z. B. zum Abrufen der geräteseitigen Protokolle oder zum Initiieren einer Änderung des Gerätestatus.

Der Befehl ist eine wiederverwendbare Ressource, die von verwaltet wird. AWS IoT Device Management Er enthält Konfigurationen, die angewendet werden, bevor sie auf dem Gerät veröffentlicht werden. Sie können eine Reihe von Befehlen für bestimmte Anwendungsfälle vordefinieren, z. B. das Einschalten einer Glühbirne oder das Entriegeln einer Fahrzeugtür.

Mithilfe der AWS IoT Befehlsfunktion können Sie:

- Erstellen Sie eine Befehlsressource und verwenden Sie deren Konfiguration erneut, um einen Befehl mehrmals an Ihr Zielgerät zu senden.
- Zielen Sie auf ein Gerät ab, das als AWS IoT Ding registriert wurde, oder auf einen MQTT-Client, in AWS IoT dem noch nicht registriert wurde.
- Führen Sie mehrere Befehle gleichzeitig auf dem Zielgerät aus, ohne das Gerät zu überlasten.
- Aktivieren Sie Benachrichtigungen für Befehlsereignisse und rufen Sie den Status des Geräts ab und verfolgen Sie ihn, während der Befehl bis zum Abschluss ausgeführt wird.

In den folgenden Themen erfahren Sie, wie Sie Befehle erstellen, sie an Ihr Gerät senden und den vom Gerät gemeldeten Status abrufen.

Themen

- Befehle, Konzepte und Status
- Arbeitsablauf für Befehle auf hoher Ebene
- Befehle erstellen und verwalten
- Befehlsausführungen starten und überwachen
- Eine Befehlsressource als veraltet kennzeichnen


# Befehle, Konzepte und Status

Verwenden Sie AWS IoT Befehle, um eine Anweisung aus der Cloud an ein Gerät zu senden, mit dem eine Verbindung besteht AWS IoT. So verwenden Sie die Befehlsfunktion:

1. Erstellen Sie zunächst eine Befehlsressource mit einer Payload, die die Konfigurationen enthält, die für die Ausführung des Befehls auf dem Gerät erforderlich sind.
2. Geben Sie das Zielgerät an, das die Payload empfängt und die angegebenen Aktionen ausführt.
3. Führen Sie den Befehl auf dem Zielgerät aus und rufen Sie die Statusinformationen vom Gerät ab. Informationen zur Behebung von Problemen finden Sie in den CloudWatch Protokollen.

Weitere Informationen zu diesem Workflow finden Sie unter Arbeitsablauf für Befehle auf hoher Ebene.

Themen


- Befehle und wichtige Konzepte
- Status des Befehls
- Status der Befehlsausführung


## Befehle und wichtige Konzepte

Im Folgenden werden einige wichtige Konzepte für die Verwendung der Befehlsfunktion beschrieben.

Befehle

> Befehle sind Anweisungen, die von der Cloud an Ihre IoT-Geräte gesendet werden. Diese Anweisungen (Befehls-Payload) werden als MQTT-Nachrichten an die Geräte gesendet. Nachdem die Geräte die Befehlsnutzdaten erhalten haben, können sie die Anweisungen

verarbeiten, um die entsprechende Aktion auszuführen. Beispiele für solche Aktionen sind das Ändern der Gerätekonfigurationseinstellungen, das Übertragen von Sensormesswerten oder das Hochladen von Protokollen. Die Geräte können dann den Befehl ausführen und das Ergebnis an die Cloud zurückgeben. Auf diese Weise können Sie angeschlossene Geräte aus der Ferne überwachen und steuern.

Namespace

Wenn Sie die Befehlsfunktion verwenden, können Sie den Namespace für den Befehl angeben. Wenn Sie einen Befehl in erstellen möchten AWS IoT Device Management, müssen Sie den `AWS-IoT` Standard-Namespace verwenden. Wenn Sie diesen Namespace verwenden, müssen Sie bei der Erstellung des Befehls eine Nutzlast angeben. Die Payload wird verwendet, wenn Sie den Befehl auf Ihrem Zielgerät ausführen. Wenn Sie stattdessen einen Befehl für erstellen möchten, müssen Sie AWS IoT FleetWise stattdessen den `AWS-IoT-FleetWise` Namespace verwenden. Weitere Informationen finden Sie unter Remote-Befehle im AWS IoT FleetWise Entwicklerhandbuch für Befehle.

Nutzlast

Wenn Sie den Befehl erstellen, müssen Sie eine Payload angeben, die die Aktionen definiert, die das Gerät ausführen muss. Die Payload kann ein beliebiges Format Ihrer Wahl verwenden. Um sicherzustellen, dass das Gerät die von Ihnen gesendeten Informationen korrekt lesen und verstehen kann, empfehlen wir Ihnen, den Payload-Formattyp im Befehl anzugeben. Wenn Ihre Geräte dies verwenden MQTT5, können sie dem MQTT-Standard folgen, um das Payload-Format zu identifizieren. Ein Formatindikator für JSON oder CBOR wird im Thema zur Befehlsanfrage verfügbar sein.

Zielgerät

Wenn Sie den Befehl ausführen möchten, müssen Sie ein Zielgerät angeben, das den Befehl empfängt und Aktionen ausführt. Wenn Ihr Gerät als Ding bei registriert wurde AWS IoT, können Sie den Namen des Dings verwenden. Wenn Ihr Gerät nicht registriert wurde, können Sie stattdessen die MQTT-Client-ID verwenden. Die Client-ID ist eine eindeutige Kennung für Ihr Gerät oder Ihren Client, die im MQTT Protokoll definiert ist. Es kann verwendet werden, um Ihr Gerät mit zu verbinden AWS IoT.

Ausführung von Befehlen

Eine Befehlsausführung ist eine Instanz eines Befehls, der auf dem Zielgerät ausgeführt wird. Wenn Sie die Ausführung starten, wird der Befehl (Payload) an das Zielgerät übermittelt. Für das Ziel wird jetzt eine eindeutige Befehlsausführungs-ID generiert. Das Gerät kann den Befehl dann

ausführen und seinen Fortschritt an melden AWS IoT. Die geräteseitige Logik bestimmt, wie der Befehl ausgeführt wird und wie der Status in den reservierten Themen veröffentlicht wird.

Themen zu Befehlen

Bevor Sie den Befehl ausführen, muss Ihr Gerät das Thema zur Befehlsanfrage abonniert haben. Wenn Sie die Anforderung zur Ausführung des Befehls an die Cloud senden, wird die Payload unter dem Thema „Befehlsanfrage“ an das Gerät gesendet. Nachdem das Gerät den Befehl ausgeführt hat, kann es das Ergebnis und den Status der Ausführung im Antwortthema des Befehls veröffentlichen. Weitere Informationen finden Sie unter Themen zu Befehlen.

## Status des Befehls

Ein Befehl, den Sie in Ihrem erstellen, AWS-Konto kann entweder den Status Verfügbar, Veraltet oder Ausstehende Löschung haben.

Verfügbar

Nachdem Sie eine Befehlsressource erfolgreich erstellt haben, befindet sie sich im Status „Verfügbar“. Der Befehl kann jetzt verwendet werden, um eine Befehlsausführung an das Gerät zu senden.

Als veraltet gekennzeichnet

Wenn Sie einen Befehl nicht mehr verwenden möchten, können Sie ihn als veraltet markieren. In diesem Status können Sie keine neuen Ausführungen des Befehls an Ihre Geräte senden. Alle ausstehenden Ausführungen, die bereits gestartet wurden, werden auf dem Gerät bis zum Abschluss weiterlaufen. Um neue Ausführungen zu senden, müssen Sie den Befehl wiederherstellen, damit er verfügbar wird.

Löschen ausstehend

Wenn Sie einen Befehl zum Löschen markieren und der Befehl für eine Dauer, die länger als das maximale Timeout ist, als veraltet gilt, wird der Befehl automatisch gelöscht. Diese Aktion ist dauerhaft und kann nicht rückgängig gemacht werden. Standardmäßig beträgt die maximale Timeout-Dauer 12 Stunden. Wenn der Befehl nicht veraltet ist oder für eine Dauer, die kürzer als das maximale Timeout ist, als veraltet gilt, befindet sich der Befehl im Status Ausstehende Löschung. Der Befehl wird nach Ablauf der maximalen Timeoutdauer automatisch aus Ihrem Konto entfernt.

# Status der Befehlsausführung

Wenn Sie die Befehlsausführung auf dem Zielgerät starten, wechselt die Befehlsausführung in einen `CREATED` Status. Es kann dann je nach dem vom Gerät gemeldeten Status in einen der anderen Befehlsausführungsstatus übergehen. Anschließend können Sie die Statusinformationen abrufen und Ihre Befehlsausführungen verfolgen.

> **Note**
>
> Für ein bestimmtes Zielgerät können Sie mehrere Befehle gleichzeitig ausführen. Sie können die Funktion zur Steuerung der Parallelität verwenden, um die maximale Anzahl von Ausführungen zu begrenzen, die an dasselbe Gerät gesendet werden, wodurch verhindert wird, dass das Gerät überlastet wird. Informationen zur maximalen Anzahl gleichzeitiger Ausführungen, die Sie für jedes Gerät ausführen können, finden Sie unter Befehlsquoten.AWS IoT Device Management

Die folgende Tabelle zeigt die verschiedenen Status einer Befehlsausführung und zeigt, wie die Befehlsausführung je nach Fortschritt der Ausführung zwischen den verschiedenen Status wechselt.

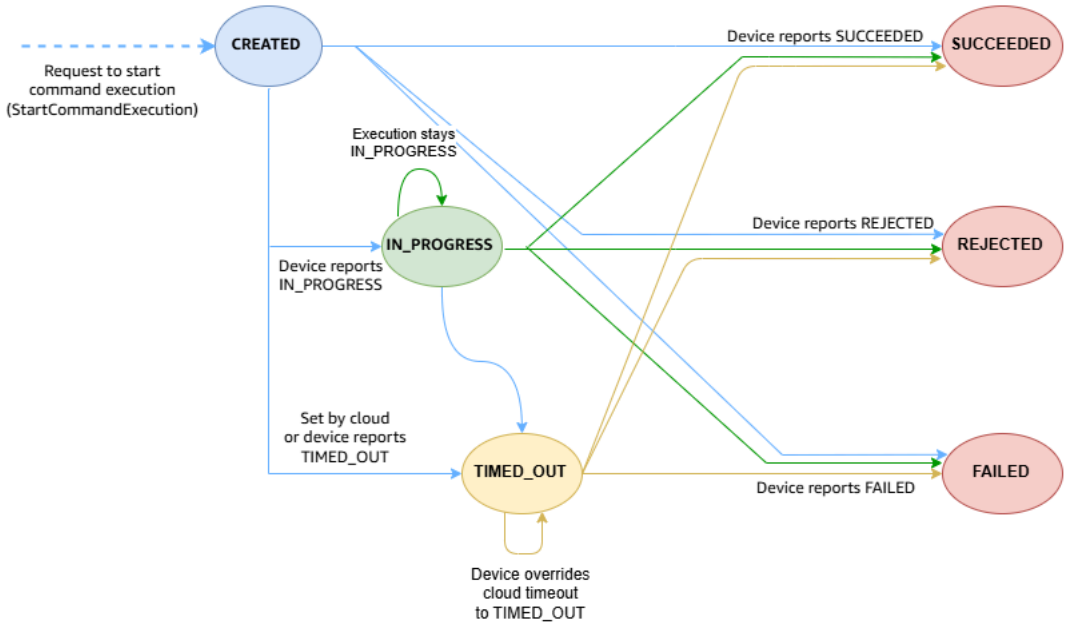
Status und Quelle der Befehlsausführung

| Status der Befehlsausführung | Vom Gerät/der Cloud initiiert? | Ausführung im Terminal? | Zulässige Statusübergänge |
|---|---|---|---|
| `CREATED` | Cloud | Nein | • IN_PROGRESS<br>• SUCCEEDED<br>• FEHLGESCHLAGEN<br>• ABGELEHNT<br>• TIMED_OUT |
| `IN_PROGRESS` | Gerät | Nein | • IN_PROGRESS<br>• SUCCEEDED<br>• FEHLGESCHLAGEN<br>• ABGELEHNT |

| Status der Befehlsausführung | Vom Gerät/der Cloud initiiert? | Ausführung im Terminal? | Zulässige Statusübergänge |
|---|---|---|---|
| | | | • TIMED_OUT |
| `TIMED_OUT` | Gerät und Cloud | Nein | • SUCCEEDED<br>• FEHLGESCHLAGEN<br>• ABGELEHNT<br>• TIMED_OUT |
| `SUCCEEDED` | Gerät | Ja | Nicht zutreffend |
| `FAILED` | Gerät | Ja | Nicht zutreffend |
| `REJECTED` | Gerät | Ja | Nicht zutreffend |

Wenn Ihre Geräte den Befehl ausführen, können sie mithilfe der für MQTT-Themen reservierten Befehle jederzeit Aktualisierungen des Status und der Ergebnisse in der Cloud veröffentlichen. Um zusätzlichen Kontext über den Status der einzelnen Befehlsausführungen in der Cloud bereitzustellen, kann sie die im `statusReason` Objekt enthaltenen `reasonCode` und `reasonDescription` verwenden.

Das folgende Diagramm zeigt die verschiedenen Status der Befehlsausführung und wie der Übergang zwischen ihnen erfolgt.




> **Note**
>
> Wenn AWS IoT festgestellt wird, dass das Gerät innerhalb des Timeout-Zeitraums nicht reagiert, wird es `TIMED_OUT` als temporärer Status festgelegt, der Wiederholungsversuche und Statusänderungen ermöglicht. Wenn Ihr Gerät `TIMED_OUT` während der Befehlsausführung explizit eine Meldung meldet, wird dies zu einem Terminalstatus, ohne dass weitere Übergänge möglich sind. Siehe Befehlsausführungen außerhalb des Terminals.

Im folgenden Abschnitt werden die Ausführung von Befehlen über das Terminal und ohne Terminal, die verschiedenen Ausführungsstatus und ihre Funktionsweise beschrieben.

Themen

- Befehlsausführungen außerhalb des Terminals
- Ausführungen von Terminal-Befehlen

## Befehlsausführungen außerhalb des Terminals

Ihre Befehlsausführung erfolgt nicht über ein Terminal, wenn bei der Ausführung Updates von Geräten oder Clients akzeptiert werden können. Eine Ausführung ohne Terminalstatus wird als Aktiv betrachtet. Bei den folgenden Status handelt es sich nicht um einen Terminalstatus.

- CREATED

  Wenn Sie die Ausführung eines Befehls von der AWS IoT Konsole aus starten oder den Befehl mithilfe der `StartCommandExecution` API an Ihr Gerät senden. Verwenden Sie dazu das Thema „Befehlsanfrage“. Wenn die Anfrage erfolgreich ist, ändert sich der Status der Befehlsausführung auf`CREATED`. Von diesem Status aus kann die Befehlsausführung in einen beliebigen anderen Status übergehen, der kein Terminal oder ein Terminal ist.

- IN_PROGRESS

  Nach Erhalt der Befehls-Payload kann Ihr Gerät mit der Ausführung der Anweisungen in der Payload beginnen und die angegebenen Aktionen ausführen. Während der Ausführung des Befehls kann das Gerät eine Antwort auf das Antwortthema des Befehls veröffentlichen und den Status der Befehlsausführung als aktualisieren. `IN_PROGRESS` Ausgehend vom `IN_PROGRESS` Status kann die Befehlsausführung in einen beliebigen anderen Terminal- oder Nicht-Terminal-Status übergehen, mit Ausnahme von. `CREATED`

  > **Note**
  >
  > Die `UpdateCommandExecution`-API kann mehrfach mit dem Status `IN_PROGRESS` aufgerufen werden. Mithilfe des Objekts können Sie zusätzliche Details zur Ausführung angeben. `statusReason`

- TIMED_OUT

  Dieser Befehlsausführungsstatus kann sowohl von der Cloud als auch vom Gerät ausgelöst werden. Eine Ausführung im `IN_PROGRESS` Status `CREATED` oder kann sich aus den folgenden Gründen in den `TIMED_OUT` Status ändern.

  - Nachdem der Befehl an das Gerät gesendet wurde, startet ein Timer. Wenn innerhalb einer bestimmten Dauer keine Antwort vom Gerät eingeht, ändert die Cloud den Status der Befehlsausführung auf`TIMED_OUT`. In diesem Fall erfolgt die Befehlsausführung nicht im Terminal.
  - Das Gerät kann den Status auf einen der anderen Terminalstatus überschreiben oder melden, dass bei der Ausführung des Befehls ein Timeout aufgetreten ist, und den Status auf setzen. `TIMED_OUT` In diesem Fall bleibt der Ausführungsstatus unverändert, `TIMED_OUT` aber die Felder des `StatusReason` Objekts ändern sich je nach den von den Geräten gemeldeten Informationen. Die Befehlsausführung wird jetzt zum Terminal.

  Weitere Informationen finden Sie unter Timeout-Wert und `TIMED_OUT` Ausführungsstatus.

### Ausführungen von Terminal-Befehlen

Eine Befehlsausführung wird zum Terminal, wenn die Ausführung keine zusätzlichen Updates von den Geräten mehr akzeptiert. Bei den folgenden Status handelt es sich um einen Terminalstatus. Eine Ausführung kann von jedem Status, der kein Terminal ist, oder, `CREATED` in den Terminalstatus übergehen. `IN_PROGRESS` `TIMED_OUT`

- SUCCEEDED

  Wenn das Gerät die Ausführung des Befehls erfolgreich abgeschlossen hat, kann es eine Antwort auf das Antwortthema des Befehls veröffentlichen und den Status der Befehlsausführung auf aktualisieren. `SUCCEEDED`

- FEHLGESCHLAGEN

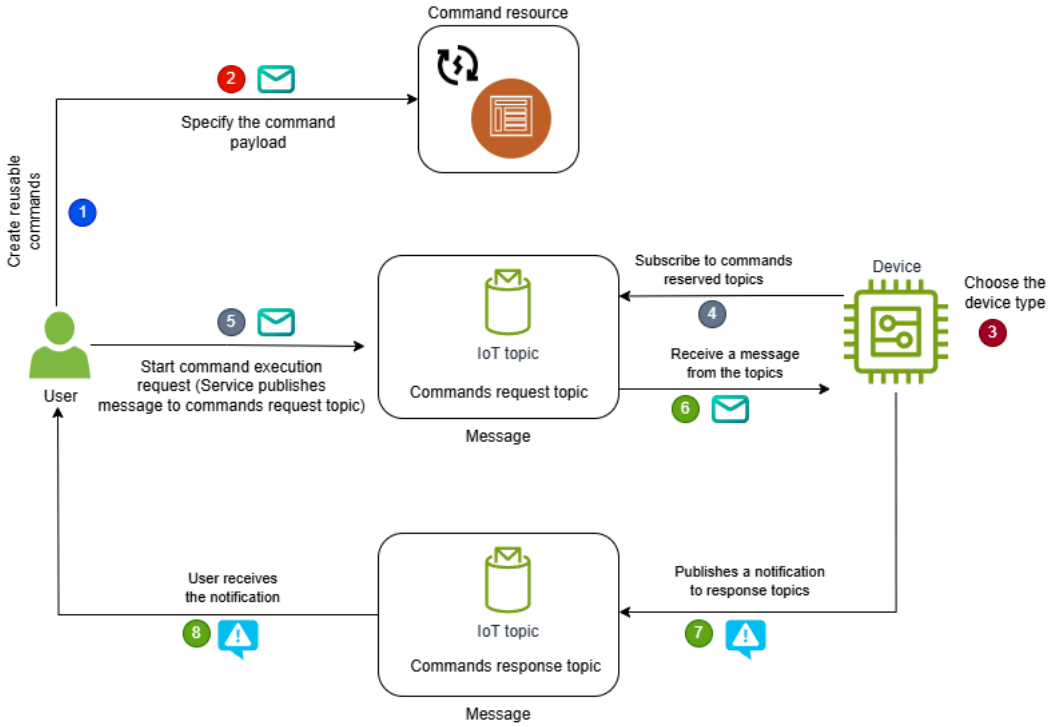
  Wenn Ihr Gerät die Ausführung des Befehls nicht abschließen kann, kann es eine Antwort auf das Antwortthema veröffentlichen und den Status der Befehlsausführung auf aktualisieren`FAILED`. Sie können die `reasonDescription` Felder `reasonCode` und des `statusReason` Objekts oder die CloudWatch Protokolle verwenden, um die Fehler weiter zu beheben.

- ABGELEHNT

  Wenn Ihr Gerät eine ungültige oder inkompatible Anfrage erhält, kann das Gerät die `UpdateCommandExecution` API mit dem Status aufrufen. `REJECTED` Sie können die `reasonDescription` Felder `reasonCode` und des `statusReason` Objekts oder die CloudWatch Protokolle verwenden, um weitere Probleme zu beheben.

## Arbeitsablauf für Befehle auf hoher Ebene

Die folgenden Schritte bieten einen Überblick über den Befehlsablauf zwischen Ihren Geräten und AWS IoT Device Management Befehlen. Wenn Sie einen der HTTP-API-Befehle verwenden, wird die Anfrage mit Sigv4-Anmeldeinformationen signiert.




Workflow-Übersicht

- Befehle erstellen und verwalten
- Wählen Sie das Zielgerät für Ihre Befehle und abonnieren Sie MQTT-Themen
- Starten und überwachen Sie die Befehlsausführungen für Ihr Zielgerät
- (Optional) Aktivieren Sie Benachrichtigungen für Befehlsereignisse

## Befehle erstellen und verwalten

Gehen Sie wie folgt vor, um Befehle für Ihre Geräte zu erstellen und zu verwalten.

1. Erstellen Sie eine Befehlsressource

   Bevor Sie den Befehl an Ihre Geräte senden können, erstellen Sie eine Befehlsressource im Command Hub der AWS IoT Konsole oder mithilfe der API-Operation der `CreateCommand`Steuerungsebene.

2. Geben Sie die Nutzlast an

   Bei der Erstellung des Befehls müssen Sie eine Nutzlast für Ihren Befehl angeben. Der Payload-Inhalt kann ein beliebiges Format Ihrer Wahl verwenden. Um sicherzustellen, dass das Gerät die Payload korrekt interpretiert, empfehlen wir, dass Sie auch den Payload-Inhaltstyp angeben.

3. (Optional) Verwalte die erstellten Befehle

   Nachdem Sie den Befehl erstellt haben, können Sie den Anzeigenamen und die Beschreibung des Befehls aktualisieren. Sie können einen Befehl auch als veraltet markieren, wenn Sie ihn nicht mehr verwenden möchten, oder den Befehl vollständig aus Ihrem Konto entfernen. Wenn Sie die Payload-Informationen ändern möchten, müssen Sie einen neuen Befehl erstellen und die neue Payload-Datei hochladen.

## Wählen Sie das Zielgerät für Ihre Befehle und abonnieren Sie MQTT-Themen

Um sich auf den Befehls-Workflow vorzubereiten, wählen Sie Ihr Zielgerät aus und geben Sie die AWS IoT reservierten MQTT-Themen an, um Befehle zu empfangen und Antwortnachrichten zu veröffentlichen.

1. Wählen Sie das Zielgerät für Ihren Befehl

   Um sich auf den Befehls-Workflow vorzubereiten, wählen Sie Ihr Zielgerät aus, das den Befehl empfangen und die angegebenen Aktionen ausführen soll. Das Zielgerät kann ein Gerät sein AWS IoT , das Sie in der AWS IoT Registrierung registriert haben, oder es kann mithilfe der MQTT-Client-ID angegeben werden, falls Ihr Gerät nicht registriert wurde. AWS IoT Weitere Informationen finden Sie unter Überlegungen zum Zielgerät.

2. Konfigurieren Sie die IoT-Geräterichtlinie

   Bevor Ihr Gerät Befehlsausführungen empfangen und Updates veröffentlichen kann, muss es eine IAM-Richtlinie verwenden, die Berechtigungen zur Ausführung dieser Aktionen gewährt. Beispiele für Beispielrichtlinien, die Sie verwenden können, je nachdem, ob Ihr Gerät als AWS IoT Ding registriert oder als MQTT-Client-ID angegeben ist, finden Sie unter. Beispiel einer IAM-Richtlinie

3. Stellen Sie eine MQTT-Verbindung her

   Um Ihre Geräte auf die Verwendung der Befehlsfunktion vorzubereiten, müssen Ihre Geräte zunächst eine Verbindung zum Message Broker herstellen und die Anfrage- und Antwortthemen abonnieren. Ihr Gerät muss in der Lage sein, die `iot:Connect` Aktion auszuführen, um eine Verbindung zum Message Broker herzustellen AWS IoT Core und eine MQTT-Verbindung mit diesem herzustellen. Verwenden Sie die `DescribeEndpoint` API oder den `describe-endpoint` CLI-Befehl AWS-Konto, um den Datenebenen-Endpunkt für Ihren zu finden, wie unten gezeigt.

   ```
   aws iot describe-endpoint --endpoint-type iot:Data-ATS
   ```

   Wenn Sie diesen Befehl ausführen, wird der kontospezifische Endpunkt der Datenebene zurückgegeben, wie unten gezeigt.

   ```
   account-specific-prefix.iot.region.amazonaws.com
   ```

4. Abonnieren Sie die Themen zu Befehlen

   Nachdem eine Verbindung hergestellt wurde, können Ihre Geräte das Thema zur Befehlsanfrage abonnieren. Wenn Sie einen Befehl erstellen und die Befehlsausführung auf Ihrem Zielgerät starten, wird die Payload-Nachricht vom Message Broker unter dem Thema der Anfrage veröffentlicht. Ihr Gerät kann dann die Payload-Nachricht empfangen und den Befehl verarbeiten.

   (Optional) Ihre Geräte können die Antwortthemen dieser Befehle auch abonnieren (`accepted`oder`rejected`), um eine Nachricht zu erhalten, die angibt, ob der Cloud-Dienst die Antwort des Geräts akzeptiert oder abgelehnt hat.

   Ersetzen Sie in diesem Beispiel:

   - *<device>*mit `thing` oder `client` abhängig davon, ob das Gerät, auf das Sie abzielen, als IoT-Ding registriert oder als MQTT-Client spezifiziert wurde.
   - *<DeviceID>*mit der eindeutigen Kennung Ihres Zielgeräts. Diese ID kann die eindeutige MQTT-Client-ID oder ein Ding-Name sein.

> **Note**
>
> Wenn der Payload-Typ nicht JSON oder CBOR ist, ist das *<PayloadFormat>* Feld möglicherweise nicht im Thema der Befehlsanfrage vorhanden. Um das Payload-Format zu erhalten, empfehlen wir, MQTT 5 zu verwenden, um die Formatinformationen aus den MQTT-Nachrichtenheadern abzurufen. Weitere Informationen finden Sie unter Themen zu Befehlen.

```
$aws/commands/<devices>/<DeviceID>/executions/+/request/<PayloadFormat>
$aws/commands/<devices>/<DeviceID>/executions/+/response/accepted/<PayloadFormat>
$aws/commands/<devices>/<DeviceID>/executions/+/response/rejected/<PayloadFormat>
```

## Starten und überwachen Sie die Befehlsausführungen für Ihr Zielgerät

Nachdem Sie die Befehle erstellt und die Ziele für den Befehl angegeben haben, können Sie die Ausführung auf dem Zielgerät starten, indem Sie die folgenden Schritte ausführen.

1. Starten Sie die Befehlsausführung auf dem Zielgerät

   Starten Sie die Befehlsausführung auf dem Zielgerät vom Command Hub der AWS IoT Konsole aus oder verwenden Sie die `StartCommandExecution` Datenebenen-API mit Ihrem kontospezifischen Endpunkt`iot:Jobs`. Die API veröffentlicht die Payload-Meldung zum oben genannten Thema der Befehlsanfrage, die das Gerät abonniert hat.

   > **Note**
   >
   > Wenn das Gerät offline war, als der Befehl aus der Cloud gesendet wurde, und wenn es persistente MQTT-Sitzungen verwendet, wartet der Befehl beim Message Broker. Wenn das Gerät vor Ablauf des Timeouts wieder online ist und das Thema für die Befehlsanfrage abonniert hat, kann das Gerät den Befehl verarbeiten und das Ergebnis im Befehlsantwortthema veröffentlichen. Wenn das Gerät vor Ablauf des Timeouts nicht wieder online ist, kommt es bei der Befehlsausführung zu einem Timeout, und die Nutzdatennachricht läuft möglicherweise ab und wird vom Message Broker verworfen.

2. Aktualisieren Sie das Ergebnis der Befehlsausführung

   Das Gerät empfängt jetzt die Payload-Nachricht und kann den Befehl verarbeiten und die angegebenen Aktionen ausführen. Anschließend kann das Ergebnis der Befehlsausführung mithilfe der `UpdateCommandExecution` API im folgenden Antwortthema für Befehle veröffentlicht werden. Wenn Ihr Gerät die Antwortthemen „Befehle akzeptiert und abgelehnt“ abonniert hat, erhält es eine Meldung, die angibt, ob die Antwort vom Cloud-Dienst akzeptiert oder abgelehnt wurde.

   Je nachdem, wie Sie im Thema der Anfrage angegeben haben, *<devices>* kann es sich entweder um Dinge oder Clients handeln, und es *<DeviceID>* kann sich dabei um Ihren IoT-Dingnamen oder die MQTT-Client-ID handeln.

   > **Note**
   >
   > Das *<PayloadFormat>* kann im Antwortthema der Befehle nur JSON oder CBOR sein.

   ```
   $aws/commands/<devices>/<DeviceID>/executions/<ExecutionId>/
   response/<PayloadFormat>
   ```

3. (Optional) Rufen Sie das Ergebnis der Befehlsausführung ab

   Um das Ergebnis der Befehlsausführung abzurufen, können Sie den Befehlsverlauf von der AWS IoT Konsole aus anzeigen oder den API-Vorgang der `GetCommandExecution` Steuerungsebene verwenden. Um die neuesten Informationen zu erhalten, muss Ihr Gerät das Ergebnis der Befehlsausführung im Thema Befehlsantwort veröffentlicht haben. Sie können auch zusätzliche Informationen zu den Ausführungsdaten abrufen, z. B. wann sie zuletzt aktualisiert wurden, das Ausführungsergebnis und wann die Ausführung abgeschlossen wurde.

## (Optional) Aktivieren Sie Benachrichtigungen für Befehlsereignisse

Sie können Befehlsereignisse abonnieren, um Benachrichtigungen zu erhalten, wenn sich der Status der Befehlsausführung ändert. In den folgenden Schritten erfahren Sie, wie Sie Befehlsereignisse abonnieren und sie dann verarbeiten.

1. Erstellen einer Themenregel

   Sie können das Thema Befehlsereignisse abonnieren und Benachrichtigungen erhalten, wenn sich der Status der Befehlsausführung ändert. Sie können auch eine Themenregel erstellen, um die vom Gerät verarbeiteten Daten an andere AWS IoT Dienste weiterzuleiten, die von Regeln unterstützt werden AWS Lambda, wie Amazon SQS und AWS Step Functions. Sie können eine Themenregel entweder mithilfe der AWS IoT Konsole oder mithilfe der API-Operation auf der `CreateTopicRule` AWS IoT Core Kontrollebene erstellen. Weitere Informationen finden Sie unter Eine AWS IoT Regel erstellen.

   Ersetzen Sie in diesem Beispiel *<CommandID>* durch die ID des Befehls, für den Sie Benachrichtigungen erhalten möchten, und *<CommandExecutionStatus>* durch den Status der Befehlsausführung.

   ```
   $aws/events/commandExecution/<CommandID>/<CommandExecutionStatus>
   ```

   > **Note**
   >
   > Um Benachrichtigungen für alle Befehle und den Status der Befehlsausführung zu erhalten, können Sie Platzhalterzeichen verwenden und das folgende Thema abonnieren.

   ```
   $aws/events/commandExecution/+/#
   ```

2. Befehlsereignisse empfangen und verarbeiten

   Wenn Sie im vorherigen Schritt eine Themenregel zum Abonnieren von Befehlsereignissen erstellt haben, können Sie die Push-Benachrichtigungen für Befehle, die Sie erhalten, verwalten und auf diesen Diensten eine Anwendung erstellen.

Der folgende Code zeigt eine Beispiel-Payload für die Benachrichtigungen über Befehlsereignisse, die Sie erhalten werden.

```
{
    "executionId": "2bd65c51-4cfd-49e4-9310-d5cbfdbc8554",
    "status":"FAILED",
    "statusReason": {
```

```
        "reasonCode": "DEVICE_TOO_BUSY",
        "reasonDescription": ""
    },
    "eventType": "COMMAND_EXECUTION",
    "commandArn":"arn:aws:iot:us-east-1:123456789012:command/0b9d9ddf-
e873-43a9-8e2c-9fe004a90086",
    "targetArn":"arn:aws:iot:us-east-1:123456789012:thing/5006c3fc-
de96-4def-8427-7eee36c6f2bd",
    "timestamp":1717708862107
}
```

# Befehle erstellen und verwalten

Sie können die AWS IoT Device Management Befehlsfunktion verwenden, um entweder wiederverwendbare Fernaktionen zu konfigurieren oder einmalige, sofortige Anweisungen an Ihre Geräte zu senden. In den folgenden Abschnitten erfahren Sie, wie Sie Befehle von der AWS IoT Konsole aus und mithilfe der erstellen und verwalten können AWS CLI.

Befehlsoperationen erstellen und verwalten

- Erstellen Sie eine Befehlsressource
- Ruft Informationen zu einem Befehl ab
- Listen Sie Befehle in Ihrem auf AWS-Konto
- Aktualisieren Sie eine Befehlsressource
- Verwerfen Sie eine Befehlsressource oder stellen Sie sie wieder her
- Löschen Sie eine Befehlsressource

## Erstellen Sie eine Befehlsressource

Wenn Sie einen Befehl erstellen, müssen Sie die folgenden Informationen angeben.

- Allgemeine Informationen

  Wenn Sie einen Befehl erstellen, müssen Sie eine Befehls-ID angeben. Dabei handelt es sich um eine eindeutige Kennung, anhand derer Sie den Befehl identifizieren können, wenn Sie ihn auf dem Zielgerät ausführen möchten. Optional können Sie auch einen Anzeigenamen, eine Beschreibung und Tags angeben, um Ihnen die Verwaltung des Befehls zu erleichtern.
- Nutzlast

Sie müssen auch eine Payload angeben, die die Aktionen definiert, die das Gerät ausführen muss. Es ist zwar optional, wir empfehlen jedoch, den Payload-Formattyp anzugeben, damit das Gerät die Payload korrekt interpretiert.

Themen zu Payload und Befehlen

Die reservierten Themen zu Befehlen verwenden ein Format, das vom Typ des Payload-Formats abhängt.

- Wenn Sie den Payload-Inhaltstyp `application/json` oder angeben`application/cbor`, lautet das Anforderungsthema wie folgt.

```
$aws/commands/<devices>/<DeviceID>/executions/+/request/<PayloadFormat>
```

- Wenn Sie einen anderen Payload-Inhaltstyp als `application/json` oder angeben`application/cbor`, oder wenn Sie den Payload-Formattyp nicht angeben, lautet das Anforderungsthema wie folgt. In diesem Fall wird das Payload-Format in den MQTT Nachrichtenheader aufgenommen.

```
$aws/commands/<devices>/<DeviceID>/executions/+/request
```

Das Antwortthema des Befehls gibt ein Format zurück, das den Payload-Formattyp verwendet `json` oder von diesem `cbor` unabhängig ist. Das Antwortthema verwendet das folgende Format, wobei der Wert `json` oder *<PayloadFormat>* `cbor` angegeben werden muss.

```
$aws/commands/<devices>/<DeviceID>/executions/<ExecutionId>/response/<PayloadFormat>
```

Erstellen Sie eine Befehlsressource (Konsole)

In den folgenden Abschnitten erfahren Sie, was beim Format der Befehlspayload zu beachten ist und wie Sie Befehle von der Konsole aus erstellen.

Themen

- Format der Befehls-Payload
- Wie erstelle ich einen Befehl (Konsole)

### Format der Befehls-Payload

Die Nutzlast kann ein beliebiges Format Ihrer Wahl verwenden. Die maximale Größe der Payload darf 32 KB nicht überschreiten. Um sicherzustellen, dass das Gerät die Payload sicher und korrekt interpretieren kann, empfehlen wir Ihnen, den Payload-Formattyp anzugeben.

Sie geben den Payload-Formattyp mithilfe des `type/subtype` Formats an, z. B. oder. `application/json` `application/cbor` Standardmäßig wird es als `application/octet-stream` festgelegt. Informationen zu Payload-Formaten, die Sie angeben können, finden Sie unter Allgemeine MIME Typen.

### Wie erstelle ich einen Befehl (Konsole)

Um einen Befehl von der Konsole aus zu erstellen, rufen Sie den Command Hub der AWS IoT Konsole auf und führen Sie die folgenden Schritte aus.

1. Um eine neue Befehlsressource zu erstellen, wählen Sie Befehl erstellen.
2. Geben Sie eine eindeutige Befehls-ID an, um den Befehl zu identifizieren, den Sie auf dem Zielgerät ausführen möchten.
3. (Optional) Geben Sie einen optionalen Anzeigenamen, eine Beschreibung und beliebige Name-Wert-Paare als Tags für Ihren Befehl an.
4. Laden Sie die Payload-Datei aus Ihrem lokalen Speicher hoch, die die Aktionen enthält, die das Gerät ausführen muss. Es ist zwar optional, wir empfehlen jedoch, den Payload-Formattyp anzugeben, damit das Gerät die Datei korrekt interpretiert und die Anweisungen verarbeitet.
5. Wählen Sie den Befehl Erstellen.

### Erstellen Sie eine Befehlsressource (CLI)

In diesem Abschnitt werden die API Operation auf der HTTP Steuerungsebene und der entsprechende AWS CLI Befehl beschrieben `create-command`, den Sie ausführen können, um eine Befehlsressource zu erstellen. `CreateCommand`

Themen

- Payload des Befehls
- Beispiel für eine Richtlinie IAM
- Beispiel für einen Befehl erstellen

### Payload des Befehls

Bei der Erstellung des Befehls müssen Sie eine Payload angeben. Die von Ihnen bereitgestellte Nutzlast ist Base64-codiert. Wenn Ihre Geräte den Befehl empfangen, kann die geräteseitige Logik die Nutzlast verarbeiten und die angegebenen Aktionen ausführen. Um sicherzustellen, dass Ihre Geräte den Befehl und die Payload korrekt empfangen, empfehlen wir Ihnen, den Payload-Inhaltstyp anzugeben.

> **Note**
>
> Nachdem Sie den Befehl erstellt haben, können Sie die Payload nicht mehr ändern. Um die Payload zu ändern, müssen Sie einen neuen Befehl erstellen.

### Beispiel für eine Richtlinie IAM

Bevor Sie diesen API Vorgang verwenden, stellen Sie sicher, dass Ihre IAM Richtlinie Sie autorisiert, diese Aktion auf dem Gerät durchzuführen. Das folgende Beispiel zeigt eine IAM Richtlinie, die dem Benutzer die Erlaubnis erteilt, die `CreateCommand` Aktion auszuführen.

Ersetzen Sie in diesem Beispiel:

- *`region`*mit Ihrem AWS-Region, wie zum Beispiel*`ap-south-1`*.
- *`account-id`*mit deiner AWS-Konto Nummer, wie*`123456789012`*.
- *`command-id`*mit einer eindeutigen Kennung für Ihre AWS IoT Befehls-ID, z. *`LockDoor`* B. Wenn Sie mehr als einen Befehl senden möchten, können Sie diese Befehle in der IAM Richtlinie im Abschnitt Ressource angeben.

```
{
    "Version": "2012-10-17",
    "Statement":
    {
        "Action": "iot:CreateCommand",
        "Effect": "Allow",
        "Resource": "arn:aws:iot:<region>:<account_id>:command/command-id"
    }
}
```

Beispiel für einen Befehl erstellen

Das folgende Beispiel zeigt, wie Sie einen Befehl erstellen können. Ersetzen Sie je nach Anwendung:

- *<command-id>*mit einer eindeutigen Kennung für den Befehl. Um beispielsweise die Dokumentenhistorie Ihres Hauses zu sperren, können Sie Folgendes angeben: *LockDoor* Wir empfehlen Ihnen, UUID zu verwenden. Sie können auch alphanumerische Zeichen, „-“ und „_“, verwenden.
- (Optional) *<display-name>* und. *<description>* Dabei handelt es sich um optionale Felder, die Sie verwenden können, um einen benutzerfreundlichen Namen und eine aussagekräftige Beschreibung für den Befehl anzugeben, z. B. *Lock the doors of my home*
- `namespace`, mit denen Sie den Namespace des Befehls angeben können. Das muss es sein. `AWS-IoT`
- `payload`enthält Informationen über die Payload, die Sie bei der Ausführung des Befehls verwenden möchten, und deren Inhaltstyp.

```
aws iot create-command \
    --command-id <command-id> \
    --display-name <display-name> \
    --description <description> \
    --namespace AWS-IoT \
    --payload
 '{"content":"eyAibWVzc2FnZSI6ICJIZWxsbyBJb1QiIH0=","contentType":"application/json"}'
```

Die Ausführung dieses Befehls generiert eine Antwort, die die ID und ARN (Amazon-Ressourcenname) des Befehls enthält. Wenn Sie den *LockDoor* Befehl beispielsweise bei der Erstellung angegeben haben, zeigt das Folgende ein Beispiel für die Ausgabe der Ausführung des Befehls.

```
{
    "commandId": "LockDoor",
    "commandArn": "arn:aws:iot:ap-south-1:123456789012:command/LockDoor"
}
```

## Ruft Informationen zu einem Befehl ab

Nachdem Sie einen Befehl erstellt haben, können Sie Informationen dazu von der AWS IoT Konsole abrufen und den verwenden AWS CLI. Sie können die folgenden Informationen abrufen.

- Die Befehls-ID, der Amazon-Ressourcenname (ARN), ein beliebiger Anzeigename und eine Beschreibung, die Sie für den Befehl angegeben haben.
- Der Befehlsstatus, der angibt, ob ein Befehl auf dem Zielgerät ausgeführt werden kann oder ob er veraltet oder gelöscht ist.
- Die von Ihnen bereitgestellte Payload und ihr Formattyp.
- Die Uhrzeit, zu der der Befehl erstellt und zuletzt aktualisiert wurde.

Ruft eine Befehlsressource (Konsole) ab

Um einen Befehl von der Konsole abzurufen, gehen Sie zum Command Hub der AWS IoT Konsole und wählen Sie dann den Befehl aus, den Sie erstellt haben, um dessen Details anzuzeigen.

Zusätzlich zu den Befehlsdetails können Sie den Befehlsverlauf einsehen, der Informationen über die Ausführung des Befehls auf dem Zielgerät enthält. Nachdem Sie diesen Befehl auf dem Gerät ausgeführt haben, finden Sie auf dieser Registerkarte Informationen zu den Ausführungen.

Rufen Sie eine Befehlsressource ab () CLI

Verwenden Sie die API Operation auf der `GetCommand`HTTPSteuerungsebene oder den `get-command` AWS CLI Befehl, um Informationen über eine Befehlsressource abzurufen. Sie müssen den Befehl bereits mit der `CreateCommand` API Anfrage oder dem erstellt haben `create-command`CLI.

Beispiel für eine IAM Richtlinie

Bevor Sie diesen API Vorgang verwenden, stellen Sie sicher, dass Ihre IAM Richtlinie Sie autorisiert, diese Aktion auf dem Gerät durchzuführen. Das folgende Beispiel zeigt eine IAM Richtlinie, die dem Benutzer die Erlaubnis erteilt, die `GetCommand` Aktion auszuführen.

Ersetzen Sie in diesem Beispiel:

- *`region`*mit Ihrem AWS-Region, wie zum Beispiel`ap-south-1`.
- *`account-id`*mit deiner AWS-Konto Nummer, wie*`123456789023`*.
- *`command-id`*mit Ihrer AWS IoT eindeutigen Befehlskennung, z. *`LockDoor`* B. Wenn Sie mehr als einen Befehl abrufen möchten, können Sie diese Befehle in der IAM Richtlinie im Abschnitt Ressource angeben.

```
{
    "Version": "2012-10-17",
```

```
    "Statement":
    {
        "Action": "iot:GetCommand",
        "Effect": "Allow",
        "Resource": "arn:aws:iot:<region>:<account_id>:command/command-id"
    }
}
```

Beispiel für einen Befehl abrufen (AWS CLI)

Das folgende Beispiel zeigt Ihnen, wie Sie Informationen zu einem Befehl mit dem abrufen können `get-command` AWS CLI. Ersetzen Sie je nach Anwendung *<command-id>* durch den Bezeichner für den Befehl, für den Sie Informationen abrufen möchten. Sie können diese Informationen der Antwort des entnehmen `create-command`CLI.

```
aws iot get-command --command-id <command-id>
```

Wenn Sie diesen Befehl ausführen, wird eine Antwort generiert, die Informationen über den Befehl, die Nutzlast und den Zeitpunkt der Erstellung und letzten Aktualisierung enthält. Es enthält auch Informationen, die angeben, ob ein Befehl veraltet ist oder gelöscht wird.

Der folgende Code zeigt beispielsweise eine Beispielantwort.

```
{
    "commandId": "LockDoor",
    "commandArn": "arn:aws:iot:<region>:<account>:command/LockDoor",
    "namespace": "AWS-IoT",
    "payload":{
        "content": "eyAibWVzc2FnZSI6ICJIZWxsbyBJb1QiIH0=",
        "contentType": "application/json"
    },
    "createdAt": "2024-03-23T00:50:10.095000-07:00",
    "lastUpdatedAt": "2024-03-23T00:50:10.095000-07:00",
    "deprecated": false,
    "pendingDeletion": false
}
```

## Listen Sie Befehle in Ihrem auf AWS-Konto

Nachdem Sie Befehle erstellt haben, können Sie sich die Befehle ansehen, die Sie in Ihrem Konto erstellt haben. In der Liste finden Sie Informationen zu:

- Die Befehls-ID und alle Anzeigenamen, die Sie für die Befehle angegeben haben.
- Der Amazon-Ressourcenname (ARN) der Befehle.
- Der Befehlsstatus, der angibt, ob die Befehle für die Ausführung auf dem Zielgerät verfügbar sind oder ob sie veraltet sind.

> **Note**
>
> In der Liste wird nicht angezeigt, welche aus Ihrem Konto gelöscht werden. Wenn die Befehle noch nicht gelöscht werden müssen, können Sie die Details zu diesen Befehlen immer noch anhand ihrer Befehls-ID anzeigen.

- Der Zeitpunkt, zu dem die Befehle erstellt und zuletzt aktualisiert wurden.

Befehle in Ihrem Konto (Konsole) auflisten

In der AWS IoT Konsole finden Sie die Liste der Befehle, die Sie erstellt haben, und deren Details, indem Sie zum Command Hub gehen.

Befehle in Ihrem Konto auflisten (CLI)

Um die Befehle aufzulisten, die Sie erstellt haben, verwenden Sie die `ListCommands`APIOperation oder die `list-commands`CLI.

Beispiel für eine IAM Richtlinie

Bevor Sie diesen API Vorgang verwenden, stellen Sie sicher, dass Ihre IAM Richtlinie Sie autorisiert, diese Aktion auf dem Gerät durchzuführen. Das folgende Beispiel zeigt eine IAM Richtlinie, die dem Benutzer die Erlaubnis erteilt, die `ListCommands` Aktion auszuführen.

Ersetzen Sie in diesem Beispiel:

- *`region`*mit Ihrem AWS-Region, wie zum Beispiel`ap-south-1`.
- *`account-id`*mit deiner AWS-Konto Nummer, wie*`123456789012`*.

```
{
    "Version": "2012-10-17",
    "Statement":
    {
        "Action": "iot:ListCommands",
```

```
        "Effect": "Allow",
        "Resource": "arn:aws:iot:<region>:<account_id>:command/*"
    }
}
```

Führen Sie Befehle in Ihrem Kontobeispiel auf

Der folgende Befehl zeigt, wie Sie Befehle in Ihrem Konto auflisten können.

```
aws iot list-commands --namespace "AWS-IoT"
```

Wenn Sie diesen Befehl ausführen, wird eine Antwort generiert, die eine Liste von Befehlen enthält, die Sie erstellt haben, sowie den Zeitpunkt, zu dem die Befehle erstellt wurden und wann sie zuletzt aktualisiert wurden. Er stellt auch Informationen zum Befehlsstatus bereit, die angeben, ob ein Befehl veraltet ist oder auf dem Zielgerät ausgeführt werden kann. Weitere Informationen zu den verschiedenen Status und den Gründen für den Status finden Sie unter. Status der Befehlsausführung

## Aktualisieren Sie eine Befehlsressource

Nachdem Sie einen Befehl erstellt haben, können Sie den Anzeigenamen und die Beschreibung des Befehls aktualisieren.

> **Note**
>
> Die Payload für den Befehl kann nicht aktualisiert werden. Um diese Informationen zu aktualisieren oder eine geänderte Payload zu verwenden, müssen Sie einen neuen Befehl erstellen.

Aktualisieren Sie eine Befehlsressource (Konsole)

Um einen Befehl von der Konsole aus zu aktualisieren, rufen Sie den Command Hub der AWS IoT Konsole auf und führen Sie die folgenden Schritte aus.

1. Um eine vorhandene Befehlsressource zu aktualisieren, wählen Sie den Befehl aus, den Sie aktualisieren möchten, und wählen Sie dann unter Aktionen die Option Bearbeiten aus.
2. Geben Sie den Anzeigenamen und die Beschreibung an, die Sie verwenden möchten, sowie alle Name-Wert-Paare als Tags für Ihren Befehl.

3. Wählen Sie Bearbeiten, um den Befehl mit den neuen Einstellungen zu speichern.

### Aktualisieren Sie eine Befehlsressource (CLI)

Verwenden Sie die API Operation auf der `UpdateCommand`Steuerungsebene oder die `update-command` AWS CLI , um eine Befehlsressource zu aktualisieren. Damit API können Sie:

- Bearbeiten Sie den Anzeigenamen und die Beschreibung eines Befehls, den Sie erstellt haben.
- Verwerfen Sie eine Befehlsressource oder stellen Sie einen Befehl wieder her, der bereits veraltet ist.

### IAMBeispiel für eine Richtlinie

Bevor Sie diesen API Vorgang verwenden, stellen Sie sicher, dass Ihre IAM Richtlinie Sie autorisiert, diese Aktion auf dem Gerät durchzuführen. Das folgende Beispiel zeigt eine IAM Richtlinie, die dem Benutzer die Erlaubnis erteilt, die `UpdateCommand` Aktion auszuführen.

Ersetzen Sie in diesem Beispiel:

- *`region`*mit Ihrem AWS-Region, wie zum Beispiel`ap-south-1`.
- *`account-id`*mit deiner AWS-Konto Nummer, wie*`123456789012`*.
- *`command-id`*mit Ihrer AWS IoT eindeutigen Befehlskennung, z. *`LockDoor`* B. Wenn Sie mehr als einen Befehl abrufen möchten, können Sie diese Befehle in der IAM Richtlinie im Abschnitt Ressource angeben.

```
{
    "Version": "2012-10-17",
    "Statement":
    {
        "Action": "iot:UpdateCommand",
        "Effect": "Allow",
        "Resource": "arn:aws:iot:<region>:<account_id>:command/<command-id>"
    }
}
```

Informationen zu einem Befehl aktualisieren — Beispiele (AWS CLI)

Das folgende Beispiel zeigt Ihnen, wie Sie Informationen zu einem Befehl mithilfe des `update-command` AWS CLI Befehls aktualisieren. Hinweise dazu, wie Sie API damit eine Befehlsressource als veraltet markieren oder wiederherstellen können, finden Sie unter. Aktualisieren Sie eine Befehlsressource (CLI)

Das Beispiel zeigt, wie Sie den Anzeigenamen und die Beschreibung eines Befehls aktualisieren können. Je nach Anwendung *<command-id>* ersetzen Sie ihn durch den Bezeichner für den Befehl, für den Sie Informationen abrufen möchten.

```
aws iot update-command \
    --command-id <command-id>
    --displayname <display-name> \
    --description <description>
```

Wenn Sie diesen Befehl ausführen, wird eine Antwort generiert, die die aktualisierten Informationen über den Befehl und den Zeitpunkt der letzten Aktualisierung enthält. Der folgende Code zeigt eine Beispielanforderung und -antwort für die Aktualisierung des Anzeigenamens und der Beschreibung eines Befehls, der die Klimaanlage ausschaltet.

```
aws iot update-command \
    --command-id <LockDoor> \
    --displayname <Secondary lock door> \
    --description <Locks doors to my home>
```

Die Ausführung dieses Befehls generiert die folgende Antwort.

```
{
    "commandId": "LockDoor",
    "commandArn": "arn:aws:iot:ap-south-1:123456789012:command/LockDoor",
    "displayName": "Secondary lock door",
    "description": "Locks doors to my home",
    "lastUpdatedAt": "2024-05-09T23:15:53.899000-07:00"
}
```

## Verwerfen Sie eine Befehlsressource oder stellen Sie sie wieder her

Wenn Sie einen Befehl erstellt haben und ihn nicht mehr weiter verwenden möchten, können Sie ihn als veraltet markieren. Wenn Sie einen Befehl als veraltet markieren, werden alle ausstehenden

Befehlsausführungen auf dem Zielgerät weiterlaufen, bis sie den Terminalstatus erreichen. Wenn ein Befehl als veraltet gilt und Sie ihn beispielsweise zum Senden einer neuen Befehlsausführung an das Zielgerät verwenden möchten, müssen Sie ihn wiederherstellen.

> **Note**
>
> Sie können einen veralteten Befehl nicht bearbeiten oder neue Ausführungen für ihn ausführen. Um neue Befehle auf dem Gerät auszuführen, müssen Sie es wiederherstellen, sodass der Befehlsstatus auf Verfügbar geändert wird.

Weitere Informationen zum Verwerfen und Wiederherstellen eines Befehls sowie zu diesbezüglichen Überlegungen finden Sie unter. Eine Befehlsressource als veraltet kennzeichnen

## Löschen Sie eine Befehlsressource

Wenn Sie einen Befehl nicht mehr verwenden möchten, können Sie ihn dauerhaft aus Ihrem Konto entfernen. Wenn die Löschaktion erfolgreich ist:

- Wenn der Befehl für eine Dauer, die länger als das maximale Timeout von 12 Stunden ist, als veraltet gilt, wird der Befehl sofort gelöscht.
- Wenn der Befehl nicht veraltet ist oder für eine Dauer, die kürzer als das maximale Timeout ist, als veraltet gilt, befindet sich der Befehl in einem Status. `pending deletion` Er wird nach Ablauf des maximalen Timeouts von 12 Stunden automatisch aus Ihrem Konto entfernt.

> **Note**
>
> Der Befehl kann gelöscht werden, auch wenn noch ausstehende Befehlsausführungen vorliegen. Der Befehl befindet sich im Status „Ausstehende Löschung“ und wird automatisch aus Ihrem Konto entfernt.

Löschen Sie eine Befehlsressource (Konsole)

Um einen Befehl von der Konsole zu löschen, rufen Sie den Command Hub der AWS IoT Konsole auf und führen Sie die folgenden Schritte aus.

1. Wählen Sie den Befehl aus, den Sie löschen möchten, und wählen Sie dann unter Aktionen die Option Löschen aus.
2. Bestätigen Sie, dass Sie den Befehl löschen möchten, und wählen Sie dann Löschen aus.

Der Befehl wird zum Löschen markiert und nach 12 Stunden dauerhaft aus Ihrem Konto entfernt.

Löscht eine Befehlsressource (CLI)

Verwenden Sie die API Operation auf der `DeleteCommand` HTTP Steuerungsebene oder den `delete-command` AWS CLI Befehl, um eine Befehlsressource zu löschen. Wenn die Löschaktion erfolgreich ist, wird ein Wert HTTP `statusCode` von 204 oder 202 angezeigt, und der Befehl wird nach Ablauf der maximalen Timeoutdauer von 12 Stunden automatisch aus Ihrem Konto gelöscht. Im Fall des Status 204 bedeutet dies, dass der Befehl gelöscht wurde.

Beispiel für eine IAM Richtlinie

Bevor Sie diesen API Vorgang verwenden, stellen Sie sicher, dass Ihre IAM Richtlinie Sie autorisiert, diese Aktion auf dem Gerät durchzuführen. Das folgende Beispiel zeigt eine IAM Richtlinie, die dem Benutzer die Erlaubnis erteilt, die `DeleteCommand` Aktion auszuführen.

Ersetzen Sie in diesem Beispiel:

- *`region`*mit Ihrem AWS-Region, wie zum Beispiel`ap-south-1`.
- *`account-id`*mit deiner AWS-Konto Nummer, wie*`123456789012`*.
- *`command-id`*mit Ihrer AWS IoT eindeutigen Befehlskennung, z. *`LockDoor`* B. Wenn Sie mehr als einen Befehl abrufen möchten, können Sie diese Befehle in der IAM Richtlinie im Abschnitt Ressource angeben.

```
{
    "Version": "2012-10-17",
    "Statement":
    {
        "Action": "iot:DeleteCommand",
        "Effect": "Allow",
        "Resource": "arn:aws:iot:<region>:<account_id>:command/command-id"
    }
}
```

Beispiel für einen Befehl löschen (AWS CLI)

Die folgenden Beispiele zeigen Ihnen, wie Sie einen Befehl mithilfe des `delete-command` AWS CLI Befehls löschen. Je nach Anwendung *<command-id>* ersetzen Sie ihn durch den Bezeichner für den Befehl, den Sie löschen möchten.

```
aws iot delete-command --command-id <command-id>
```

Wenn die API Anfrage erfolgreich ist, generiert der Befehl den Statuscode 202 oder 204. Sie können den verwenden `GetCommand`API, um zu überprüfen, ob der Befehl in Ihrem Konto nicht mehr vorhanden ist.

## Befehlsausführungen starten und überwachen

Nachdem Sie eine Befehlsressource erstellt haben, können Sie eine Befehlsausführung auf dem Zielgerät starten. Sobald das Gerät mit der Ausführung des Befehls beginnt, kann es damit beginnen, das Ergebnis der Befehlsausführung zu aktualisieren und Statusaktualisierungen und Ergebnisinformationen in den reservierten MQTT-Themen zu veröffentlichen. Sie können dann den Status der Befehlsausführung abrufen und den Status der Ausführungen in Ihrem Konto überwachen.

In diesem Abschnitt wird gezeigt, wie Sie Befehle sowohl mit der AWS IoT Konsole als auch mit dem starten und überwachen können. AWS CLI

Befehlsvorgänge starten und überwachen

- Starten Sie die Ausführung eines Befehls
- Aktualisieren Sie das Ergebnis einer Befehlsausführung
- Rufen Sie die Ausführung eines Befehls ab
- Befehlsaktualisierungen mit dem MQTT-Testclient anzeigen
- Listet die Befehlsausführungen in Ihrem auf AWS-Konto
- Löschen Sie die Ausführung eines Befehls

# Starten Sie die Ausführung eines Befehls

> **Important**
>
> Sie sind allein dafür verantwortlich, Befehle auf sichere und gesetzeskonforme Weise bereitzustellen.

Bevor Sie mit der Ausführung eines Befehls beginnen, müssen Sie Folgendes sicherstellen:

- Sie haben einen Befehl im AWS IoT Namespace erstellt und die Payload-Informationen bereitgestellt. Wenn Sie mit der Ausführung des Befehls beginnen, verarbeitet das Gerät die Anweisungen in der Payload und führt die angegebenen Aktionen aus. Hinweise zum Erstellen von Befehlen finden Sie unterErstellen Sie eine Befehlsressource.
- Ihr Gerät hat die für MQTT reservierten Themen für Befehle abonniert. Wenn Sie die Befehlsausführung starten, werden die Payload-Informationen unter dem folgenden reservierten Thema für MQTT-Anfragen veröffentlicht.

  In diesem Fall *<devices>* kann es sich entweder um IoT oder um MQTT-Clients handeln und *<DeviceID>* ist der Name der Sache oder die Client-ID. Die unterstützten *<PayloadFormat>* sind JSON und CBOR. Weitere Informationen zu Befehlen finden Sie unterThemen zu Befehlen.

  ```
  $aws/commands/<devices>/<DeviceID>/executions/+/request/<PayloadFormat>
  ```

  Wenn *<PayloadFormat>* es sich nicht um JSON und CBOR handelt, wird im Folgenden das Themenformat der Befehle beschrieben.

  ```
  $aws/commands/<devices>/<DeviceID>/executions/+/request
  ```

### Überlegungen zum Zielgerät

Wenn Sie den Befehl ausführen möchten, müssen Sie das Zielgerät angeben, das den Befehl empfangen und die angegebenen Anweisungen ausführen soll. Das Zielgerät kann entweder ein AWS IoT Ding oder die Client-ID sein, falls das Gerät nicht in der AWS IoT Registrierung registriert wurde. Nach Erhalt der Befehlspayload kann das Gerät mit der Ausführung des Befehls beginnen und die angegebenen Aktionen ausführen.

AWS IoT Sache

Das Zielgerät für den Befehl kann ein AWS IoT Ding sein, das Sie in der AWS IoT Ding-Registrierung registriert haben. Dinge AWS IoT , die darin enthalten sind, erleichtern die Suche und Verwaltung Ihrer Geräte.

Sie können Ihr Gerät als Ding registrieren, wenn Sie Ihr Gerät über die Connect-Geräteseite oder mithilfe der `CreateThing`API verbinden. AWS IoT Sie können ein vorhandenes Ding, für das Sie den Befehl ausführen möchten, auf der Thing Hub-Seite der AWS IoT Konsole oder mithilfe der `DescribeThing`API suchen. Informationen dazu, wie Sie Ihr Gerät als Objekt AWS IoT registrieren, finden Sie unter Dinge mit der Registrierung verwalten.

Client-ID

Wenn Ihr Gerät nicht als Ding bei registriert wurde AWS IoT, können Sie stattdessen die Client-ID verwenden.

Die Client-ID ist eine eindeutige Kennung, die Sie Ihrem Gerät oder Client zuweisen. Die Client-ID ist im MQTT-Protokoll definiert und kann alphanumerische Zeichen, Unterstriche oder Bindestriche enthalten. Sie muss für jedes Gerät, mit dem eine Verbindung hergestellt wird, eindeutig sein. AWS IoT

> **Note**
>
> - Wenn Ihr Gerät als Ding in der AWS IoT Registrierung registriert wurde, kann die Client-ID mit dem Namen des Dings identisch sein.
> - Wenn Ihre Befehlsausführung auf eine bestimmte MQTT-Client-ID abzielt, muss Ihr Gerät über dieselbe Client-ID eine Verbindung herstellen, um die Befehls-Payload aus dem Thema Client-ID-basierte Befehle zu AWS IoT erhalten.

Die Client-ID ist in der Regel die MQTT-Client-ID, mit der Ihre Geräte eine Verbindung herstellen können. AWS IoT Core Diese ID wird verwendet AWS IoT , um jedes spezifische Gerät zu identifizieren und Verbindungen und Abonnements zu verwalten.

Überlegungen zum Timeout bei der Befehlsausführung

Das Timeout gibt die Dauer in Sekunden an, innerhalb derer Ihr Gerät das Ergebnis der Befehlsausführung bereitstellen kann.

Nachdem Sie eine Befehlsausführung erstellt haben, wird ein Timer gestartet. Wenn das Gerät offline gegangen ist oder das Ausführungsergebnis nicht innerhalb der Timeoutdauer gemeldet werden konnte, wird die Befehlsausführung unterbrochen und der Ausführungsstatus wird als `TIMED_OUT` angezeigt.

Dieses Feld ist optional und wird standardmäßig auf 10 Sekunden gesetzt, wenn Sie keinen Wert angeben. Sie können das Timeout auch auf einen Höchstwert von 12 Stunden konfigurieren.

Timeout-Wert und **`TIMED_OUT`** Ausführungsstatus

Ein Timeout kann sowohl von der Cloud als auch vom Gerät gemeldet werden.

Nachdem der Befehl an das Gerät gesendet wurde, startet ein Timer. Wenn innerhalb der angegebenen Timeout-Dauer keine Antwort vom Gerät empfangen wurde, wie oben beschrieben. In diesem Fall legt die Cloud den Befehlsausführungsstatus `TIMED_OUT` mit dem Ursachencode auf fest`$NO_RESPONSE_FROM_DEVICE`.

Dies kann in einem der folgenden Fälle passieren.

- Das Gerät ging während der Ausführung des Befehls offline.
- Das Gerät konnte die Ausführung des Befehls nicht innerhalb der angegebenen Dauer abschließen.
- Das Gerät konnte die aktualisierten Statusinformationen nicht innerhalb der Timeoutdauer melden.

Wenn in diesem Fall der Ausführungsstatus von aus der Cloud gemeldet `TIMED_OUT` wird, erfolgt die Befehlsausführung nicht terminalgebunden. Ihr Gerät kann eine Antwort veröffentlichen, die den Status eines beliebigen Terminalstatus,`SUCCEEDED`, `FAILED` oder überschreibt. `REJECTED` Die Befehlsausführung erfolgt jetzt im Terminal und akzeptiert keine weiteren Updates.

Ihr Gerät kann auch einen von der Cloud initiierten `TIMED_OUT` Status aktualisieren, indem es meldet, dass bei der Ausführung des Befehls ein Timeout aufgetreten ist. In diesem Fall bleibt der Status der Befehlsausführung unverändert, das `statusReason` Objekt wird `TIMED_OUT` jedoch auf der Grundlage der vom Gerät gemeldeten Informationen aktualisiert. Die Befehlsausführung wird nun zum Terminal und es werden keine weiteren Aktualisierungen akzeptiert.

Verwenden persistenter MQTT-Sitzungen

Sie können persistente MQTT-Sitzungen für die Verwendung mit der AWS IoT Device Management Befehlsfunktion konfigurieren. Diese Funktion ist besonders nützlich, wenn Ihr Gerät offline geht und

Sie sicherstellen möchten, dass das Gerät den Befehl auch dann empfängt, wenn es vor Ablauf des Timeouts wieder online ist und die angegebenen Anweisungen ausführt.

Standardmäßig ist der Ablauf einer persistenten MQTT-Sitzung auf 60 Minuten festgelegt. Wenn Ihr Timeout für die Befehlsausführung auf einen Wert konfiguriert ist, der diese Dauer überschreitet, können Befehlsausführungen, die länger als 60 Minuten dauern, vom Message Broker abgelehnt werden und sie können fehlschlagen. Um Befehle auszuführen, die länger als 60 Minuten dauern, können Sie eine Verlängerung der Ablaufzeit für persistente Sitzungen beantragen.

> **Note**
>
> Um sicherzustellen, dass Sie die Funktion für persistente MQTT-Sitzungen korrekt verwenden, stellen Sie sicher, dass das Clean Start-Flag auf Null gesetzt ist. Weitere Informationen finden Sie unter Persistente MQTT-Sitzungen.

### Starten Sie eine Befehlsausführung (Konsole)

Um mit der Ausführung des Befehls von der Konsole aus zu beginnen, rufen Sie die Command Hub-Seite der AWS IoT Konsole auf und führen Sie die folgenden Schritte aus.

1. Um den von Ihnen erstellten Befehl auszuführen, wählen Sie Befehl ausführen.
2. Lesen Sie die Informationen über den Befehl, den Sie erstellt haben, die Payload-Datei und den Formattyp sowie die reservierten MQTT-Themen.
3. Geben Sie das Zielgerät an, für das Sie den Befehl ausführen möchten. Das Gerät kann als AWS IoT Ding angegeben werden, wenn es registriert wurde AWS IoT, oder mithilfe der Client-ID, falls Ihr Gerät noch nicht registriert wurde. Weitere Informationen finden Sie unter Überlegungen zum Zielgerät.
4. (Optional) Konfigurieren Sie einen Timeout-Wert für den Befehl, der die Dauer festlegt, für die der Befehl ausgeführt werden soll, bevor das Timeout eintritt. Wenn Ihr Befehl länger als 60 Minuten ausgeführt werden muss, müssen Sie möglicherweise die Ablaufzeit für persistente MQTT-Sitzungen erhöhen. Weitere Informationen finden Sie unter Überlegungen zum Timeout bei der Befehlsausführung.
5. Wählen Sie Befehl ausführen aus.

Starten Sie die Ausführung eines Befehls ()AWS CLI

Verwenden Sie den API-Vorgang für die `StartCommandExecution`HTTP-Datenebene, um die Ausführung eines Befehls zu starten. Die API-Anforderung und -Antwort korrelieren anhand der Befehlsausführungs-ID. Nachdem das Gerät die Ausführung des Befehls abgeschlossen hat, kann es den Status und das Ausführungsergebnis an die Cloud melden, indem es eine Nachricht im Antwortthema des Befehls veröffentlicht. Bei einem benutzerdefinierten Antwortcode können Anwendungscodes, deren Eigentümer Sie sind, die Antwortnachricht verarbeiten und das Ergebnis an sie senden AWS IoT.

Wenn Ihre Geräte das Thema für die Befehlsanfrage abonniert haben, veröffentlicht die `StartCommandExecution` API die Payload-Meldung zum Thema. Die Payload kann jedes Format Ihrer Wahl verwenden. Weitere Informationen finden Sie unter Payload des Befehls.

```
$aws/commands/<devices>/<DeviceID>/executions/+/request/<PayloadFormat>
```

Wenn das Payload-Format nicht JSON oder CBOR ist, wird im Folgenden das Format des Themas zur Befehlsanfrage angezeigt.

```
$aws/commands/<devices>/<DeviceID>/executions/+/request
```

Beispiel einer IAM-Richtlinie

Bevor Sie diesen API-Vorgang verwenden, stellen Sie sicher, dass Ihre IAM-Richtlinie Sie autorisiert, diese Aktion auf dem Gerät auszuführen. Das folgende Beispiel zeigt eine IAM-Richtlinie, die dem Benutzer die Erlaubnis erteilt, die Aktion auszuführen. `StartCommandExecution`

Ersetzen Sie in diesem Beispiel:

- *`region`*mit Ihrem AWS-Region, wie `ap-south-1` zum Beispiel.
- *`account-id`*mit deiner AWS-Konto Nummer, wie*`123456789012`*.
- *`command-id`*mit einer eindeutigen Kennung für Ihren AWS IoT Befehl, wie *`LockDoor`* z. Wenn Sie mehr als einen Befehl senden möchten, können Sie diese Befehle in der IAM-Richtlinie angeben.
- *`devices`*entweder `thing` oder `client` je nachdem, ob Ihre Geräte als AWS IoT Dinge registriert wurden oder als MQTT-Clients angegeben sind.
- *`device-id`*mit deinem AWS IoT `thing-name` oder`client-id`.

```
{
```

```
  "Effect": "Allow",
  "Action": [
      "iot:StartCommandExecution"
  ],
  "Resource": [
      "arn:aws:iot:region:account-id:command/command-id",
      "arn:aws:iot:region:account-id:devices/device-id"
  ]
}
```

Besorgen Sie sich einen kontospezifischen Endpunkt auf der Datenebene

Bevor Sie den API-Befehl ausführen, müssen Sie die kontospezifische Endpunkt-URL für den Endpunkt abrufen. `iot:Jobs` Wenn Sie z. B. den folgenden Befehl ausführen:

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

Es wird die kontospezifische Endpunkt-URL zurückgegeben, wie in der folgenden Beispielantwort gezeigt.

```
{
    "endpointAddress": "<account-specific-prefix>.jobs.iot.<region>.amazonaws.com"
}
```

Beispiel für eine Befehlsausführung starten ()AWS CLI

Das folgende Beispiel zeigt, wie die Ausführung eines Befehls mithilfe des `start-command-execution` AWS CLI Befehls gestartet wird.

Ersetzen Sie in diesem Beispiel:

- *<command-arn>*mit dem ARN für den Befehl, den Sie ausführen möchten. Sie können diese Informationen aus der Antwort des `create-command` CLI-Befehls abrufen. Wenn Sie beispielsweise den Befehl zum Ändern des Lenkradmodus ausführen, verwenden Sie`arn:aws:iot:`*region*`:`*account-id*`:command/`*SetComfortSteeringMode*.
- *<target-arn>*mit dem Thing-ARN für das Zielgerät, das ein IoT-Ding oder ein MQTT-Client sein kann, für den Sie den Befehl ausführen möchten. Wenn Sie beispielsweise den Befehl für das Zielgerät ausführen`myRegisteredThing`, verwenden Sie`arn:aws:iot:`*region*`:`*account-id*`:thing/`*myRegisteredThing*.

- *<endpoint-url>*mit dem kontospezifischen Endpunkt, den Sie abgerufen habenBesorgen Sie sich einen kontospezifischen Endpunkt auf der Datenebene, mit dem Präfix. `https://` Beispiel, `https://`*123456789012abcd*`.jobs.iot.`*ap-south-1*`.amazonaws.com`.
- (Optional) Sie können bei der Ausführung des API-Vorgangs auch einen zusätzlichen Parameter angeben. `executionTimeoutSeconds` `StartCommandExecution` Dieses optionale Feld gibt die Zeit in Sekunden an, innerhalb derer das Gerät die Ausführung des Befehls abschließen muss. Standardmäßig ist der Wert 10 Sekunden. Wenn der Status der Befehlsausführung lautet`CREATED`, wird ein Timer gestartet. Wenn das Ergebnis der Befehlsausführung nicht vor Ablauf des Timers eingeht, ändert sich der Status automatisch auf`TIMED_OUT`.

```
aws iot-jobs-data start-command-execution \
    --command-arn <command-arn>  \
    --target-arn <target-arn> \
    --endpoint <endpoint-url> \
    --execution-timeout-seconds 900
```

Wenn Sie diesen Befehl ausführen, wird eine Befehlsausführungs-ID zurückgegeben. Sie können diese ID verwenden, um den Status der Befehlsausführung, die Details und den Verlauf der Befehlsausführung abzufragen.

> **Note**
>
> Wenn der Befehl veraltet ist, schlägt die `StartCommandExecution` API-Anfrage mit einer Validierungsausnahme fehl. Um diesen Fehler zu beheben, stellen Sie zuerst den Befehl mithilfe der `UpdateCommand` API wieder her und führen Sie dann die `StartCommandExecution` Anfrage aus.

```
{
    "executionId": "07e4b780-7eca-4ffd-b772-b76358da5542"
}
```

## Aktualisieren Sie das Ergebnis einer Befehlsausführung

Verwenden Sie die `UpdateCommandExecution` MQTT-Datenebene-API-Operation, um den Status oder das Ergebnis einer Befehlsausführung zu aktualisieren.

> **Note**
>
> Bevor Sie diese API verwenden:
>
> - Ihr Gerät muss eine MQTT-Verbindung hergestellt und die Themen Commands Request und Response abonniert haben. Weitere Informationen finden Sie unter Arbeitsablauf für Befehle auf hoher Ebene.
> - Sie müssen diesen Befehl bereits mithilfe der `StartCommandExecution` API-Operation ausgeführt haben.

Beispiel einer IAM-Richtlinie

Bevor Sie diesen API-Vorgang verwenden, stellen Sie sicher, dass Ihre IAM-Richtlinie Ihr Gerät autorisiert, diese Aktionen auszuführen. Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die Ihr Gerät zur Ausführung der Aktion autorisiert. Weitere Beispiele für IAM-Richtlinien, die dem Benutzer die Erlaubnis geben, die `UpdateCommandExecution` Aktion auszuführen, finden Sie unter. Beispiele zu den Verbinden- und Veröffentlichen-Richtlinien

Ersetzen Sie in diesem Beispiel:

- *`Region`*mit Ihrem AWS-Region, wie `ap-south-1` zum Beispiel.
- *`AccountID`*mit deiner AWS-Konto Nummer, wie*`123456789012`*.
- *`ThingName`*mit dem Namen Ihres AWS IoT Dings, für das Sie die Befehlsausführung anstreben, z. *`myRegisteredThing`* B.
- *`commands-request-topic`*und *`commands-response-topic`* mit den Namen der Anfrage- und Antwortthemen Ihrer AWS IoT Befehle. Weitere Informationen finden Sie unter Arbeitsablauf für Befehle auf hoher Ebene.

Beispiel für eine IAM-Richtlinie für die MQTT-Client-ID

Der folgende Code zeigt ein Beispiel für eine Geräterichtlinie bei Verwendung der MQTT-Client-ID.

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

```
      "Resource": [
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/clients/
${iot:ClientId}/executions/*/response",
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/clients/
${iot:ClientId}/executions/*/response/json"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iot:Receive",
      "Resource": [
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/clients/
${iot:ClientId}/executions/*/request",
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/clients/
${iot:ClientId}/executions/*/response/accepted",
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/clients/
${iot:ClientId}/executions/*/response/rejected",
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/clients/
${iot:ClientId}/executions/*/request/json",
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/clients/
${iot:ClientId}/executions/*/response/accepted/json",
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/clients/
${iot:ClientId}/executions/*/response/rejected/json"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iot:Subscribe",
      "Resource": [
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/clients/
${iot:ClientId}/executions/+/request",
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/clients/
${iot:ClientId}/executions/+/response/accepted",
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/clients/
${iot:ClientId}/executions/+/response/rejected",
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/clients/
${iot:ClientId}/executions/+/request/json",
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/clients/
${iot:ClientId}/executions/+/response/accepted/json",
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/clients/
${iot:ClientId}/executions/+/response/rejected/json"
      ]
    },
    {
```

```
      "Effect": "Allow",
      "Action": "iot:Connect",
      "Resource": "arn:aws:iot:us-east-1:123456789012:client/${iot:ClientId}"
    }
  ]
}
```

Beispiel für eine IAM-Richtlinie für das IoT-Ding

Der folgende Code zeigt ein Beispiel für eine Geräterichtlinie bei der Verwendung AWS IoT eines Dings.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:Publish",
      "Resource": "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/*/response"
    },
    {
      "Effect": "Allow",
      "Action": "iot:Receive",
      "Resource": [
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/*/request",
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/*/response/accepted",
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/*/response/rejected",
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/*/request/json",
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/*/response/accepted/json",
        "arn:aws:iot:us-east-1:123456789012:topic/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/*/response/rejected/json"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iot:Subscribe",
      "Resource": [
```

```
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/+/request",
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/+/response/accepted",
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/+/response/rejected",
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/+/request/json",
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/+/response/accepted/json",
        "arn:aws:iot:us-east-1:123456789012:topicfilter/$aws/commands/things/
${iot:Connection.Thing.ThingName}/executions/+/response/rejected/json"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iot:Connect",
      "Resource": "arn:aws:iot:us-east-1:123456789012:client/${iot:ClientId}"
    }
  ]
}
```

Wie benutzt man die **`UpdateCommandExecution`** API

Nachdem die Befehlsausführung unter dem Thema der Anfrage eingegangen ist, verarbeitet das Gerät den Befehl. Anschließend verwendet es die `UpdateCommandExecution` API, um den Status und das Ergebnis der Befehlsausführung auf das folgende Antwortthema zu aktualisieren.

```
$aws/commands/<devices>/<DeviceID>/executions/<ExecutionId>/response/<PayloadFormat>
```

In diesem Beispiel *<DeviceID>* ist dies die eindeutige Kennung Ihres Zielgeräts und *<execution-id>* die Kennung der Befehlsausführung auf dem Zielgerät. Das *<PayloadFormat>* kann JSON oder CBOR sein.

> **Note**
>
> Wenn Sie Ihr Gerät nicht bei registriert haben AWS IoT, können Sie die Client-ID anstelle eines Dingnamens als Kennung verwenden.

```
$aws/commands/clients/<ClientID>/executions/<ExecutionId>/response/<PayloadFormat>
```

Das Gerät hat Aktualisierungen des Ausführungsstatus gemeldet

Ihre Geräte können die API verwenden, um alle der folgenden Statusaktualisierungen zur Befehlsausführung zu melden. Weitere Informationen zu diesen Status finden Sie unterStatus der Befehlsausführung.

- `IN_PROGRESS`: Wenn das Gerät mit der Ausführung des Befehls beginnt, kann es den Status auf `IN_PROGRESS` aktualisieren.
- `SUCCEEDED`: Wenn das Gerät den Befehl erfolgreich verarbeitet und die Ausführung abgeschlossen hat, kann das Gerät eine Nachricht im Antwortthema als veröffentlichen`SUCCEEDED`.
- `FAILED`: Wenn das Gerät den Befehl nicht ausführen konnte, kann es eine Nachricht im Antwortthema als veröffentlichen`FAILED`.
- `REJECTED`: Wenn das Gerät den Befehl nicht akzeptiert hat, kann es eine Nachricht im Antwortthema als veröffentlichen`REJECTED`.
- `TIMED_OUT`: Der Status der Befehlsausführung kann aus einem der folgenden Gründe auf geändert werden. `TIMED_OUT`
  - Das Ergebnis der Befehlsausführung wurde nicht empfangen. Dies kann passieren, weil die Ausführung nicht innerhalb der angegebenen Dauer abgeschlossen wurde oder wenn das Gerät die Statusinformationen nicht im Antwortthema veröffentlicht hat.
  - Das Gerät meldet, dass beim Versuch, den Befehl auszuführen, ein Timeout aufgetreten ist.

Weitere Informationen zum `TIMED_OUT` Status finden Sie unterTimeout-Wert und `TIMED_OUT` Ausführungsstatus.

Überlegungen bei der Verwendung der **`UpdateCommandExecution`** API

Im Folgenden sind einige wichtige Überlegungen zur Verwendung der `UpdateCommandExecution` API aufgeführt.

- Ihre Geräte können ein optionales `statusReason` Objekt verwenden, das verwendet werden kann, um zusätzliche Informationen zur Ausführung bereitzustellen. Wenn Ihre Geräte dieses Objekt bereitstellen, ist das `reasonCode` Feld des Objekts erforderlich, aber das `reasonDescription` Feld ist optional.
- Wenn Ihre Geräte das `statusReason` Objekt verwenden, `reasonCode` müssen sie das Muster `[A-Z0-9_-]+` verwenden und es darf nicht länger als 64 Zeichen sein. Wenn Sie das

angeben`reasonDescription`, stellen Sie sicher, dass es nicht länger als 1.024 Zeichen ist. Es können alle Zeichen außer Steuerzeichen, wie z. B. neue Zeilen, verwendet werden.

- Ihre Geräte können ein optionales `result` Objekt verwenden, um Informationen über das Ergebnis der Befehlsausführung bereitzustellen, z. B. den Rückgabewert eines Remote-Funktionsaufrufs. Wenn Sie das angeben`result`, muss mindestens ein Eintrag erforderlich sein.
- In dem `result` Feld geben Sie die Einträge als Schlüssel-Wert-Paare an. Für jeden Eintrag müssen Sie die Datentypinformationen als Zeichenfolge, boolescher Wert oder Binärwert angeben. Ein Zeichenkettendatentyp muss den Schlüssel verwendens, ein boolescher Datentyp verwendet den Schlüssel b und ein binärer Datentyp muss den Schlüssel verwenden. `bin` Sie müssen sicherstellen, dass diese Datentypen in Kleinbuchstaben angegeben werden.
- Wenn Sie beim Ausführen der `UpdateCommandExecution` API auf einen Fehler stoßen, können Sie den Fehler in der `AWSIoTLogsV2` Protokollgruppe in Amazon anzeigen CloudWatch. Informationen zum Aktivieren der Protokollierung und zum Anzeigen der Protokolle finden Sie unterKonfigurieren Sie die AWS IoT Protokollierung.

### **`UpdateCommandExecution`**API-Beispiel

Der folgende Code zeigt ein Beispiel dafür, wie Ihr Gerät die `UpdateCommandExecution` API verwenden kann, um den Ausführungsstatus zu melden, das `statusReason` Feld, um zusätzliche Informationen zum Status bereitzustellen, und das Ergebnisfeld, um Informationen über das Ergebnis der Ausführung bereitzustellen, wie in diesem Fall den Prozentsatz der Autobatterie.

```
{
  "status": "IN_PROGRESS",
  "statusReason": {
    "reasonCode": "200",
    "reasonDescription": "Execution_in_progress"
  },
  "result": {
        "car_battery": {
            "s": "car battery at 50 percent"
        }
    }
}
```

# Rufen Sie die Ausführung eines Befehls ab

Nachdem Sie einen Befehl ausgeführt haben, können Sie Informationen über die Befehlsausführung von der AWS IoT Konsole abrufen und den AWS CLI Sie können die folgenden Informationen abrufen.

> **Note**
>
> Um den aktuellen Status der Befehlsausführung abzurufen, muss Ihr Gerät die Statusinformationen mithilfe der `UpdateCommandExecution` MQTT-API im Antwortthema veröffentlichen, wie unten beschrieben. Bis das Gerät zu diesem Thema veröffentlicht, meldet die `GetCommandExecution` API den Status als `CREATED` oder`TIMED_OUT`.

Für jede Befehlsausführung, die Sie erstellen, gilt Folgendes:

- Eine Ausführungs-ID, bei der es sich um eine eindeutige Kennung der Befehlsausführung handelt.
- Der Status der Befehlsausführung. Wenn Sie den Befehl auf dem Zielgerät ausführen, wechselt die Befehlsausführung in einen `CREATED` Status. Es kann dann in einen anderen Status der Befehlsausführung übergehen, wie unten beschrieben.
- Das Ergebnis der Befehlsausführung.
- Die eindeutige Befehls-ID und das Zielgerät, für das Ausführungen erstellt wurden.
- Das Startdatum, das die Uhrzeit angibt, zu der die Befehlsausführung erstellt wurde.

Rufen Sie eine Befehlsausführung ab (Konsole)

Sie können eine Befehlsausführung mit einer der folgenden Methoden von der Konsole abrufen.

- Von der Command-Hub-Seite

  Gehen Sie zur Command Hub-Seite der AWS IoT Konsole und führen Sie diese Schritte aus.

  1. Wählen Sie den Befehl aus, für den Sie eine Ausführung auf dem Zielgerät erstellt haben.
  2. Auf der Seite mit den Befehlsdetails auf der Registerkarte Befehlsverlauf sehen Sie die Ausführungen, die Sie erstellt haben. Wählen Sie die Ausführung aus, für die Sie Informationen abrufen möchten.

3. Wenn Ihre Geräte die `UpdateCommandExecution` API zur Bereitstellung der Ergebnisinformationen verwendet haben, finden Sie diese Informationen dann auf der Registerkarte Ergebnisse auf dieser Seite.

- Auf der Thing-Hub-Seite

  Wenn Sie bei der Ausführung des Befehls ein AWS IoT Ding als Zielgerät ausgewählt haben, können Sie die Ausführungsdetails auf der Thing-Hub-Seite einsehen.

  1. Gehen Sie in der AWS IoT Konsole zur Thing Hub-Seite und wählen Sie das Ding aus, für das Sie die Befehlsausführung erstellt haben.
  2. Auf der Seite mit den Ding-Details im Befehlsverlauf sehen Sie die Ausführungen, die Sie erstellt haben. Wählen Sie die Ausführung aus, für die Sie Informationen abrufen möchten.
  3. Wenn Ihre Geräte die `UpdateCommandExecution` API zur Bereitstellung der Ergebnisinformationen verwendet haben, finden Sie diese Informationen dann auf der Registerkarte Ergebnisse auf dieser Seite.

Rufen Sie eine Befehlsausführung ab (CLI)

Verwenden Sie den HTTP-API-Vorgang der `GetCommandExecution` AWS IoT Core Steuerungsebene, um Informationen über die Ausführung eines Befehls abzurufen. Sie müssen diesen Befehl bereits mithilfe der `StartCommandExecution` API-Operation ausgeführt haben.

Beispiel einer IAM-Richtlinie

Bevor Sie diesen API-Vorgang verwenden, stellen Sie sicher, dass Ihre IAM-Richtlinie Sie autorisiert, diese Aktion auf dem Gerät auszuführen. Das folgende Beispiel zeigt eine IAM-Richtlinie, die dem Benutzer die Erlaubnis erteilt, die Aktion auszuführen. `GetCommandExecution`

Ersetzen Sie in diesem Beispiel:

- *`region`*mit Ihrem AWS-Region, wie `ap-south-1` zum Beispiel.
- *`account-id`*mit deiner AWS-Konto Nummer, wie*`123456789012`*.
- *`command-id`*mit Ihrer eindeutigen AWS IoT Befehlskennung, z. *`LockDoor`* B.
- *`devices`*entweder `thing` oder `client` je nachdem, ob Ihre Geräte als AWS IoT Dinge registriert wurden oder als MQTT-Clients spezifiziert sind.
- *`device-id`*mit deinem AWS IoT `thing-name` oder`client-id`.

```
{
  "Effect": "Allow",
  "Action": [
      "iot:GetCommandExecution"
  ],
  "Resource": [
      "arn:aws:iot:region:account-id:command/command-id",
      "arn:aws:iot:region:account-id:devices/device-id"
  ]
}
```

Rufen Sie ein Beispiel für die Befehlsausführung ab

Das folgende Beispiel zeigt Ihnen, wie Sie Informationen über einen Befehl abrufen, der mit dem `start-command-execution` AWS CLI Befehl ausgeführt wurde. Das folgende Beispiel zeigt, wie Sie Informationen über einen Befehl abrufen können, der ausgeführt wurde, um den Lenkradmodus auszuschalten.

Ersetzen Sie in diesem Beispiel:

- *<execution-id>*mit der Kennung für die Befehlsausführung, für die Sie Informationen abrufen möchten.
- *<target-arn>*mit der Amazon-Ressourcennummer (ARN) des Geräts, für das Sie die Ausführung anstreben. Sie können diese Informationen aus der Antwort des `start-command-execution` CLI-Befehls abrufen.
- Wenn Ihre Geräte die `UpdateCommandExection` API zur Bereitstellung des Ausführungsergebnisses verwendet haben, können Sie optional angeben, ob das Ergebnis der Befehlsausführung in die Antwort der `GetCommandExecution` API über die `GetCommandExecution` API aufgenommen werden soll.

```
aws iot get-command-execution
    --execution-id <execution-id> \
    --target-arn <target-arn> \
    --include-result
```

Die Ausführung dieses Befehls generiert eine Antwort, die Informationen über den ARN der Befehlsausführung, den Ausführungsstatus und den Zeitpunkt des Beginns und des Abschlusses der Ausführung enthält. Es stellt auch ein `statusReason` Objekt bereit, das zusätzliche Informationen

über den Status enthält. Weitere Informationen zu den verschiedenen Status und den Gründen für den Status finden Sie unterStatus der Befehlsausführung.

Der folgende Code zeigt eine Beispielantwort aus der API-Anfrage.

> **Note**
>
> Das `completedAt` Feld in der Ausführungsantwort entspricht dem Zeitpunkt, zu dem das Gerät einen Terminalstatus an die Cloud meldet. Im Fall des `TIMED_OUT` Status wird dieses Feld nur gesetzt, wenn das Gerät einen Timeout meldet. Wenn der `TIMED_OUT` Status von der Cloud festgelegt wird, wird der `TIMED_OUT` Status nicht aktualisiert. Weitere Informationen zum Timeout-Verhalten finden Sie unterÜberlegungen zum Timeout bei der Befehlsausführung.

```
{
    "executionId": "07e4b780-7eca-4ffd-b772-b76358da5542",
    "commandArn": "arn:aws:iot:ap-south-1:123456789012:command/LockDoor",
    "targetArn": "arn:aws:iot:ap-south-1:123456789012:thing/myRegisteredThing",
    "status": "SUCCEEDED",
    "statusReason": {
        "reasonCode": "DEVICE_SUCCESSFULLY_EXECUTED",
        "reasonDescription": "SUCCESS"
    },
    "result": {
        "sn": { "s": "ABC-001" },
        "digital": { "b": true }
    },
    "createdAt": "2024-03-23T00:50:10.095000-07:00",
    "completedAt": "2024-03-23T00:50:10.095000-07:00"
}
```

## Befehlsaktualisierungen mit dem MQTT-Testclient anzeigen

Sie können den MQTT-Testclient verwenden, um sich den Nachrichtenaustausch über MQTT anzusehen, wenn Sie die Befehlsfunktion verwenden. Nachdem Ihr Gerät eine MQTT-Verbindung mit hergestellt hat AWS IoT, können Sie einen Befehl erstellen, die Nutzlast angeben und ihn dann auf dem Gerät ausführen. Wenn Sie den Befehl ausführen und Ihr Gerät das MQTT-Request-Thema für Befehle abonniert hat, wird die zu diesem Thema veröffentlichte Payload-Meldung angezeigt.

Das Gerät empfängt dann die Nutzlastanweisungen und führt die angegebenen Operationen auf dem IoT-Gerät aus. Anschließend verwendet es die `UpdateCommandExecution` API, um das Ergebnis der Befehlsausführung und die Statusinformationen in den MQTT-Antwortthemen zu veröffentlichen, die für Befehle reserviert sind. AWS IoT Device Management hört sich Updates zu den Antwortthemen an, speichert die aktualisierten Informationen und veröffentlicht Protokolle an AWS CloudTrail und Amazon. CloudWatch Sie können dann die neuesten Informationen zur Befehlsausführung von der Konsole oder mithilfe der API abrufen. `GetCommandExecution`

Die folgenden Schritte zeigen, wie Sie den MQTT-Testclient verwenden, um Nachrichten zu beobachten.

1. Öffnen Sie den MQTT-Testclient in der AWS IoT Konsole.
2. Geben Sie auf der Registerkarte Abonnieren das folgende Thema ein und wählen Sie dann Abonnieren aus. Dabei *<thingId>* steht der Name des Geräts, mit AWS IoT dem Sie sich registriert haben.

   > **Note**
   >
   > Sie finden den Dingnamen für Ihr Gerät auf der Thing Hub-Seite der AWS IoT Konsole. Wenn Sie Ihr Gerät nicht als Ding registriert haben, können Sie das Gerät registrieren, wenn Sie über die Seite Connect-Gerät eine Verbindung herstellen. AWS IoT

   ```
   $aws/commands/things/<thingId>/executions/+/request
   ```

3. (Optional) Auf der Registerkarte Abonnieren können Sie auch die folgenden Themen eingeben und Abonnieren auswählen.

   ```
   $aws/commands/things/+/executions/+/response/accepted/json
   $aws/commands/things/+/executions/+/response/rejected/json
   ```

4. Wenn Sie die Ausführung eines Befehls starten, wird die Payload der Nachricht an das Gerät gesendet, wobei das Anforderungsthema verwendet wird, das das Gerät abonniert hat. `$aws/commands/things/<thingId>/executions/+/request` Im MQTT-Testclient sollten Sie die Befehls-Payload sehen, die die Anweisungen für das Gerät zur Verarbeitung des Befehls enthält.

5. Nachdem das Gerät mit der Ausführung des Befehls begonnen hat, kann es Statusaktualisierungen zum folgenden MQTT-Antwortthema veröffentlichen, das für Befehle reserviert ist.

```
$aws/commands/<devices>/<device-id>/executions/<executionId>/response/json
```

Stellen Sie sich zum Beispiel einen Befehl vor, den Sie ausgeführt haben, um die Klimaanlage Ihres Autos einzuschalten und die Temperatur auf einen gewünschten Wert zu senken. Die folgende JSON-Datei zeigt eine Beispielnachricht, die das Fahrzeug im Antwortthema veröffentlicht hat und aus der hervorgeht, dass der Befehl nicht ausgeführt werden konnte.

```
{
  "deviceId": "My_Car",
  "executionId": "07e4b780-7eca-4ffd-b772-b76358da5542",
  "status": "FAILED",
  "statusReason": {
    "reasonCode": "CAR_LOW_ON_BATTERY",
    "reasonDescription": "Car battery is lower than 5 percent"
  }
}
```

In diesem Fall können Sie die Batterie Ihres Autos aufladen und den Befehl dann erneut ausführen.

## Listet die Befehlsausführungen in Ihrem auf AWS-Konto

Nachdem Sie einen Befehl ausgeführt haben, können Sie Informationen über die Befehlsausführung von der AWS IoT Konsole abrufen und die AWS CLI. Sie können die folgenden Informationen abrufen.

- Eine Ausführungs-ID, bei der es sich um eine eindeutige Kennung der Befehlsausführung handelt.
- Der Status der Befehlsausführung. Wenn Sie den Befehl auf dem Zielgerät ausführen, wechselt die Befehlsausführung in einen `CREATED` Status. Es kann dann in einen anderen Status der Befehlsausführung übergehen, wie unten beschrieben.
- Die eindeutige Befehls-ID und das Zielgerät, für das Ausführungen erstellt wurden.
- Das Startdatum, das die Uhrzeit angibt, zu der die Befehlsausführung erstellt wurde.

Listet die Befehlsausführungen in Ihrem Konto (Konsole) auf

Sie können alle Befehlsausführungen von der Konsole aus mit einer der folgenden Methoden anzeigen.

- Auf der Command-Hub-Seite

  Gehen Sie zur Command Hub-Seite der AWS IoT Konsole und führen Sie diese Schritte aus.

  1. Wählen Sie den Befehl aus, für den Sie eine Ausführung auf dem Zielgerät erstellt haben.
  2. Gehen Sie auf der Seite mit den Befehlsdetails zur Registerkarte Befehlsverlauf. Dort wird eine Liste der von Ihnen erstellten Ausführungen angezeigt.
- Von der Thing-Hub-Seite

  Wenn Sie bei der Ausführung des Befehls ein AWS IoT Ding als Zielgerät ausgewählt und mehrere Befehlsausführungen für ein einzelnes Gerät erstellt haben, können Sie die Ausführungen für das Gerät auf der Thing-Hub-Seite anzeigen.

  1. Gehen Sie in der AWS IoT Konsole zur Thing Hub-Seite und wählen Sie das Ding aus, für das Sie die Ausführungen erstellt haben.
  2. Auf der Seite mit den Ding-Details sehen Sie im Befehlsverlauf eine Liste der Ausführungen, die Sie für das Gerät erstellt haben.

Befehlsausführungen in Ihrem Konto auflisten (CLI)

Verwenden Sie den HTTP-API-Vorgang der `ListCommandExecutions` AWS IoT Core Steuerungsebene, um alle Befehlsausführungen in Ihrem Konto aufzulisten.

Beispiel einer IAM-Richtlinie

Bevor Sie diesen API-Vorgang verwenden, stellen Sie sicher, dass Ihre IAM-Richtlinie Sie autorisiert, diese Aktion auf dem Gerät auszuführen. Das folgende Beispiel zeigt eine IAM-Richtlinie, die dem Benutzer die Erlaubnis erteilt, die Aktion auszuführen. `ListCommandExecutions`

Ersetzen Sie in diesem Beispiel:

- *`region`*mit Ihrem AWS-Region, wie `ap-south-1` zum Beispiel.
- *`account-id`*mit deiner AWS-Konto Nummer, wie*`123456789012`*.
- *`command-id`*mit Ihrer eindeutigen AWS IoT Befehlskennung, z. *`LockDoor`* B.

```
{
  "Effect": "Allow",
  "Action": "iot:ListCommandExecutions",
  "Resource": *
}
```

Beispiel für Befehlsausführungen auflisten

Das folgende Beispiel zeigt Ihnen, wie Sie Befehlsausführungen in Ihrem auflisten. AWS-Konto

Bei der Ausführung des Befehls müssen Sie angeben, ob die Liste so gefiltert werden soll, dass nur Befehlsausführungen angezeigt werden, die mit dem für ein bestimmtes Gerät erstellt wurden`targetArn`, oder Ausführungen für einen bestimmten Befehl, der mit dem angegeben wurde. `commandArn`

Ersetzen Sie in diesem Beispiel:

- *<target-arn>*mit der Amazon-Ressourcennummer (ARN) des Geräts, für das Sie die Ausführung planen, z. `arn:aws:iot:`*us-east-1*`:`*123456789012*`:thing/`*b8e4157c98f332cffb37627f* B.
- *<target-arn>*mit der Amazon-Ressourcennummer (ARN) des Geräts, für das Sie die Ausführung planen, z. `arn:aws:iot:`*us-east-1*`:`*123456789012*`:thing/`*b8e4157c98f332cffb37627f* B.
- *<after>*mit der Zeit, nach der Sie die Ausführungen auflisten möchten, die erstellt wurden, zum Beispiel. `2024-11-01T03:00`

```
aws iot list-command-executions \
--target-arn <target-arn> \
--started-time-filter '{after=<after>}' \
--sort-order "ASCENDING"
```

Wenn Sie diesen Befehl ausführen, wird eine Antwort generiert, die eine Liste der von Ihnen erstellten Befehlsausführungen sowie die Uhrzeit enthält, zu der die Ausführung begonnen und abgeschlossen wurde. Es enthält auch Statusinformationen und das `statusReason` Objekt, das zusätzliche Informationen über den Status enthält.

```
{
    "commandExecutions": [
        {
```

```
            "commandArn": "arn:aws:iot:us-east-1:123456789012:command/TestMe002",
            "executionId": "b2b654ca-1a71-427f-9669-e74ae9d92d24",
            "targetArn": "arn:aws:iot:us-east-1:123456789012:thing/
b8e4157c98f332cffb37627f",
            "status": "TIMED_OUT",
            "createdAt": "2024-11-24T14:39:25.791000-08:00",
            "startedAt": "2024-11-24T14:39:25.791000-08:00"
        },
        {
            "commandArn": "arn:aws:iot:us-east-1:123456789012:command/TestMe002",
            "executionId": "34bf015f-ef0f-4453-acd0-9cca2d42a48f",
            "targetArn": "arn:aws:iot:us-east-1:123456789012:thing/
b8e4157c98f332cffb37627f",
            "status": "IN_PROGRESS",
            "createdAt": "2024-11-24T14:05:36.021000-08:00",
            "startedAt": "2024-11-24T14:05:36.021000-08:00"
        }
    ]
}
```


Weitere Informationen zu den verschiedenen Status und den Gründen für den Status finden Sie unterStatus der Befehlsausführung.

## Löschen Sie die Ausführung eines Befehls

Wenn Sie eine Befehlsausführung nicht mehr verwenden möchten, können Sie sie dauerhaft aus Ihrem Konto entfernen.

> **Note**
>
> - Eine Befehlsausführung kann nur gelöscht werden, wenn sie einen Terminalstatus wie `SUCCEEDED`FAILED, oder erreicht hat`REJECTED`.
> - Dieser Vorgang kann nur mit der AWS IoT Core API oder der ausgeführt werden AWS CLI. Er ist nicht über die Konsole verfügbar.

### Beispiel einer IAM-Richtlinie

Bevor Sie diesen API-Vorgang verwenden, stellen Sie sicher, dass Ihre IAM-Richtlinie Ihr Gerät autorisiert, diese Aktionen auszuführen. Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die Ihr Gerät zur Ausführung der Aktion autorisiert.

Ersetzen Sie in diesem Beispiel:

- *Region*mit Ihrem AWS-Region, wie `ap-south-1` zum Beispiel.
- *AccountID*mit deiner AWS-Konto Nummer, wie*123456789012*.
- *CommandID*mit der Kennung des Befehls, für den Sie die Ausführung löschen möchten.
- *devices*entweder `thing` oder `client` je nachdem, ob Ihre Geräte als AWS IoT Dinge registriert wurden oder als MQTT-Clients spezifiziert sind.
- *device-id*mit deinem AWS IoT `thing-name` oder`client-id`.

```
{
  "Effect": "Allow",
  "Action": [
      "iot:DeleteCommandExecution"
  ],
  "Resource": [
      "arn:aws:iot:region:account-id:command/command-id",
      "arn:aws:iot:region:account-id:devices/device-id"
  ]
}
```

Löschen Sie ein Beispiel für die Befehlsausführung

Das folgende Beispiel zeigt Ihnen, wie Sie einen Befehl mithilfe des `delete-command` AWS CLI Befehls löschen. Ersetzen Sie je nach Anwendung *<execution-id>* durch die Kennung für die Befehlsausführung, die Sie löschen, und dann *<target-arn>* durch den ARN Ihres Zielgeräts.

```
aws iot delete-command-execution \
--execution-id <execution-id> \
--target-arn <target-arn>
```

Wenn die API-Anfrage erfolgreich ist, generiert die Befehlsausführung den Statuscode 200. Sie können die `GetCommandExecution` API verwenden, um zu überprüfen, ob die Befehlsausführung in Ihrem Konto nicht mehr vorhanden ist.

## Eine Befehlsressource als veraltet kennzeichnen

Sie können einen Befehl als veraltet kennzeichnen, um anzugeben, dass er veraltet ist und nicht verwendet werden sollte. Sie könnten beispielsweise einen Befehl verwerfen, der nicht mehr aktiv

verwaltet wird, oder Sie möchten einen neueren Befehl mit derselben Befehls-ID erstellen, der jedoch andere Payload-Informationen verwendet.

## Wichtige Überlegungen

Im Folgenden sind einige wichtige Überlegungen zur Ablehnung eines Befehls aufgeführt:

- Wenn Sie einen Befehl als veraltet markieren, wird er nicht gelöscht. Sie können den Befehl immer noch mit seiner Befehls-ID abrufen und wiederherstellen, wenn Sie den Befehl wiederverwenden möchten.
- Wenn Sie versuchen, auf Ihrem Zielgerät eine neue Befehlsausführung für einen veralteten Befehl zu starten, wird ein Fehler generiert, der Sie daran hindert, Befehle zu verwenden out-of-date.
- Um einen veralteten Befehl auf Ihrem Zielgerät auszuführen, müssen Sie ihn zunächst wiederherstellen. Nach der Wiederherstellung ist der Befehl verfügbar und kann als regulärer Befehl verwendet werden, und Sie können Befehlsausführungen auf dem Zielgerät ausführen.
- Wenn Sie einen Befehl verwerfen, während die Befehlsausführungen ausgeführt werden, werden die Ausführungen auf dem Zielgerät weiter ausgeführt, bis sie abgeschlossen sind. Sie können auch den Status der Befehlsausführungen abrufen.

## Eine Befehlsressource (Konsole) als veraltet kennzeichnen

Um einen Befehl aus der Konsole als veraltet zu kennzeichnen, gehen Sie zum Command Hub der AWS IoT Konsole und führen Sie die folgenden Schritte aus.

1. Wählen Sie den Befehl aus, den Sie verwerfen möchten, und wählen Sie dann unter Aktionen die Option Veraltet aus.
2. Bestätigen Sie, dass Sie den Befehl als veraltet markieren möchten, und wählen Sie dann Veraltet aus.

## Eine Befehlsressource (CLI) verwerfen

Sie können einen Befehl mit der CLI als veraltet markieren. `update-command` Sie müssen einen Befehl zuerst als veraltet markieren, bevor er gelöscht werden kann. Wenn ein Befehl als veraltet gilt und Sie ihn verwenden möchten, z. B. um eine Befehlsausführung an das Zielgerät zu senden, müssen Sie ihn rückgängig machen.

```
aws iot update-command \
```

```
    --command-id <command-id> \
    --deprecated
```

Wenn Sie beispielsweise den *ACSwitch* Befehl, den Sie im obigen Beispiel aktualisiert haben, als veraltet eingestuft haben, zeigt der folgende Code eine Beispielausgabe der Ausführung des Befehls.

```
{
    "commandId": "turnOffAc",
    "deprecated": true,
    "lastUpdatedAt": "2024-05-09T23:16:51.370000-07:00"
}
```

## Überprüfen Sie den Zeitpunkt und den Status der Deprecation

Sie können den `GetCommand` API-Vorgang verwenden, um festzustellen, ob ein Befehl veraltet ist und wann er zuletzt als veraltet eingestuft wurde.

```
aws iot get-command --command-id <turnOffAC>
```

Wenn Sie diesen Befehl ausführen, wird eine Antwort generiert, die Informationen über den Befehl enthält. Anhand der zuletzt aktualisierten Informationen können Sie Informationen darüber abrufen, wann er erstellt wurde und wann er veraltet war. Anhand dieser Informationen können Sie die Gültigkeitsdauer eines Befehls bestimmen und feststellen, ob Sie den Befehl löschen oder wiederverwenden möchten. Im obigen *turnOffAc* Beispiel zeigt der folgende Code beispielsweise eine Beispielantwort.

```
{
    "commandId": "turnOffAC",
    "commandArn": "arn:aws:iot:ap-south-1:123456789012:command/turnOffAC",
    "namespace": "AWS-IoT",
    "payload": {
        "content": "testPayload.json",
        "contentType": "application/json"
    },
    "createdAt": "2024-03-23T00:50:10.095000-07:00",
    "lastUpdatedAt": "2024-05-09T23:16:51.370000-07:00",
    "deprecated": false
}
```

# Stellen Sie eine Befehlsressource wieder her

Um den `ACSwitch` Befehl zu verwenden oder ihn an Ihr Gerät zu senden, müssen Sie ihn wiederherstellen.

Um einen Befehl von der Konsole wiederherzustellen, rufen Sie den Command Hub der AWS IoT Konsole auf, wählen Sie den Befehl aus, den Sie wiederherstellen möchten, und wählen Sie dann unter Aktionen die Option Wiederherstellen aus.

Verwenden Sie den AWS IoT Core API-Vorgang oder die `update-command` CLI AWS CLI, um einen Befehl mithilfe der `UpdateCommand` API oder der wiederherzustellen. Der folgende Code zeigt ein Beispiel für eine Anfrage und eine Antwort.

```
aws iot update-command \
    --command-id <command-id>
    --no-deprecated
```

Der folgende Code zeigt eine Beispielausgabe.

```
{
    "commandId": "ACSwitch",
    "deprecated": false,
    "lastUpdatedAt": "2024-05-09T23:17:21.954000-07:00"
}
```

# AWS IoT sicheres Tunneling

Wenn Geräte hinter eingeschränkten Firewalls an Remote-Standorten bereitgestellt werden, brauchen Sie für die Fehlerbehebung, Konfigurationsupdates und andere betriebliche Aufgaben eine Zugriffsmöglichkeit auf diese Geräte. Verwenden Sie sicheres Tunneling, um eine bidirektionale Kommunikation mit Remotegeräten über eine sichere Verbindung herzustellen, die von verwaltet wird. AWS IoT Für Secure Tunneling sind keine Aktualisierungen der vorhandenen eingehenden Firewallregel erforderlich, sodass Sie die gleiche Sicherheitsstufe beibehalten können, die von Firewallregeln an einem Remote-Standort bereitgestellt wird.

Beispiel: Ein Sensorgerät, das sich in einer Fabrik befindet, die ein paar hundert Kilometer entfernt ist, hat Probleme bei der Messung der Temperatur in der Fabrik. Sie können Secure Tunneling verwenden, um eine Sitzung mit diesem Sensorgerät zu öffnen und schnell zu starten. Nachdem Sie das Problem identifiziert haben (z. B. eine fehlerhafte Konfigurationsdatei), können Sie die Datei zurücksetzen und das Sensorgerät über dieselbe Sitzung neu starten. Im Vergleich zu herkömmlichen Fehlerbehebungen (z. B. beim Senden eines Technikers zur Fabrik, um das Sensorgerät zu untersuchen) senkt Secure Tunneling die Reaktionszeit, die Wiederherstellungszeit und die Betriebskosten.

## Was ist Secure Tunneling?

Verwenden Sie Secure Tunneling, um auf Geräte zuzugreifen, die hinter portbeschränkten Firewalls an entfernten Standorten installiert sind. Sie können von Ihrem Laptop oder Desktop-Computer als Quellgerät aus eine Verbindung zum Zielgerät herstellen, indem Sie den AWS Cloud verwenden. Quelle und Ziel kommunizieren über einen lokalen Open-Source-Proxy, der auf jedem Gerät ausgeführt wird. Der lokale Proxy kommuniziert mit dem über einen offenen Port, der AWS Cloud von der Firewall zugelassen wird, normalerweise 443. Daten, die durch den Tunnel übertragen werden, werden mittels Transported Layer Security (TLS) verschlüsselt.

Themen


- Secure Tunneling-Konzepte
- Wie funktioniert Secure Tunneling
- Sicherer Tunnellebenszyklus

# Secure Tunneling-Konzepte

Die folgenden Begriffe werden beim Secure Tunneling verwendet, wenn die Kommunikation mit Remote-Geräten hergestellt wird. Weitere Informationen zum Einrichten eines sicheren Tunnels finden Sie unter Wie funktioniert Secure Tunneling.

Client-Zugriffstoken (CAT)

Ein Token-Paar, das durch Secure Tunneling generiert wird, wenn ein neuer Tunnel erstellt wird. Das CAT wird von den Quell- und Zielgeräten verwendet, um eine Verbindung mit dem Secure-Tunneling-Service herzustellen. Das CAT kann nur einmal verwendet werden, um eine Verbindung zum Tunnel herzustellen. Um die Verbindung zum Tunnel wiederherzustellen, rotieren Sie die Client-Zugriffstoken mithilfe der RotateTunnelAccessTokenAPI-Operation oder des rotate-tunnel-access-tokenCLI-Befehls.

Client-Token

Ein vom Client generierter eindeutiger Wert, den AWS IoT Secure Tunneling für alle nachfolgenden Wiederholungsverbindungen zu demselben Tunnel verwenden kann. Dies ist ein optionales Feld. Wenn das Client-Token nicht bereitgestellt wird, kann das Client-Zugriffstoken (CAT) nur einmal für denselben Tunnel verwendet werden. Nachfolgende Verbindungsversuche mit demselben CAT werden abgewiesen. Weitere Informationen zur Verwendung von Client-Token finden Sie in der Referenzimplementierung für lokale Proxys unter. GitHub

Zielanwendung

Die Anwendung, die auf dem Zielgerät ausgeführt wird. Beispielsweise kann die Zielanwendung ein SSH-Daemon für die Einrichtung einer SSH-Sitzung mit Secure Tunneling sein.

Zielgerät

Das Remote-Gerät, auf das Sie zugreifen möchten.

Geräte-Agent

Eine IoT-Anwendung, die eine Verbindung zum AWS IoT Geräte-Gateway herstellt und über MQTT auf neue Tunnelbenachrichtigungen wartet. Weitere Informationen finden Sie unter IoT-Agent-Snippet.

Lokaler Proxy

Ein Software-Proxy, der auf den Quell- und Zielgeräten ausgeführt wird und einen Datenstrom zwischen dem Secure Tunneling-Service und der Geräteanwendung ermöglicht. Der lokale Proxy

kann im Quell- oder Zielmodus ausgeführt werden. Weitere Informationen finden Sie unter Lokaler Proxy.

Quellgerät

Das Gerät, das ein Bediener verwendet, um eine Sitzung mit dem Zielgerät zu initiieren, normalerweise ein Laptop oder Desktop-Computer.

Tunnel

Ein logischer Pfad AWS IoT , der die bidirektionale Kommunikation zwischen einem Quellgerät und einem Zielgerät ermöglicht.

## Wie funktioniert Secure Tunneling

Im Folgenden wird gezeigt, wie Secure Tunneling eine Verbindung zwischen Ihrem Quell- und Zielgerät herstellt. Informationen zu den verschiedenen Begriffen wie Client-Zugriffstoken (CAT) finden Sie unter. Secure Tunneling-Konzepte

1. Tunnel öffnen

   Um einen Tunnel für die Initiierung einer Sitzung mit Ihrem Remote-Zielgerät zu öffnen, können Sie den AWS Management Console Befehl AWS CLI open-tunnel oder die API verwenden. OpenTunnel

2. Client-Zugriffstokenpaar herunterladen

   Nachdem Sie einen Tunnel geöffnet haben, können Sie das Client-Zugriffstoken (CAT) für Ihre Quelle und Ihr Ziel herunterladen und auf Ihrem Quellgerät speichern. Sie müssen das CAT jetzt abrufen und speichern, bevor Sie den lokalen Proxy starten können.

3. Lokalen Proxy im Zielmodus starten

   Der IoT-Agent, der auf Ihrem Zielgerät installiert wurde und läuft, abonniert das reservierte MQTT-Thema `$aws/things/thing-name/tunnels/notify` und erhält das CAT. Hier *`thing-name`* ist der Name der AWS IoT Sache, die Sie für Ihr Ziel erstellen. Weitere Informationen finden Sie unter Themen zu Secure Tunneling.

   Der IoT-Agent verwendet dann das CAT, um den lokalen Proxy im Zielmodus zu starten und eine Verbindung auf der Zielseite des Tunnels einzurichten. Weitere Informationen finden Sie unter IoT-Agent-Snippet.

4. Lokalen Proxy im Quellmodus starten

AWS IoT Device Management Stellt nach dem Öffnen des Tunnels den CAT für die Quelle bereit, den Sie auf das Quellgerät herunterladen können. Sie können das CAT verwenden, um den lokalen Proxy im Quellmodus zu starten, der dann die Quellseite des Tunnels verbindet. Weitere Informationen zum lokalen Proxy finden Sie unter Lokaler Proxy.

5. Eine SSH-Sitzung öffnen

   Da beide Seiten des Tunnels verbunden sind, können Sie eine SSH-Sitzung starten, indem Sie den lokalen Proxy auf der Quellseite verwenden.

Weitere Informationen zur Verwendung des zum Öffnen eines Tunnels und AWS Management Console zum Starten einer SSH-Sitzung finden Sie unterÖffnen Sie einen Tunnel und starten Sie eine SSH-Sitzung zum Remote-Gerät.

Das folgende Video beschreibt, wie Secure Tunneling funktioniert, und führt Sie durch den Prozess der Einrichtung einer SSH-Sitzung zu einem Raspberry Pi-Gerät.

## Sicherer Tunnellebenszyklus

Tunnel können den Status `OPEN` oder `CLOSED` haben. Verbindungen zum Tunnel können den Status `CONNECTED` oder `DISCONNECTED` haben. Im Folgenden wird gezeigt, wie die verschiedenen Tunnel- und Verbindungsstatus funktionieren.

1. Wenn Sie einen Tunnel öffnen, hat er den Status `OPEN`. Der Quell- und Zielverbindungsstatus des Tunnels ist auf `DISCONNECTED` eingestellt.
2. Wenn sich ein Gerät (Quelle oder Ziel) mit dem Tunnel verbindet, ändert sich der zugehörige Verbindungsstatus in `CONNECTED`.
3. Wenn ein Gerät die Verbindung zum Tunnel trennt, während der Tunnelstatus `OPEN` bleibt, wechselt der entsprechende Verbindungsstatus wieder auf `DISCONNECTED`. Ein Gerät kann wiederholt eine Verbindung zu einem Tunnel herstellen und diese trennen, solange der Tunnel `OPEN` bleibt.

> **Note**
>
> Das Client-Zugriffstoken (CAT) kann nur einmal verwendet werden, um eine Verbindung zum Tunnel herzustellen. Um die Verbindung zum Tunnel wiederherzustellen, rotieren Sie die Client-Zugriffstoken mithilfe der RotateTunnelAccessTokenAPI-Operation oder des rotate-tunnel-access-tokenCLI-Befehls. Beispiele finden Sie unter Lösung von

Verbindungsproblemen beim AWS IoT sicheren Tunneling durch rotierende Client-Zugriffstoken.

4. Wenn Sie `CloseTunnel` aufrufen oder der Tunnel `OPEN` verbleibt und zwar länger als der `MaxLifetimeTimeout` -Wert, wird der Status eines Tunnels zu `CLOSED`. Sie können `MaxLifetimeTimeout` beim Aufruf von `OpenTunnel` konfigurieren. `MaxLifetimeTimeout` ist standardmäßig 12 Stunden, wenn Sie keinen Wert angeben.

> **Note**
>
> Ein Tunnel kann nicht wieder geöffnet werden, wenn er `CLOSED` ist.

5. Während der Tunnel sichtbar ist, können Sie `DescribeTunnel` und `ListTunnels` aufrufen, um Tunnelmetadaten anzuzeigen. Der Tunnel kann mindestens drei Stunden lang in der AWS IoT Konsole sichtbar sein, bevor er gelöscht wird.

# AWS IoT Tutorials zum sicheren Tunneling

AWS IoT Secure Tunneling hilft Kunden dabei, eine bidirektionale Kommunikation mit Remote-Geräten, die sich hinter einer Firewall befinden, über eine sichere Verbindung herzustellen, die von verwaltet wird. AWS IoT

Um AWS IoT sicheres Tunneling zu demonstrieren, verwenden Sie unsere AWS IoT Demo für sicheres Tunneling unter. GitHub

In den folgenden Tutorials erfahren Sie, wie Sie mit Secure Tunneling beginnen und wie Sie es verwenden können. Sie lernen, wie Sie:

1. Einen sicheren Tunnel mithilfe des Quick Setups und der manuellen Einrichtung für den Zugriff auf das Remote-Gerät erstellen.
2. Den lokalen Proxy konfigurieren, wenn Sie die manuelle Einrichtungsmethode verwenden, und eine Verbindung zum Tunnel herstellen, um auf das Zielgerät zuzugreifen.
3. Über einen Browser eine SSH-Verbindung zum Remote-Gerät herstellen, ohne den lokalen Proxy konfigurieren zu müssen.
4. Konvertieren Sie einen Tunnel, der mit der AWS CLI oder mit der manuellen Einrichtungsmethode erstellt wurde, in die Schnelleinrichtungsmethode.

# Tutorials in diesem Abschnitt

Die Tutorials in diesem Abschnitt konzentrieren sich auf die Erstellung eines Tunnels mithilfe der AWS Management Console und der AWS IoT API-Referenz. In der AWS IoT Konsole können Sie einen Tunnel von der Tunnel-Hub-Seite oder von der Detailseite eines von Ihnen erstellten Objekts aus erstellen. Weitere Informationen finden Sie unter Methoden zur Tunnelerstellung in der AWS IoT Konsole.

Dieser Abschnitt enthält die folgenden Tutorials:

- Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen

  Dieses Tutorial zeigt, wie Sie mithilfe von Quick Setup einen Tunnel von der Tunnel-Hub-Seite aus öffnen. Außerdem erfahren Sie, wie Sie browserbasiertes SSH verwenden, um über eine kontextabhängige Befehlszeilenschnittstelle in der Konsole auf das Remote-Gerät zuzugreifen. AWS IoT

- Öffnen Sie mithilfe der manuellen Einrichtung einen Tunnel und stellen Sie eine Verbindung zum Remote-Gerät her

  Dieses Tutorial zeigt, wie Sie mithilfe der manuellen Einrichtungsmethode einen Tunnel von der Tunnel-Hub-Seite aus öffnen. Sie lernen auch, wie Sie den lokalen Proxy von einem Terminal auf Ihrem Quellgerät aus konfigurieren und starten und eine Verbindung zum Tunnel herstellen.
- Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen

  Dieses Tutorial zeigt, wie Sie einen Tunnel von der Detailseite eines Objekts aus öffnen, das Sie erstellt haben. Sie lernen, wie Sie einen neuen Tunnel erstellen und einen vorhandenen verwenden. Der bestehende Tunnel entspricht dem letzten offenen Tunnel, der für das Gerät erstellt wurde. Sie können auch das browserbasierte SSH verwenden, um auf das Remote-Gerät zuzugreifen.

AWS IoT Tutorials zum sicheren Tunneling

- Öffnen Sie einen Tunnel und starten Sie eine SSH-Sitzung zum Remote-Gerät
- Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen

# Öffnen Sie einen Tunnel und starten Sie eine SSH-Sitzung zum Remote-Gerät

In diesen Tutorials lernen Sie, wie Sie per Fernzugriff auf ein Gerät zugreifen können, das sich hinter einer Firewall befindet. Sie können keine direkte SSH-Sitzung auf dem Gerät starten, da die Firewall den gesamten eingehenden Datenverkehr blockiert. Die Tutorials zeigen Ihnen, wie Sie einen Tunnel öffnen und diesen Tunnel dann verwenden können, um eine SSH-Sitzung zu einem Remote-Gerät zu starten.

## Voraussetzungen für das Tutorial

Die Voraussetzungen für die Ausführung des Tutorials können variieren, je nachdem, ob Sie die manuelle oder die Quick Setup Methode für das Öffnen eines Tunnels und den Zugriff auf das Remote-Gerät verwenden.

> **Note**
>
> Für beide Einrichtungsmethoden müssen Sie ausgehenden Datenverkehr auf Port 443 zulassen.

- Informationen zu den Voraussetzungen für das Tutorial zur Quick Setup Methode finden Sie unter Voraussetzungen für die Quick Setup Methode.
- Informationen zu den Voraussetzungen für das Tutorial zur manuellen Einrichtungsmethode finden Sie unter Voraussetzungen für die manuelle Einrichtungsmethode. Wenn Sie diese Einrichtungsmethode verwenden, müssen Sie den lokalen Proxy auf Ihrem Quellgerät konfigurieren. Informationen zum Herunterladen des lokalen Proxyquellcodes finden Sie unter Referenzimplementierung für lokale Proxys auf. GitHub

## Methoden zur Tunneleinrichtung

In diesen Tutorials erfahren Sie mehr über die manuellen und Quick Setup Methoden zum Öffnen eines Tunnels und zum Herstellen einer Verbindung zum Remote-Gerät. In der folgenden Tabelle wird der Unterschied zwischen den Einrichtungsmethoden dargestellt. Nachdem Sie den Tunnel erstellt haben, können Sie über eine Befehlszeilen-Schnittstelle im Browser eine SSH-Verbindung zum Remote-Gerät herstellen. Wenn Sie die Token verlegen oder der Tunnel unterbrochen wird, können Sie neue Zugriffstoken senden, um die Verbindung zum Tunnel wiederherzustellen.

Schnelle und manuelle Einrichtungsmethoden

| Kriterien | Quick Setup | Manuelle Einrichtung |
| --- | --- | --- |
| Tunnel-Erstellung | Erstellen Sie einen neuen Tunnel mit editierbaren Standardkonfigurationen. Um auf Ihr Remote-Gerät zuzugreifen, können Sie SSH nur als Zieldienst verwenden. | Erstellen Sie einen Tunnel, indem Sie die Tunnelkonfigurationen manuell angeben. Sie können diese Methode verwenden, um über andere Dienste als SSH eine Verbindung zum Remote-Gerät herzustellen. |
| Zugriffstoken | Das Zielzugriffstoken wird Ihrem Gerät automatisch zum reservierten MQTT-Thema zugestellt, wenn bei der Erstellung des Tunnels ein Objektname angegeben wurde. Sie müssen das Token nicht auf Ihr Quellgerät herunterladen oder dort verwalten. | Sie müssen das Token manuell auf Ihrem Quellgerät herunterladen und verwalten. Das Zielzugriffstoken wird Ihrem Gerät automatisch zum reservierten MQTT-Thema zugestellt, wenn bei der Erstellung des Tunnels ein Objektname angegeben wurde. |
| Lokaler Proxy | Für die Interaktion mit dem Gerät wird automatisch ein webbasierter lokaler Proxy für Sie konfiguriert. Sie müssen den lokalen Proxy nicht manuell konfigurieren. | Sie müssen den lokalen Proxy manuell konfigurieren und starten. Um den lokalen Proxy zu konfigurieren, können Sie entweder den AWS IoT Geräteclient verwenden oder die Referenzimplementierung für den lokalen Proxy herunterladen GitHub. |

## Methoden zur Tunnelerstellung in der AWS IoT Konsole

Die Tutorials in diesem Abschnitt zeigen Ihnen, wie Sie mithilfe der AWS Management Console und der OpenTunnelAPI einen Tunnel erstellen. Wenn Sie das Ziel bei der Erstellung eines Tunnels konfigurieren, übermittelt AWS IoT Secure Tunneling das Ziel-Client-Zugriffstoken über MQTT und das reservierte MQTT-Thema,) an das Remote-Gerät. `$aws/things/RemoteDeviceA/tunnels/notify` Nach Erhalt der MQTT-Nachricht startet der IoT-Agent auf dem Remote-Gerät den lokalen Proxy im Zielmodus. Weitere Informationen finden Sie unter Reservierte Themen.

> **Note**
>
> Sie können die Zielkonfiguration weglassen, wenn Sie das Zugriffstoken für den Zielclient über eine andere Methode an das Remote-Gerät senden möchten. Weitere Informationen finden Sie unter Ein Remote-Gerät konfigurieren und IoT-Agent verwenden.

In der AWS IoT Konsole können Sie einen Tunnel mit einer der folgenden Methoden erstellen. Informationen zu Tutorials, in denen Sie lernen, wie Sie mit diesen Methoden einen Tunnel erstellen, finden Sie unter Tutorials in diesem Abschnitt.

- Tunnel-Hub

  Bei der Erstellung des Tunnels können Sie angeben, ob Sie Quick Setup oder die manuelle Einrichtung für die Erstellung des Tunnels verwenden möchten, und die optionalen Details zur Tunnelkonfiguration angeben. Zu den Konfigurationsdetails gehören auch der Name des Zielgeräts und der Dienst, den Sie für die Verbindung mit dem Gerät verwenden möchten. Nachdem Sie einen Tunnel erstellt haben, können Sie entweder SSH im Browser verwenden oder ein Terminal außerhalb der AWS IoT Konsole öffnen, um auf Ihr Remote-Gerät zuzugreifen.

- Seite mit Objektdetails

  Bei der Erstellung des Tunnels können Sie außerdem angeben, ob Sie den zuletzt geöffneten Tunnel verwenden oder einen neuen Tunnel für das Gerät erstellen möchten. Außerdem können Sie die Einrichtungsmethoden auswählen und alle optionalen Details zur Tunnelkonfiguration angeben. Sie können die Konfigurationsdetails eines vorhandenen Tunnels nicht bearbeiten. Sie können die Quick Setup Methode verwenden, um die Zugriffstoken zu rotieren und über den Browser eine SSH-Verbindung zum Remote-Gerät herzustellen. Um einen Tunnel mit dieser Methode zu öffnen, müssen Sie in der AWS IoT Registrierung ein IoT-Ding (z. B. `RemoteDeviceA`) erstellt haben. Weitere Informationen finden Sie unter Registrieren eines Geräts in der AWS IoT Registrierung.

Tutorials in diesem Abschnitt

- Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen
- Öffnen Sie mithilfe der manuellen Einrichtung einen Tunnel und stellen Sie eine Verbindung zum Remote-Gerät her

## Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen

Sie können die Quick Setup Methode oder die manuelle Einrichtungsmethode verwenden, um einen Tunnel zu erstellen. Dieses Tutorial zeigt, wie Sie einen Tunnel mit der Quick Setup Methode öffnen und das browserbasierte SSH verwenden, um eine Verbindung zum Remote-Gerät herzustellen. Ein Beispiel, das zeigt, wie ein Tunnel mithilfe der manuellen Einrichtungsmethode geöffnet wird, finden Sie unter Öffnen Sie mithilfe der manuellen Einrichtung einen Tunnel und stellen Sie eine Verbindung zum Remote-Gerät her.

Mithilfe der Quick Setup Methode können Sie einen neuen Tunnel mit Standardkonfigurationen erstellen, die bearbeitet werden können. Ein webbasierter lokaler Proxy wird für Sie konfiguriert und das Zugriffstoken wird automatisch über MQTT an Ihr Remote-Zielgerät gesendet. Nachdem Sie einen Tunnel erstellt haben, können Sie über eine Befehlszeilen-Schnittstelle innerhalb der Konsole mit Ihrem Remote-Gerät interagieren.

Bei der Quick Setup Methode müssen Sie SSH als Zieldienst für den Zugriff auf das Remote-Gerät verwenden. Weitere Informationen zu den verschiedenen Einrichtungsmethoden finden Sie unter Methoden zur Tunneleinrichtung.

### Voraussetzungen für die Quick Setup Methode

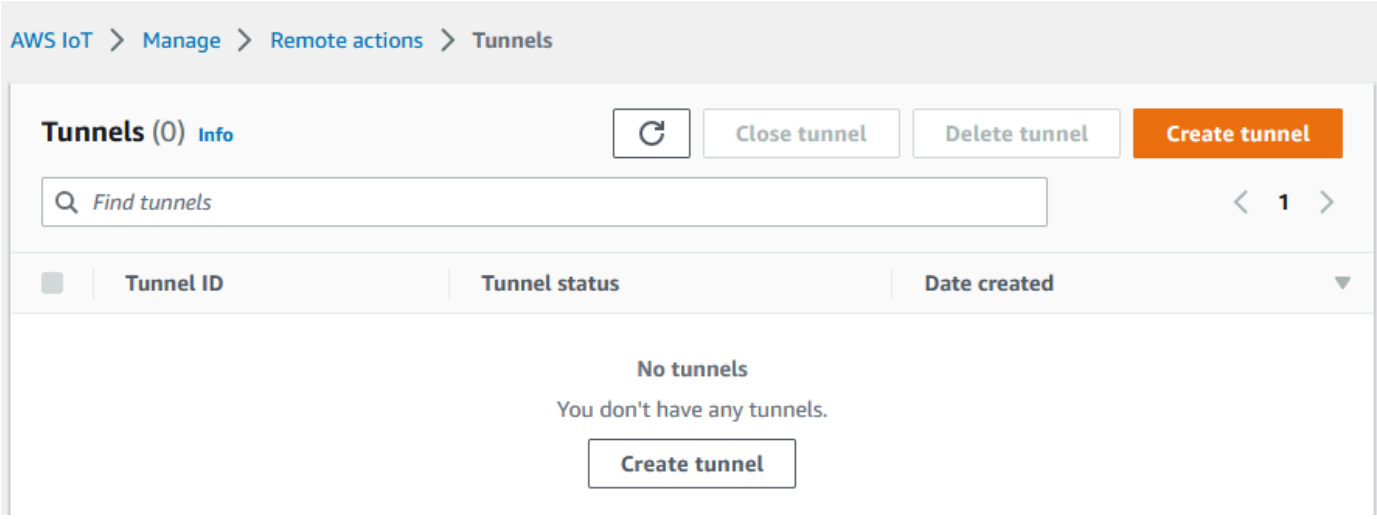
- Die Firewalls, hinter denen sich das Remote-Gerät befindet, müssen ausgehenden Datenverkehr an Port 443 zulassen. Der Tunnel, den Sie erstellen, verwendet diesen Port, um eine Verbindung zum Remote-Gerät herzustellen.
- Auf dem Remote-Gerät läuft ein IoT-Geräteagent (siehe IoT-Agent-Snippet), der eine Verbindung zum AWS IoT Gerätegateway herstellt und mit einem MQTT-Themenabonnement konfiguriert ist. Weitere Informationen finden Sie unter Ein Gerät mit dem AWS IoT Geräte-Gateway verbinden.
- Auf dem Remote-Gerät muss ein SSH-Daemon ausgeführt werden.

### Tunnel öffnen

Sie können einen sicheren Tunnel mit dem AWS Management Console, der AWS IoT API-Referenz oder dem öffnen AWS CLI. Sie können optional einen Zielnamen konfigurieren, der für dieses Tutorial jedoch nicht erforderlich ist. Wenn Sie das Ziel konfigurieren, übermittelt Secure Tunneling das Zugriffstoken automatisch mithilfe von MQTT an das Remote-Gerät. Weitere Informationen finden Sie unter Methoden zur Tunnelerstellung in der AWS IoT Konsole.

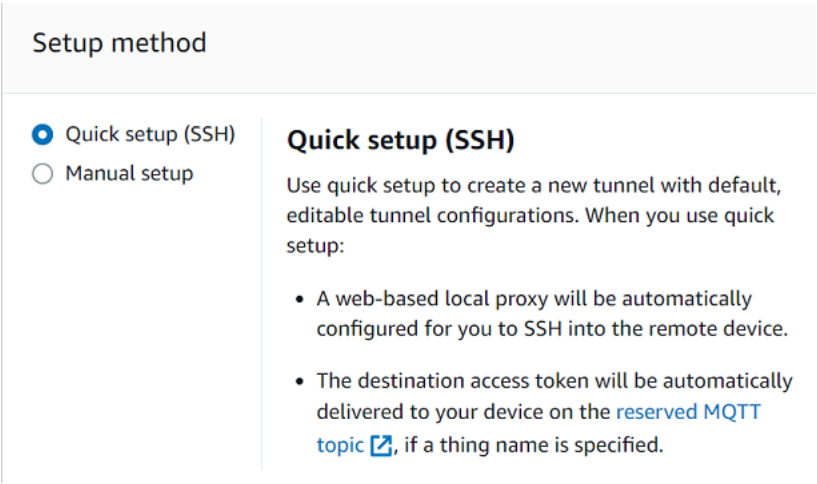
Um einen Tunnel mit der Konsole zu öffnen,

1. Gehen Sie zum Tunnel-Hub der AWS IoT -Konsole und wählen Sie Tunnel erstellen.




2. Wählen Sie für dieses Tutorial die Quick Setup Methode zur Tunnelerstellung und wählen Sie dann Weiter.

> **Note**
>
> Wenn Sie auf der Detailseite eines von Ihnen erstellten Objekts einen sicheren Tunnel erstellen, können Sie wählen, ob Sie einen neuen Tunnel erstellen oder einen vorhandenen verwenden möchten. Weitere Informationen finden Sie unter Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen.

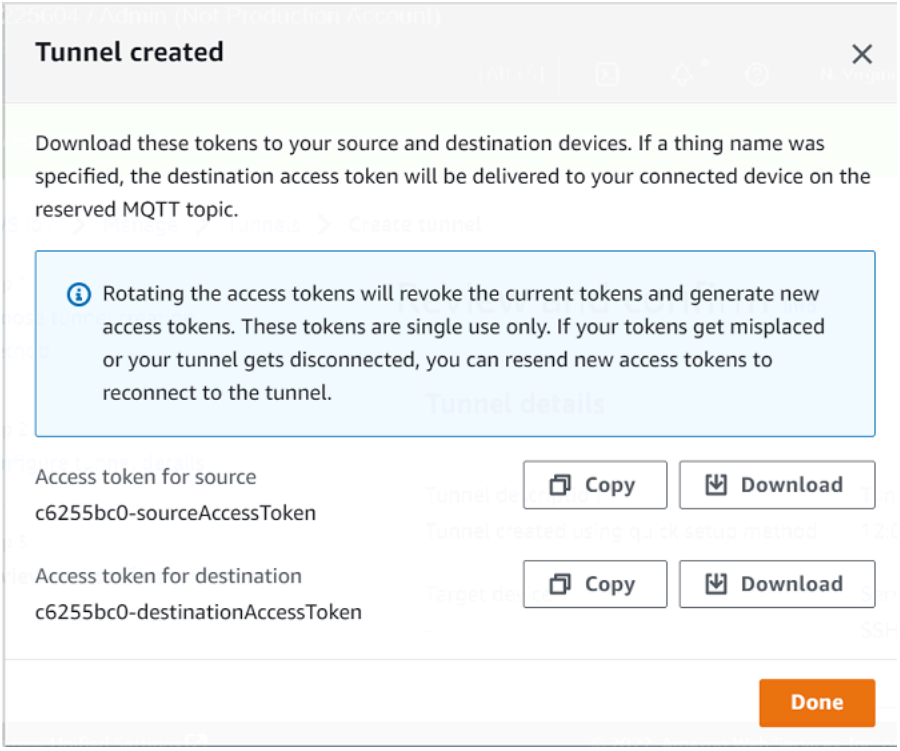


3. Überprüfen und bestätigen Sie die Details der Tunnelkonfiguration. Um einen Tunnel zu erstellen, wählen Sie Bestätigen und erstellen. Wenn Sie die Details bearbeiten möchten, wählen Sie Zurück, um zur vorherigen Seite zurückzukehren. Bestätigen Sie dann und erstellen Sie den Tunnel.

   > **Note**
   >
   > Wenn Sie die Quick Setup Methode verwenden, kann der Dienstname nicht bearbeitet werden. Sie müssen SSH als Dienst verwenden.

4. Um den Tunnel zu erstellen, wählen Sie Fertig.

   Für dieses Tutorial müssen Sie die Quell- oder Zielzugriffstoken nicht herunterladen. Diese Token können nur einmal verwendet werden, um eine Verbindung zum Tunnel herzustellen. Wenn Ihr Tunnel unterbrochen wird, können Sie neue Token generieren und an Ihr Remote-Gerät senden, um die Verbindung zum Tunnel wiederherzustellen. Weitere Informationen finden Sie unter Tunnelzugriffstoken erneut senden.




So öffnen Sie einen Tunnel über die API

Um einen neuen Tunnel zu öffnen, können Sie die OpenTunnelAPI-Operation verwenden.

> **Note**
>
> Sie können einen Tunnel mit der Quick Setup Methode nur von der AWS IoT -Konsole aus erstellen. Wenn Sie die AWS IoT API-Referenz-API oder die verwenden AWS CLI, wird die manuelle Einrichtungsmethode verwendet. Sie können den vorhandenen Tunnel, den Sie erstellt haben, öffnen und dann die Einrichtungsmethode des Tunnels ändern, um die Quick Setup Methode zu verwenden. Weitere Informationen finden Sie unter Öffnen eines vorhandenen Tunnels und Verwenden von browserbasiertem SSH.

Im Folgenden wird ein Beispiel gezeigt, wie dieser API-Vorgang ausgeführt wird. Wenn Sie optional den Objektnamen und den Zieldienst angeben möchten, verwenden Sie den `DestinationConfig`-Parameter. Ein Beispiel, das zeigt, wie dieser Parameter verwendet wird, finden Sie unterÖffnen Sie einen neuen Tunnel für das Remote-Gerät.

```
aws iotsecuretunneling open-tunnel
```

Wenn Sie diesen Befehl ausführen, wird ein neuer Tunnel erstellt und Sie erhalten die Quell- und Zielzugriffstoken.

```
{
    "tunnelId": "01234567-89ab-0123-4c56-789a01234bcd",
    "tunnelArn": "arn:aws:iot:us-
east-1:123456789012:tunnel/01234567-89ab-0123-4c56-789a01234bcd",
    "sourceAccessToken": "<SOURCE_ACCESS_TOKEN>",
    "destinationAccessToken": "<DESTINATION_ACCESS_TOKEN>"
}
```

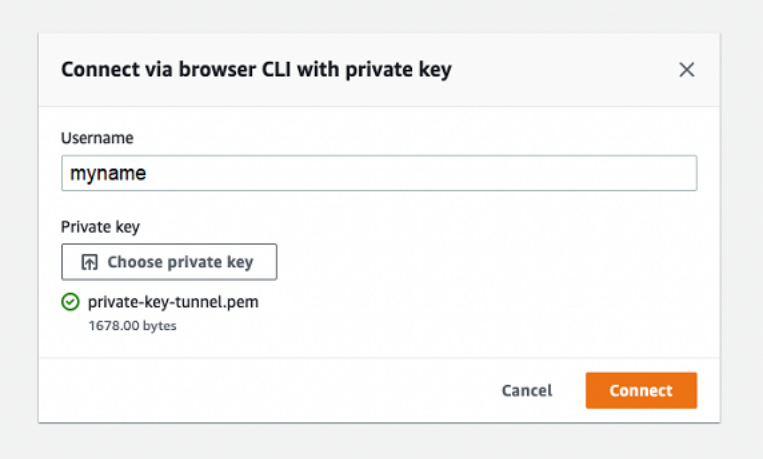
Verwenden von browserbasiertem SSH

Nachdem Sie mit der Quick Setup Methode einen Tunnel erstellt haben und Ihr Zielgerät eine Verbindung zum Tunnel hergestellt hat, können Sie über ein browserbasiertes SSH auf das Remote-Gerät zugreifen. Mithilfe des browserbasierten SSH können Sie direkt mit dem Remote-Gerät kommunizieren, indem Sie Befehle in eine kontextinterne Befehlszeilen-Schnittstelle in der Konsole eingeben. Diese Funktion erleichtert Ihnen die Interaktion mit dem Remote-Gerät, da Sie kein Terminal außerhalb der Konsole öffnen oder den lokalen Proxy konfigurieren müssen.

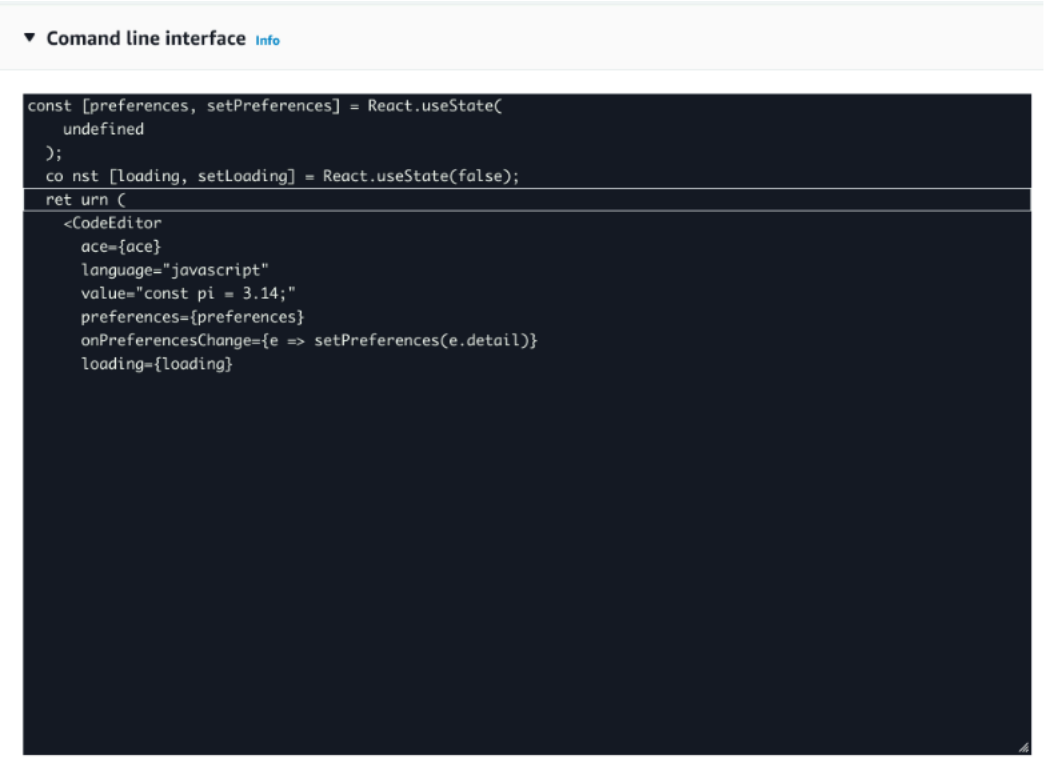
Browserbasiertes SSH verwenden

1. Gehen Sie zum Tunnel-Hub der AWS IoT -Konsole und wählen Sie den von Ihnen erstellten Tunnel aus, um seine Details anzuzeigen.
2. Erweitern Sie den Abschnitt Secure Shell (SSH) und wählen Sie dann Verbinden.
3. Wählen Sie aus, ob Sie sich bei der SSH-Verbindung authentifizieren möchten, indem Sie Ihren Benutzernamen und Ihr Passwort angeben, oder ob Sie für eine sicherere Authentifizierung den privaten Schlüssel Ihres Geräts verwenden können. Wenn Sie sich mit dem privaten Schlüssel authentifizieren, beachten Sie, dass nur RSA-Schlüssel im PEM-Format (256 und 512) mit der SSH-Konsole funktionieren. AWS IoT Secure Tunneling

   - Um mit Ihrem Benutzernamen und Passwort eine Verbindung herzustellen, wählen Sie Passwort verwenden. Sie können dann Ihren Benutzernamen und Ihr Passwort eingeben und das In-Browser-CLI verwenden.
   - Um mit dem privaten Schlüssel Ihres Zielgeräts eine Verbindung herzustellen, wählen Sie Privaten Schlüssel verwenden aus. Geben Sie Ihren Benutzernamen an, laden Sie die private Schlüsseldatei des Geräts hoch und wählen Sie dann Verbinden, um mit der Verwendung des CLI im Browser zu beginnen.




Nachdem Sie sich bei der SSH-Verbindung authentifiziert haben, können Sie schnell mit der Eingabe von Befehlen beginnen und über das Browser-CLI mit dem Gerät interagieren, da der lokale Proxy bereits für Sie konfiguriert wurde.




Wenn die Browser-CLI nach Ablauf der Tunneldauer geöffnet bleibt, kann es zu einem Timeout kommen, wodurch die Befehlszeilen-Schnittstelle unterbrochen wird. Sie können den Tunnel duplizieren und eine weitere Sitzung starten, um mit dem Remote-Gerät in der Konsole selbst zu interagieren.

Behebung von Problemen bei der Verwendung des browserbasierten SSH

Im Folgenden wird gezeigt, wie Sie einige Probleme beheben können, auf die Sie bei der Verwendung von browserbasiertem SSH stoßen könnten.

- Anstelle der Befehlszeilen-Schnittstelle wird ein Fehler angezeigt.

  Möglicherweise wird der Fehler angezeigt, weil die Verbindung zu Ihrem Zielgerät unterbrochen wurde. Sie können Neue Zugriffstoken generieren wählen, um neue Zugriffstoken zu generieren und die Token mithilfe von MQTT an Ihr Remote-Gerät zu senden. Die neuen Token können verwendet werden, um die Verbindung zum Tunnel wiederherzustellen. Beim erneuten Herstellen der Verbindung mit dem Tunnel wird der Verlauf gelöscht und die Befehlszeilensitzung aktualisiert.
- Bei der Authentifizierung mit einem privaten Schlüssel wird ein Fehler angezeigt, dass die Verbindung zum Tunnel unterbrochen wurde

Möglicherweise wird der Fehler angezeigt, weil Ihr privater Schlüssel vom Zielgerät vielleicht nicht akzeptiert wurde. Um diesen Fehler zu beheben, überprüfen Sie die Datei mit dem privaten Schlüssel, die Sie zur Authentifizierung hochgeladen haben. Wenn Sie immer noch einen Fehler sehen, überprüfen Sie Ihre Geräteprotokolle. Sie können auch versuchen, erneut eine Verbindung zum Tunnel herzustellen, indem Sie neue Zugriffstoken an Ihr Remote-Gerät senden.

- Ihr Tunnel wurde geschlossen, als Sie die Sitzung verwendet haben

  Wenn Ihr Tunnel geschlossen wurde, weil er länger als die angegebene Dauer geöffnet blieb, wird Ihre Befehlszeilensitzung möglicherweise unterbrochen. Ein Tunnel kann nicht wieder geöffnet werden, wenn er einmal geschlossen wurde. Um die Verbindung wieder herzustellen, müssen Sie einen weiteren Tunnel zum Gerät öffnen.

  Sie können einen Tunnel duplizieren, um einen neuen Tunnel mit denselben Konfigurationen wie der geschlossene Tunnel zu erstellen. Sie können einen geschlossenen Tunnel von der Konsole aus duplizieren. AWS IoT Um den Tunnel zu duplizieren, wählen Sie den Tunnel aus, der geschlossen wurde, um seine Details anzuzeigen, und wählen Sie dann Tunnel duplizieren aus. Geben Sie die Tunneldauer an, die Sie verwenden möchten, und erstellen Sie dann den neuen Tunnel.

Bereinigen

- Tunnel schließen

  Wir empfehlen, den Tunnel zu schließen, wenn Sie ihn nicht mehr verwenden. Ein Tunnel kann auch geschlossen werden, wenn er länger als die angegebene Tunneldauer geöffnet blieb. Ein Tunnel kann nicht wieder geöffnet werden, wenn er einmal geschlossen wurde. Sie können einen Tunnel trotzdem duplizieren, indem Sie den geschlossenen Tunnel und dann Tunnel duplizieren auswählen. Geben Sie die Tunneldauer an, die Sie verwenden möchten, und erstellen Sie dann den neuen Tunnel.

  - Um einen einzelnen Tunnel oder mehrere Tunnel von der AWS IoT -Konsole aus zu schließen, wechseln Sie zum Tunnel-Hub, wählen Sie die Tunnel aus, die Sie schließen möchten, und wählen Sie dann Tunnel schließen aus.
  - Verwenden Sie die API, um einen einzelnen Tunnel oder mehrere Tunnel mithilfe der AWS IoT CloseTunnelAPI-Referenz-API zu schließen.

    ```
    aws iotsecuretunneling close-tunnel \
    ```

```
    --tunnel-id "01234567-89ab-0123-4c56-789a01234bcd"
```

- Löschen eines Tunnels

  Sie können einen Tunnel dauerhaft aus Ihrem löschen AWS-Konto.

  > **Warning**
  >
  > Dieser Löschvorgang ist dauerhaft und kann nicht rückgängig gemacht werden.

  - Um einen einzelnen Tunnel oder mehrere Tunnel von der AWS IoT -Konsole aus zu löschen, wechseln Sie zum Tunnel-Hub, wählen Sie die Tunnel aus, die Sie löschen möchten, und wählen Sie dann Tunnel löschen aus.
  - Verwenden Sie die API, um einen einzelnen Tunnel oder mehrere Tunnel mithilfe der AWS IoT CloseTunnelAPI-Referenz-API zu löschen. Wenn Sie die API verwenden, setzen Sie das `delete`-Flag auf `true`.

    ```
    aws iotsecuretunneling close-tunnel \
        --tunnel-id "01234567-89ab-0123-4c56-789a01234bcd"
        --delete true
    ```

## Öffnen Sie mithilfe der manuellen Einrichtung einen Tunnel und stellen Sie eine Verbindung zum Remote-Gerät her

Wenn Sie einen Tunnel öffnen, können Sie die Quick Setup Methode oder die manuelle Einrichtungsmethode wählen, um einen Tunnel zum Remote-Gerät zu öffnen. Dieses Tutorial zeigt, wie Sie einen Tunnel mithilfe der manuellen Einrichtungsmethode öffnen und den lokalen Proxy konfigurieren und starten, um eine Verbindung zum Remote-Gerät herzustellen.

Wenn Sie die manuelle Einrichtungsmethode verwenden, müssen Sie die Tunnelkonfigurationen bei der Erstellung des Tunnels manuell angeben. Nachdem Sie den Tunnel erstellt haben, können Sie SSH im Browser verwenden oder ein Terminal außerhalb der AWS IoT Konsole öffnen. Dieses Tutorial zeigt, wie Sie das Terminal außerhalb der Konsole verwenden, um auf das Remote-Gerät zuzugreifen. Sie erfahren auch, wie Sie den lokalen Proxy konfigurieren und dann eine Verbindung zum lokalen Proxy herstellen, um mit dem Remote-Gerät zu interagieren. Um eine Verbindung zum lokalen Proxy herzustellen, müssen Sie beim Erstellen des Tunnels das Quellzugriffstoken herunterladen.

Sie können diese Methode verwenden, um über andere Dienste als SSH eine Verbindung zum Remote-Gerät herzustellen. Weitere Informationen zu den verschiedenen Einrichtungsmethoden finden Sie unter Methoden zur Tunneleinrichtung.

Voraussetzungen für die manuelle Einrichtungsmethode

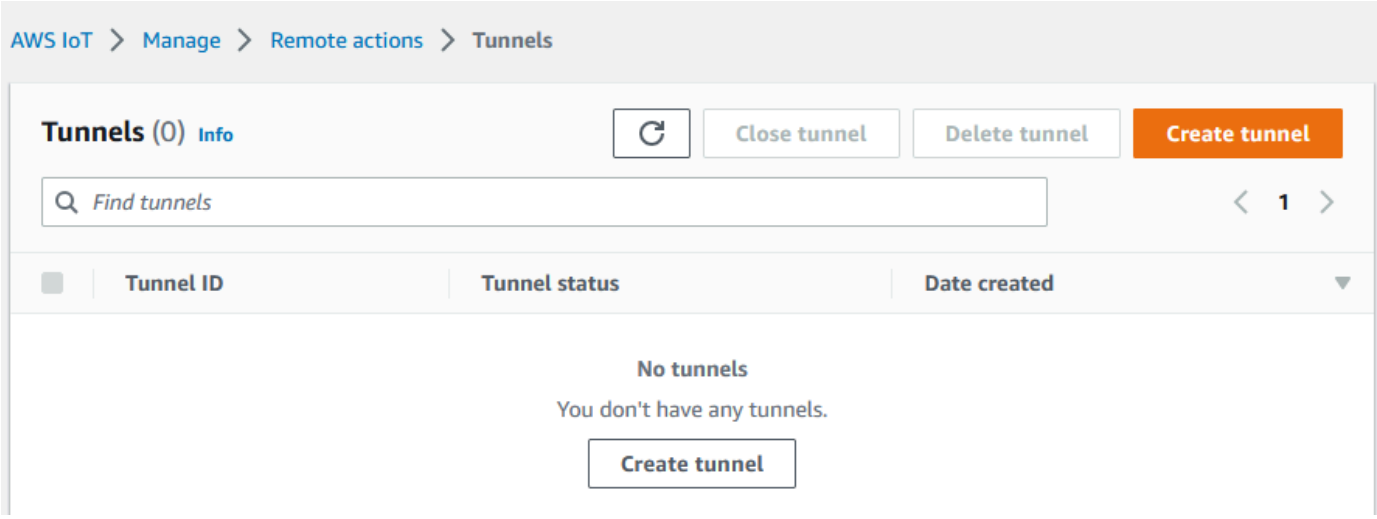
- Die Firewalls, hinter denen sich das Remote-Gerät befindet, müssen ausgehenden Datenverkehr an Port 443 zulassen. Der Tunnel, den Sie erstellen, verwendet diesen Port, um eine Verbindung zum Remote-Gerät herzustellen.
- Auf dem Remote-Gerät läuft ein IoT-Geräteagent (siehe IoT-Agent-Snippet), der eine Verbindung zum AWS IoT Gerätegateway herstellt und mit einem MQTT-Themenabonnement konfiguriert ist. Weitere Informationen finden Sie unter Ein Gerät mit dem AWS IoT Geräte-Gateway verbinden.
- Auf dem Remote-Gerät muss ein SSH-Daemon ausgeführt werden.
- Sie haben den lokalen Proxy-Quellcode von der Plattform Ihrer Wahl heruntergeladen GitHub und ihn für die Plattform Ihrer Wahl erstellt. In diesem Tutorial verweisen wir auf die erstellte lokale ausführbare Proxy-Datei als `localproxy`.

Tunnel öffnen

Sie können einen sicheren Tunnel mit dem AWS Management Console, der AWS IoT API-Referenz oder dem öffnen AWS CLI. Sie können optional einen Zielnamen konfigurieren, der für dieses Tutorial jedoch nicht erforderlich ist. Wenn Sie das Ziel konfigurieren, übermittelt Secure Tunneling das Zugriffstoken automatisch mithilfe von MQTT an das Remote-Gerät. Weitere Informationen finden Sie unter Methoden zur Tunnelerstellung in der AWS IoT Konsole.

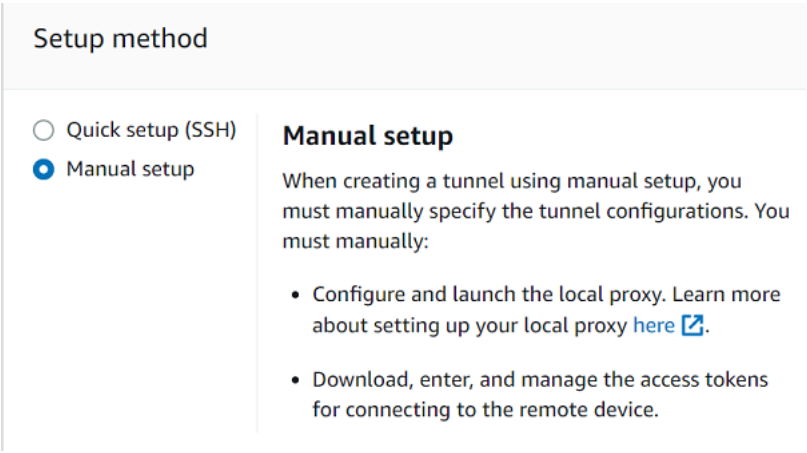
Um einen Tunnel mit der Konsole zu öffnen,

1. Gehen Sie zum Tunnel-Hub der AWS IoT -Konsole und wählen Sie Tunnel erstellen.




2. Wählen Sie für dieses Tutorial Manuelle Einrichtungsmethode zur Erstellung des Tunnels und wählen Sie dann Weiter. Informationen zur Verwendung der Quick Setup Methode zum Erstellen eines Tunnels finden Sie unter Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen.

> **Note**
>
> Wenn Sie auf der Detailseite eines von Ihnen erstellten Objekts einen sicheren Tunnel erstellen, können Sie wählen, ob Sie einen neuen Tunnel erstellen oder einen vorhandenen verwenden möchten. Weitere Informationen finden Sie unter Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen.



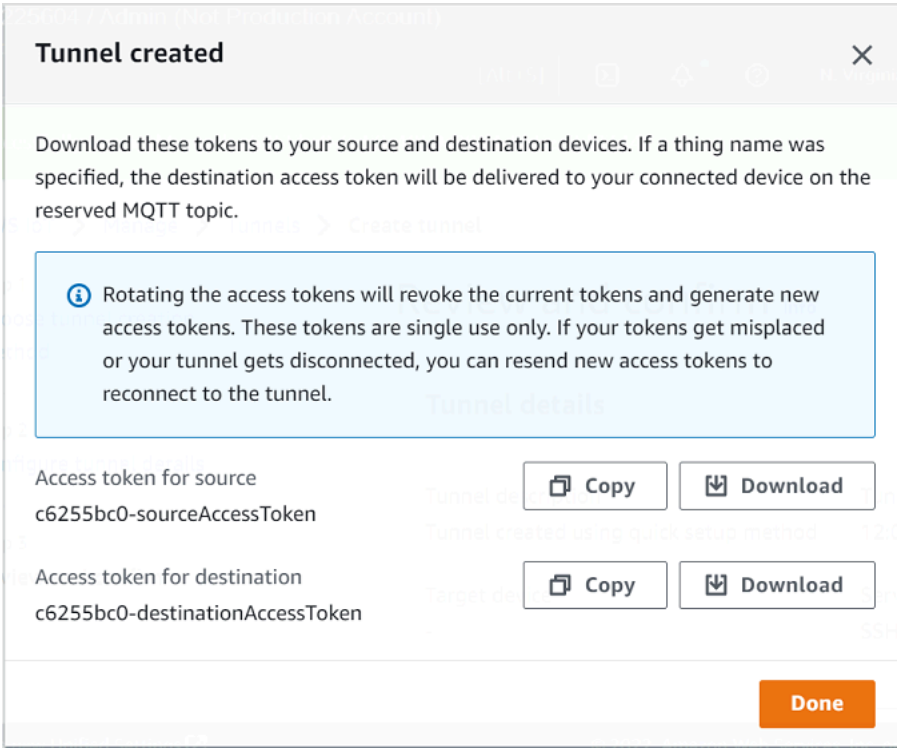
3. (Optional) Geben Sie die Konfigurationseinstellungen für Ihren Tunnel ein. Sie können diesen Schritt auch überspringen und mit dem nächsten Schritt fortfahren, um einen Tunnel zu erstellen.

   Geben Sie eine Tunnelbeschreibung, eine Dauer des Tunnel-Timeouts und Ressourcen-Tags als Schlüssel-Wert-Paare ein, um Ihre Ressource leichter identifizieren zu können. Für dieses Tutorial können Sie die Zielkonfiguration überspringen.

   > **Note**
   >
   > Für die Dauer der Offenhaltung eines Tunnels werden Ihnen keine Gebühren in Rechnung gestellt. Gebühren fallen nur an, wenn Sie einen neuen Tunnel erstellen. Preisinformationen finden Sie im Abschnitt Secure Tunneling unter AWS IoT Device Management -Preise.

4. Laden Sie die Client-Zugriffstoken herunter und wählen Sie dann Fertig aus. Die Token können nicht heruntergeladen werden, nachdem Sie Fertig ausgewählt haben.

   Diese Token können nur einmal verwendet werden, um eine Verbindung zum Tunnel herzustellen. Wenn Sie die Token verlegen oder die Verbindung zum Tunnel unterbrochen wird, können Sie neue Token erzeugen und an Ihr Remote-Gerät senden, um die Verbindung zum Tunnel wiederherzustellen.



So öffnen Sie einen Tunnel über die API

Um einen neuen Tunnel zu öffnen, können Sie die OpenTunnelAPI-Operation verwenden. Sie können mithilfe der API auch zusätzliche Konfigurationen angeben, z. B. die Tunneldauer und die Zielkonfiguration.

```
aws iotsecuretunneling open-tunnel \
    --region us-east-1 \
    --endpoint https://api.us-east-1.tunneling.iot.amazonaws.com
```

Wenn Sie diesen Befehl ausführen, wird ein neuer Tunnel erstellt und Sie erhalten die Quell- und Zielzugriffstoken.

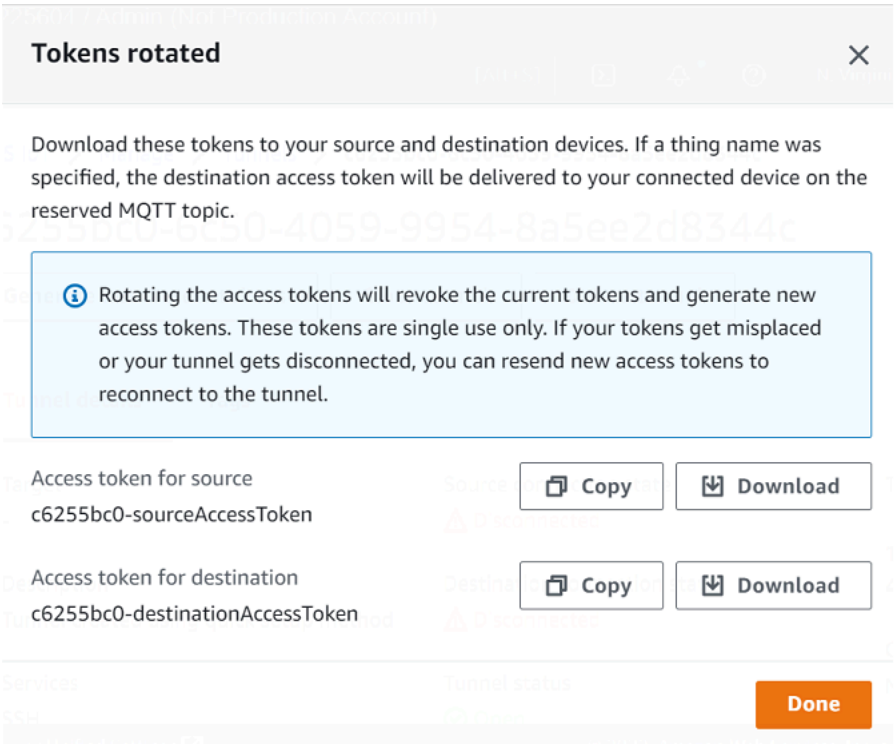
```
{
    "tunnelId": "01234567-89ab-0123-4c56-789a01234bcd",
    "tunnelArn": "arn:aws:iot:us-
east-1:123456789012:tunnel/01234567-89ab-0123-4c56-789a01234bcd",
    "sourceAccessToken": "<SOURCE_ACCESS_TOKEN>",
    "destinationAccessToken": "<DESTINATION_ACCESS_TOKEN>"
}
```

Tunnelzugriffstoken erneut senden

Die Token, die Sie beim Erstellen eines Tunnels erhalten haben, können nur einmal verwendet werden, um eine Verbindung zum Tunnel herzustellen. Wenn Sie das Zugriffstoken verlegen oder der Tunnel unterbrochen wird, können Sie neue Zugriffstoken mit MQTT ohne zusätzliche Kosten erneut an das Remote-Gerät senden. AWS IoT Sicheres Tunneling widerruft die aktuellen Token und gibt neue Zugriffstoken zurück, um die Verbindung zum Tunnel wiederherzustellen.

Um die Token von der Konsole aus zu rotieren,

1. Gehen Sie zum Tunnel-Hub der AWS IoT Konsole und wählen Sie den Tunnel aus, den Sie erstellt haben.
2. Wählen Sie auf der Seite mit den Tunneldetails die Option Neue Zugriffstoken generieren und dann Weiter aus.
3. Laden Sie die neuen Zugriffstoken für Ihren Tunnel herunter und wählen Sie Fertig. Diese Token können nur einmal verwendet werden. Wenn Sie die Token verlegen oder der Tunnel unterbrochen wird, können Sie neue Zugriffstoken senden, um die Verbindung zum Tunnel wiederherzustellen.




So rotieren Sie Zugriffstokens über die API

Um die Tunnelzugriffstoken rotieren zu lassen, können Sie den RotateTunnelAccessTokenAPI-Vorgang verwenden, um die aktuellen Token zu widerrufen und neue Zugriffstoken für die erneute Verbindung mit dem Tunnel zurückzugeben. Mit dem folgenden Befehl werden beispielsweise die Zugriffstoken für das Zielgerät rotiert, *RemoteThing1*.

```
aws iotsecuretunneling rotate-tunnel-access-token \
    --tunnel-id <tunnel-id> \
    --client-mode DESTINATION \
    --destination-config thingName=<RemoteThing1>,services=SSH \
    --region <region>
```

Wenn Sie diesen Befehl ausführen, wird das neue Zugriffstoken generiert, siehe folgendes Beispiel. Das Token wird dann über MQTT an das Gerät übermittelt, um eine Verbindung zum Tunnel herzustellen, sofern der Geräteagent korrekt eingerichtet ist.

```
{
    "destinationAccessToken": "destination-access-token",
    "tunnelArn": "arn:aws:iot:region:account-id:tunnel/tunnel-id"
}
```

Beispiele, die zeigen, wie und wann die Zugriffstoken rotiert werden müssen, finden Sie unter Lösung von Verbindungsproblemen beim AWS IoT sicheren Tunneling durch rotierende Client-Zugriffstoken.

Konfigurieren und Starten des lokalen Proxys

Um eine Verbindung zum Remote-Gerät herzustellen, öffnen Sie ein Terminal auf Ihrem Laptop und konfigurieren und starten Sie den lokalen Proxy. Der lokale Proxy überträgt Daten, die von der auf dem Quellgerät ausgeführten Anwendung gesendet werden, mithilfe von sicherem Tunneling über eine WebSocket sichere Verbindung. Sie können die lokale Proxyquelle von herunterladen. GitHub

Öffnen Sie ein Terminal auf Ihrem Laptop, kopieren Sie das Zugriffstoken für den Quell-Client und starten Sie den lokalen Proxy im Quellmodus. Im Folgenden finden Sie einen Beispielbefehl zum Starten des lokalen Proxys. Im folgenden Befehl ist der lokale Proxy so konfiguriert, dass er auf neue Verbindungen an Port 5555 wartet. In diesem Befehl gilt Folgendes:

- `-r`gibt die an AWS-Region, was dieselbe Region sein muss, in der Ihr Tunnel erstellt wurde.
- `-s` gibt den Port an, zu dem der Proxy eine Verbindung herstellen soll.
- `-t` gibt den Client-Token-Text an.

```
./localproxy -r us-east-1 -s 5555 -t source-client-access-token
```

Wenn Sie diesen Befehl ausführen, wird der lokale Proxy im Quellmodus gestartet. Wenn Sie nach der Ausführung des Befehls die folgende Fehlermeldung erhalten, richten Sie den CA-Pfad ein. Weitere Informationen finden Sie unter Lokaler Proxy für sicheres Tunneling auf. GitHub

```
Could not perform SSL handshake with proxy server: certificate verify failed
```

Im Folgenden finden Sie eine Beispielausgabe für die Ausführung des lokalen Proxys im `source`-Modus.

```
...
...

Starting proxy in source mode
Attempting to establish web socket connection with endpoint wss://
data.tunneling.iot.us-east-1.amazonaws.com:443
Resolved proxy  server IP: 10.10.0.11
Connected successfully with proxy server
```

```
Performing SSL handshake with proxy server
Successfully completed SSL handshake with proxy server
HTTP/1.1 101 Switching Protocols

...

Connection: upgrade
channel-id: 01234567890abc23-00001234-0005678a-b1234c5de677a001-2bc3d456
upgrade: websocket

...

Web socket session ID: 01234567890abc23-00001234-0005678a-b1234c5de677a001-2bc3d456
Web socket subprotocol selected: aws.iot.securetunneling-2.0
Successfully established websocket connection with proxy server: wss://
data.tunneling.iot.us-east-1.amazonaws.com:443
Setting up web socket pings for every 5000 milliseconds
Scheduled next read:

...

Starting web socket read loop continue reading...
Resolved bind IP: 127.0.0.1
Listening for new connection on port 5555
```

Starten einer SSH-Sitzung

Öffnen Sie ein anderes Terminal und verwenden Sie den folgenden Befehl, um eine neue SSH-Sitzung zu starten, indem Sie eine Verbindung zum lokalen Proxy auf Port 5555 herstellen.

```
ssh username@localhost -p 5555
```

Möglicherweise werden Sie zur Eingabe eines Passworts für die SSH-Sitzung aufgefordert. Wenn Sie mit der SSH-Sitzung fertig sind, geben Sie **`exit`** ein, um die Sitzung zu schließen.

Bereinigen

- Tunnel schließen

  Wir empfehlen, den Tunnel zu schließen, wenn Sie ihn nicht mehr verwenden. Ein Tunnel kann auch geschlossen werden, wenn er länger als die angegebene Tunneldauer geöffnet blieb. Ein Tunnel kann nicht wieder geöffnet werden, wenn er einmal geschlossen wurde. Sie können einen

Tunnel trotzdem duplizieren, indem Sie den geschlossenen Tunnel öffnen und dann Tunnel duplizieren auswählen. Geben Sie die Tunneldauer an, die Sie verwenden möchten, und erstellen Sie dann den neuen Tunnel.

- Um einen einzelnen Tunnel oder mehrere Tunnel von der AWS IoT -Konsole aus zu schließen, wechseln Sie zum Tunnel-Hub, wählen Sie die Tunnel aus, die Sie schließen möchten, und wählen Sie dann Tunnel schließen aus.
- Verwenden Sie den API-Vorgang, um einen einzelnen Tunnel oder mehrere Tunnel mithilfe der AWS IoT API-Referenz-API zu schließen. CloseTunnel

```
aws iotsecuretunneling close-tunnel \
    --tunnel-id "01234567-89ab-0123-4c56-789a01234bcd"
```

- Löschen eines Tunnels

  Sie können einen Tunnel dauerhaft aus Ihrem löschen AWS-Konto.

  > **Warning**
  >
  > Dieser Löschvorgang ist dauerhaft und kann nicht rückgängig gemacht werden.

  - Um einen einzelnen Tunnel oder mehrere Tunnel von der AWS IoT -Konsole aus zu löschen, wechseln Sie zum Tunnel-Hub, wählen Sie die Tunnel aus, die Sie löschen möchten, und wählen Sie dann Tunnel löschen aus.
  - Verwenden Sie den API-Vorgang, um einen einzelnen Tunnel oder mehrere Tunnel mithilfe der AWS IoT CloseTunnelAPI-Referenz-API zu löschen. Wenn Sie die API verwenden, setzen Sie das `delete`-Flag auf `true`.

```
aws iotsecuretunneling close-tunnel \
    --tunnel-id "01234567-89ab-0123-4c56-789a01234bcd"
    --delete true
```

## Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen

Von der AWS IoT Konsole aus können Sie einen Tunnel entweder vom Tunnel-Hub oder von der Detailseite eines IoT-Dings aus erstellen, das Sie erstellt haben. Wenn Sie einen Tunnel vom Tunnel-

Hub aus erstellen, können Sie mithilfe von Quick Setup oder der manuellen Einrichtung angeben, ob Sie einen Tunnel erstellen möchten. Ein Tutorial finden Sie unter Öffnen Sie einen Tunnel und starten Sie eine SSH-Sitzung zum Remote-Gerät.

Wenn Sie einen Tunnel auf der Seite mit den Ding-Details der AWS IoT Konsole erstellen, können Sie auch angeben, ob Sie einen neuen Tunnel erstellen oder einen vorhandenen Tunnel für dieses Ding öffnen möchten, wie in diesem Tutorial dargestellt. Wenn Sie einen vorhandenen Tunnel auswählen, können Sie auf den neuesten, offenen Tunnel zugreifen, den Sie für dieses Gerät erstellt haben. Sie können dann die Befehlszeilen-Schnittstelle im Terminal verwenden, um eine SSH-Verbindung zum Gerät herzustellen.

## Voraussetzungen

- Die Firewalls, hinter denen sich das Remote-Gerät befindet, müssen ausgehenden Datenverkehr an Port 443 zulassen. Der Tunnel, den Sie erstellen, verwendet diesen Port, um eine Verbindung zum Remote-Gerät herzustellen.
- Sie haben ein IoT-Ding (zum Beispiel`RemoteDevice1`) in der AWS IoT Registrierung erstellt. Dieses Objekt entspricht der Darstellung Ihres Remote-Geräts in der Cloud. Weitere Informationen finden Sie unter Registrierung eines Geräts in der AWS IoT -Registry.
- Auf dem Remote-Gerät läuft ein IoT-Geräteagent (siehe IoT-Agent-Snippet), der eine Verbindung zum AWS IoT Gerätegateway herstellt und mit einem MQTT-Themenabonnement konfiguriert ist. Weitere Informationen finden Sie unter Ein Gerät mit dem AWS IoT Geräte-Gateway verbinden.
- Auf dem Remote-Gerät muss ein SSH-Daemon ausgeführt werden.

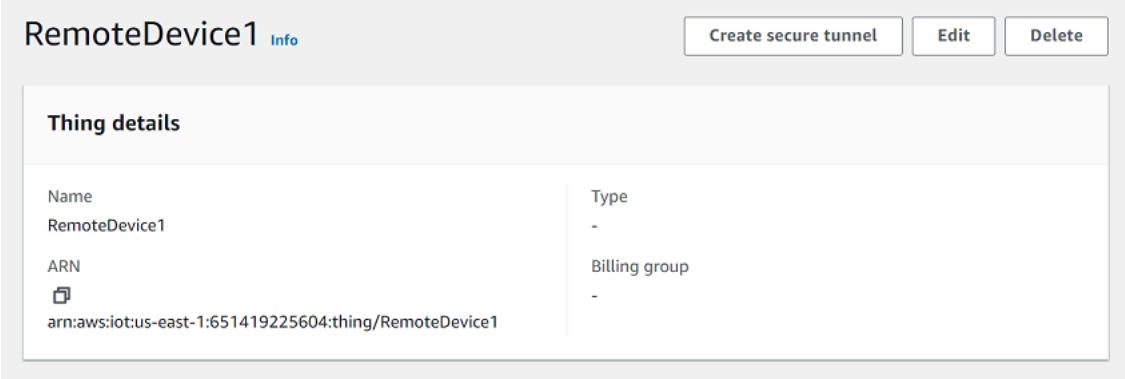
## Öffnen Sie einen neuen Tunnel für das Remote-Gerät

Angenommen, Sie möchten einen Tunnel zu Ihrem Remote-Gerät `RemoteDevice1` öffnen. Erstellen Sie zunächst ein IoT-Objekt mit dem Namen `RemoteDevice1` in der AWS IoT -Registry. Anschließend können Sie einen Tunnel mithilfe der AWS Management Console, der AWS IoT API-Referenz-API oder der erstellen AWS CLI.

Wenn Sie das Ziel beim Erstellen des Tunnels konfigurieren, liefert der Secure Tunneling-Service das Zugriffstoken für den Zielclient über MQTT an das Remote-Gerät und das reservierte MQTT-Thema (`$aws/things/RemoteDeviceA/tunnels/notify`). Weitere Informationen finden Sie unter Methoden zur Tunnelerstellung in der AWS IoT Konsole.

Um von der Konsole aus einen Tunnel für ein Remote-Gerät zu erstellen,

1. Wählen Sie das Objekt `RemoteDevice1` aus, um seine Details anzuzeigen, und wählen Sie dann Sicheren Tunnel erstellen aus.




2. Wählen Sie aus, ob Sie einen neuen Tunnel erstellen oder einen vorhandenen Tunnel öffnen möchten. Um einen neuen Tunnel zu erstellen, wählen Sie Neuen Tunnel erstellen. Sie können die Quick Setup Methode oder die manuelle Einrichtungsmethode verwenden, um einen Tunnel zu erstellen. Weitere Informationen erhalten Sie unter Öffnen Sie mithilfe der manuellen Einrichtung einen Tunnel und stellen Sie eine Verbindung zum Remote-Gerät her und Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen.

So erstellen Sie einen Tunnel für ein Remote-Gerät mithilfe der API

Um einen neuen Tunnel zu öffnen, können Sie den OpenTunnelAPI-Vorgang verwenden. Der folgende Code zeigt ein Beispiel für die Ausführung dieses Befehls.

```
aws iotsecuretunneling open-tunnel \
    --region us-east-1 \
    --endpoint https://api.us-east-1.tunneling.iot.amazonaws.com
    --cli-input-json file://input.json
```

Im Folgenden werden die Inhalte der `input.json`-Datei angezeigt. Sie können den `destinationConfig`-Parameter verwenden, um den Namen des Zielgeräts (z. B. *`RemoteDevice1`*) und den Dienst anzugeben, den Sie für den Zugriff auf das Zielgerät verwenden möchten, z. B. *`SSH`*. Optional können Sie auch zusätzliche Parameter wie die Tunnelbeschreibung und Tags angeben.

Inhalt von input.json

```
{
```

```
   "description": "Tunnel to remote device1",
   "destinationConfig": {
      "services": [ "SSH" ],
      "thingName": "RemoteDevice1"
   }
}
```

Wenn Sie diesen Befehl ausführen, wird ein neuer Tunnel erstellt und Sie erhalten die Quell- und Zielzugriffstoken.

```
{
    "tunnelId": "01234567-89ab-0123-4c56-789a01234bcd",
    "tunnelArn": "arn:aws:iot:us-
east-1:123456789012:tunnel/01234567-89ab-0123-4c56-789a01234bcd",
    "sourceAccessToken": "<SOURCE_ACCESS_TOKEN>",
    "destinationAccessToken": "<DESTINATION_ACCESS_TOKEN>"
}
```

## Öffnen eines vorhandenen Tunnels und Verwenden von browserbasiertem SSH

Angenommen, `RemoteDevice1` Sie haben den Tunnel für Ihr Remote-Gerät mithilfe der manuellen Einrichtungsmethode oder mithilfe der AWS IoT API-Referenz-API erstellt. Sie können dann den vorhandenen Tunnel für das Gerät öffnen und dieQuick Setup Methode wählen, um die browserbasierte SSH-Funktion zu verwenden. Die Konfigurationen eines vorhandenen Tunnels können nicht bearbeitet werden, sodass Sie die manuelle Einrichtungsmethode nicht verwenden können.

Um die browserbasierte SSH-Funktion zu verwenden, müssen Sie weder das Quellzugriffstoken herunterladen noch den lokalen Proxy konfigurieren. Ein webbasierter lokaler Proxy wird automatisch für Sie konfiguriert, sodass Sie mit der Interaktion mit Ihrem Remote-Gerät beginnen können.

So verwenden Sie die Quick Setup Methode und browserbasiertes SSH

1. Gehen Sie zur Detailseite des Objekts `RemoteDevice1`, das Sie erstellt haben, und klicken Sie auf Sicheren Tunnel erstellen.
2. Wählen Sie Bestehenden Tunnel verwenden, um den letzten offenen Tunnel zu öffnen, den Sie für das Remote-Gerät erstellt haben. Die Konfigurationen eines vorhandenen Tunnels können nicht bearbeitet werden, sodass Sie die manuelle Einrichtungsmethode nicht verwenden können. Um die Quick Setup Methode zu verwenden, wählen Sie Schnelle Einrichtung.

3. Überprüfen und bestätigen Sie die Details der Tunnelkonfiguration und erstellen Sie den Tunnel. Die Tunnelkonfigurationen können nicht bearbeitet werden.

   Wenn Sie den Tunnel erstellen, verwendet Secure Tunneling den RotateTunnelAccessTokenAPI-Vorgang, um die ursprünglichen Zugriffstoken zu widerrufen und neue Zugriffstoken zu generieren. Wenn Ihr Remote-Gerät MQTT verwendet, werden diese Token automatisch zu dem MQTT-Thema, das es abonniert hat, an das Remote-Gerät gesendet. Sie können sich auch dafür entscheiden, diese Token manuell auf Ihr Quellgerät herunterzuladen.

Nachdem Sie den Tunnel erstellt haben, können Sie das browserbasierte SSH verwenden, um über die kontextinterne Befehlszeilen-Schnittstelle direkt von der Konsole aus mit dem Remote-Gerät zu interagieren. Um diese Befehlszeilen-Schnittstelle zu verwenden, wählen Sie den Tunnel für das Objekt aus, das Sie erstellt haben, und erweitern Sie auf der Detailseite den Abschnitt Befehlszeilen-Schnittstelle. Da der lokale Proxy bereits für Sie konfiguriert wurde, können Sie mit der Eingabe von Befehlen beginnen, um schnell mit dem Zugriff auf und der Interaktion mit Ihrem Remote-Gerät `RemoteDevice1` zu beginnen.

Weitere Informationen zur Quick Setup Methode und zur Verwendung von browserbasiertem SSH finden Sie unter Öffnen Sie einen Tunnel und verwenden Sie browserbasiertes SSH, um auf das Remote-Gerät zuzugreifen.

## Bereinigen

- Tunnel schließen

  Wir empfehlen, den Tunnel zu schließen, wenn Sie ihn nicht mehr verwenden. Ein Tunnel kann auch geschlossen werden, wenn er länger als die angegebene Tunneldauer geöffnet blieb. Ein Tunnel kann nicht wieder geöffnet werden, wenn er einmal geschlossen wurde. Sie können einen Tunnel trotzdem duplizieren, indem Sie den geschlossenen Tunnel öffnen und dann Tunnel duplizieren auswählen. Geben Sie die Tunneldauer an, die Sie verwenden möchten, und erstellen Sie dann den neuen Tunnel.

  - Um einen einzelnen Tunnel oder mehrere Tunnel von der AWS IoT -Konsole aus zu schließen, wechseln Sie zum Tunnel-Hub, wählen Sie die Tunnel aus, die Sie schließen möchten, und wählen Sie dann Tunnel schließen aus.
  - Verwenden Sie den API-Vorgang, um einen einzelnen Tunnel oder mehrere Tunnel mithilfe der AWS IoT API-Referenz-API zu schließen. CloseTunnel

```
aws iotsecuretunneling close-tunnel \
    --tunnel-id "01234567-89ab-0123-4c56-789a01234bcd"
```

- Löschen eines Tunnels

  Sie können einen Tunnel dauerhaft aus Ihrem löschen AWS-Konto.

  > **Warning**
  >
  > Dieser Löschvorgang ist dauerhaft und kann nicht rückgängig gemacht werden.

  - Um einen einzelnen Tunnel oder mehrere Tunnel von der AWS IoT -Konsole aus zu löschen, wechseln Sie zum Tunnel-Hub, wählen Sie die Tunnel aus, die Sie löschen möchten, und wählen Sie dann Tunnel löschen aus.
  - Verwenden Sie den API-Vorgang, um einen einzelnen Tunnel oder mehrere Tunnel mithilfe der AWS IoT CloseTunnelAPI-Referenz-API zu löschen. Wenn Sie die API verwenden, setzen Sie das `delete`-Flag auf `true`.

    ```
    aws iotsecuretunneling close-tunnel \
        --tunnel-id "01234567-89ab-0123-4c56-789a01234bcd"
        --delete true
    ```

## Lokaler Proxy

Der lokale Proxy überträgt Daten, die von der auf dem Quellgerät ausgeführten Anwendung gesendet werden, mithilfe von sicherem Tunneling über eine WebSocket sichere Verbindung. Sie können die lokale Proxyquelle von herunterladen. GitHub

Der lokale Proxy kann in zwei Modi ausgeführt werden: `source` oder `destination`. Im Quellmodus wird der lokale Proxy auf demselben Gerät oder Netzwerk ausgeführt wie die Clientanwendung, die die TCP-Verbindung initiiert. Im Zielmodus wird der lokale Proxy zusammen mit der Zielanwendung auf dem Remote-Gerät ausgeführt. Ein einzelner Tunnel kann mithilfe von Tunnelmultiplexing bis zu drei Datenströme gleichzeitig unterstützen. Für jeden Datenstrom werden beim Secure Tunneling mehrere TCP-Verbindungen verwendet, wodurch das Risiko eines Timeouts reduziert wird. Weitere Informationen finden Sie unter Multiplex-Datenströme und gleichzeitige Verwendung von TCP-Verbindungen in einem sicheren Tunnel.

# Wie man den lokalen Proxy benutzt

Sie können den lokalen Proxy auf den Quell- und Zielgeräten ausführen, um Daten an die sicheren Tunneling-Endpunkte zu übertragen. Wenn sich Ihre Geräte in einem Netzwerk befinden, das einen Web-Proxy verwendet, kann der Web-Proxy die Verbindungen abfangen, bevor er sie an das Internet weiterleitet. In diesem Fall müssen Sie Ihren lokalen Proxy so konfigurieren, dass er den Web-Proxy verwendet. Weitere Informationen finden Sie unter Konfigurieren Sie den lokalen Proxy für Geräte, die einen Web-Proxy verwenden.

## Workflow des lokalen Proxy

Die folgenden Schritte zeigen, wie der lokale Proxy auf den Quell- und Zielgeräten ausgeführt wird.

1. Lokalen Proxy mit Secure Tunneling verbinden

   Der lokale Proxy stellt zunächst eine Verbindung zum Secure Tunneling her. Wenn Sie den lokalen Proxy starten, verwenden Sie die folgenden Argumente:

   - Das `-r` Argument zur Angabe des, AWS-Region in dem der Tunnel geöffnet wird.
   - Verwenden Sie das `-t`-Argument, um entweder das vom `OpenTunnel` zurückgegebene Quell- oder Zielclient-Zugriffstoken zu übergeben.

   > **Note**
   >
   > Zwei lokale Proxys, die dasselbe Client-Zugriffstoken verwenden, können nicht gleichzeitig verbunden werden.

2. Quell- oder Zielaktionen ausführen

   Nachdem die WebSocket Verbindung hergestellt wurde, führt der lokale Proxy je nach Konfiguration entweder Aktionen im Quellmodus oder im Zielmodus aus.

   Standardmäßig versucht der lokale Proxy, erneut eine Verbindung zum Secure Tunneling herzustellen input/output (I/O (falls Fehler auftreten) oder wenn die WebSocket Verbindung unerwartet geschlossen wird. Dadurch wird die TCP-Verbindung geschlossen. Wenn TCP-Socket-Fehler auftreten, sendet der lokale Proxy eine Nachricht über den Tunnel, um die andere Seite zu benachrichtigen, dass die TCP-Verbindung geschlossen wird. Standardmäßig verwendet der lokale Proxy immer die SSL-Kommunikation.

3. Lokalen Proxy stoppen

Nachdem Sie den Tunnel verwendet haben, ist es sicher, den lokalen Proxyprozess zu stoppen. Wir empfehlen Ihnen, den Tunnel explizit durch Aufrufen von `CloseTunnel` zu schließen. Aktive Tunnelclients werden möglicherweise nicht sofort nach dem Anruf geschlossen. `CloseTunnel`

Weitere Informationen zur Verwendung von zum Öffnen eines Tunnels und AWS Management Console zum Starten einer SSH-Sitzung finden Sie unterÖffnen Sie einen Tunnel und starten Sie eine SSH-Sitzung zum Remote-Gerät.

## Bewährte Methoden des lokalen Proxy

Befolgen Sie beim Ausführen des lokalen Proxy die folgenden bewährten Methoden:

- Vermeiden Sie beim Übergeben von Zugriffstoken die Verwendung des lokalen Proxy-Arguments `-t`. Es wird empfohlen, dass Sie die `AWSIOT_TUNNEL_ACCESS_TOKEN`-Umgebungsvariable verwenden, um das Zugriffstoken für den lokalen Proxy festzulegen.
- Führen Sie die ausführbare Datei des lokalen Proxys mit den geringsten Berechtigungen im Betriebssystem oder in der Umgebung aus.
  - Führen Sie den lokalen Proxy nicht als Administrator unter Windows aus.
  - Führen Sie den lokalen Proxy als Root unter Linux und macOS aus.
- Erwägen Sie, den lokalen Proxy auf separaten Hosts, Containern, Sandboxen, Chroot-Jail oder einer virtualisierten Umgebung auszuführen.
- Erstellen Sie den lokalen Proxy mit relevanten Sicherheits-Flags, abhängig von Ihrer Toolchain.
- Verwenden Sie auf Geräten mit mehreren Netzwerkschnittstellen das `-b`-Argument, um den TCP-Socket an die Netzwerkschnittstelle zu binden, die zur Kommunikation mit der Zielanwendung verwendet wird.

## Beispielbefehl und Ausgabe

Hier ein Beispiel für einen Befehl, den Sie ausführen, und die entsprechende Ausgabe. Das Beispiel zeigt, wie der lokale Proxy sowohl im `source`- als auch im `destination`-Modus konfiguriert werden kann. Der lokale Proxy aktualisiert das HTTPS-Protokoll, WebSockets um eine langlebige Verbindung herzustellen, und beginnt dann mit der Übertragung von Daten über die Verbindung an die Endpunkte der sicheren Tunneling-Geräte.

Bevor Sie diese Befehle ausführen:

Müssen Sie einen Tunnel geöffnet und die Client-Zugriffstoken für die Quelle und das Ziel abgerufen haben. Müssen Sie auch den lokalen Proxy wie zuvor beschrieben erstellt haben. Um den lokalen Proxy zu erstellen, öffnen Sie den lokalen Proxy-Quellcode im GitHub Repository und folgen Sie den Anweisungen zum Erstellen und Installieren des lokalen Proxys.

> **Note**
>
> Die folgenden Befehle, die in den Beispielen verwendet werden, verwenden das `verbosity`-Flag, um einen Überblick über die verschiedenen zuvor beschriebenen Schritte zu veranschaulichen, nachdem Sie den lokalen Proxy ausgeführt haben. Wir empfehlen, dass Sie das Flag nur für Tests verwenden.

Lokalen Proxy im Quellmodus betreiben

Die folgenden Befehle zeigen, wie der lokale Proxy im Quellmodus ausgeführt wird.

Linux/macOS

Führen Sie unter Linux oder macOS die folgenden Befehle im Terminal aus, um den lokalen Proxy auf Ihrer Quelle zu konfigurieren und zu starten.

```
export AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
./localproxy -s 5555 -v 5 -r us-west-2
```

Wobei gilt:

- `-s` ist der Quell-Listen-Port, der den lokalen Proxy im Quellmodus startet.
- `-v` ist die Ausführlichkeit der Ausgabe, die ein Wert zwischen null und dechs sein kann.
- `-r` ist die Endpunktregion, in der der Tunnel geöffnet ist.

Weitere Informationen zu den Parametern finden Sie unter Mit Befehlszeilenargumenten festgelegte Optionen.

Windows

In Windows konfigurieren Sie den lokalen Proxy ähnlich wie für Linux oder macOS, aber die Art und Weise, wie Sie die Umgebungsvariablen definieren, unterscheidet sich von den anderen

Plattformen. Führen Sie die folgenden Befehle im `cmd`-Fenster aus, um den lokalen Proxy auf Ihrer Quelle zu konfigurieren und zu starten.

```
set AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
.\localproxy -s 5555 -v 5 -r us-west-2
```

Wobei gilt:

- `-s` ist der Quell-Listen-Port, der den lokalen Proxy im Quellmodus startet.
- `-v` ist die Ausführlichkeit der Ausgabe, die ein Wert zwischen null und dechs sein kann.
- `-r` ist die Endpunktregion, in der der Tunnel geöffnet ist.

Weitere Informationen zu den Parametern finden Sie unter Mit Befehlszeilenargumenten festgelegte Optionen.

> **Note**
>
> Wenn Sie die neueste Version des lokalen Proxys im Quellmodus verwenden, müssen Sie den AWS CLI Parameter aus Gründen der Abwärtskompatibilität `--destination-client-type V1` auf dem Quellgerät angeben. Dies gilt, wenn Sie eine Verbindung zu einem der folgenden Zielmodi herstellen:
>
> - AWS IoT Geräte-Client
> - AWS IoT Komponente für sicheres Tunneling oder Komponente für AWS IoT Greengrass Version 2 sicheres Tunneling
> - Beliebiger AWS IoT Secure Tunneling-Democode, der vor 2022 geschrieben wurde
> - 1.X-Versionen des lokalen Proxys
>
> Dieser Parameter gewährleistet die korrekte Kommunikation zwischen dem aktualisierten Quell-Proxy und älteren Zielclients. Weitere Informationen zu lokalen Proxyversionen finden Sie unter AWS IoT Secure Tunneling on. GitHub

Im Folgenden finden Sie ein Beispiel für die Ausführung des lokalen Proxys im `source` Modus.

```
...
```

```
...

Starting proxy in source mode
Attempting to establish web socket connection with endpoint wss://
data.tunneling.iot.us-west-2.amazonaws.com:443
Resolved proxy  server IP: 10.10.0.11
Connected successfully with proxy server
Performing SSL handshake with proxy server
Successfully completed SSL handshake with proxy server
HTTP/1.1 101 Switching Protocols

...

Connection: upgrade
channel-id: 01234567890abc23-00001234-0005678a-b1234c5de677a001-2bc3d456
upgrade: websocket

...

Web socket session ID: 01234567890abc23-00001234-0005678a-b1234c5de677a001-2bc3d456
Web socket subprotocol selected: aws.iot.securetunneling-2.0
Successfully established websocket connection with proxy server: wss://
data.tunneling.iot.us-west-2.amazonaws.com:443
Setting up web socket pings for every 5000 milliseconds
Scheduled next read:

...

Starting web socket read loop continue reading...
Resolved bind IP: 127.0.0.1
Listening for new connection on port 5555
```

Lokalen Proxy im Zielmodus betreiben

Die folgenden Befehle zeigen, wie der lokale Proxy im Zielmodus ausgeführt wird.

Linux/macOS

Führen Sie unter Linux oder macOS die folgenden Befehle im Terminal aus, um den lokalen Proxy auf Ihrem Ziel zu konfigurieren und zu starten.

```
export AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
./localproxy -d 22 -v 5 -r us-west-2
```

Wobei gilt:

- `-d` ist die Zielanwendung, die den lokalen Proxy im Zielmodus startet.
- `-v` ist die Ausführlichkeit der Ausgabe, die ein Wert zwischen null und dechs sein kann.
- `-r` ist die Endpunktregion, in der der Tunnel geöffnet ist.

Weitere Informationen zu den Parametern finden Sie unter Mit Befehlszeilenargumenten festgelegte Optionen.

Windows

In Windows konfigurieren Sie den lokalen Proxy ähnlich wie für Linux oder macOS, aber die Art und Weise, wie Sie die Umgebungsvariablen definieren, unterscheidet sich von den anderen Plattformen. Führen Sie die folgenden Befehle im `cmd`-Fenster aus, um den lokalen Proxy auf Ihrem Ziel zu konfigurieren und zu starten.

```
set AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
.\localproxy -d 22 -v 5 -r us-west-2
```

Wobei gilt:

- `-d` ist die Zielanwendung, die den lokalen Proxy im Zielmodus startet.
- `-v` ist die Ausführlichkeit der Ausgabe, die ein Wert zwischen null und dechs sein kann.
- `-r` ist die Endpunktregion, in der der Tunnel geöffnet ist.

Weitere Informationen zu den Parametern finden Sie unter Mit Befehlszeilenargumenten festgelegte Optionen.

> **Note**
>
> Wenn Sie die neueste Version des lokalen Proxys im Zielmodus verwenden, müssen Sie den AWS CLI Parameter aus Gründen der Abwärtskompatibilität `--destination-client-type V1` auf dem Zielgerät angeben. Dies gilt, wenn Sie eine Verbindung zu einem der folgenden Quellmodi herstellen:
>
> - Browserbasiertes Secure Tunneling von der Konsole aus. AWS
> - 1.X-Versionen des lokalen Proxys

Dieser Parameter gewährleistet die korrekte Kommunikation zwischen dem aktualisierten Ziel-Proxy und älteren Quellclients. Weitere Informationen zu lokalen Proxyversionen finden Sie unter AWS IoT Secure Tunneling on. GitHub

Im Folgenden finden Sie ein Beispiel für die Ausführung des lokalen Proxys im `destination` Modus.

```
...
...

Starting proxy in destination mode
Attempting to establish web socket connection with endpoint wss://
data.tunneling.iot.us-west-2.amazonaws.com:443
Resolved proxy  server IP: 10.10.0.11
Connected successfully with proxy server
Performing SSL handshake with proxy server
Successfully completed SSL handshake with proxy server
HTTP/1.1 101 Switching Protocols

...

Connection: upgrade
channel-id: 01234567890abc23-00001234-0005678a-b1234c5de677a001-2bc3d456
upgrade: websocket

...

Web socket session ID: 01234567890abc23-00001234-0005678a-b1234c5de677a001-2bc3d456
Web socket subprotocol selected: aws.iot.securetunneling-2.0
Successfully established websocket connection with proxy server: wss://
data.tunneling.iot.us-west-2.amazonaws.com:443
Setting up web socket pings for every 5000 milliseconds
Scheduled next read:

...

Starting web socket read loop continue reading...
```

# Konfigurieren Sie den lokalen Proxy für Geräte, die einen Web-Proxy verwenden

Sie können den lokalen Proxy auf AWS IoT Geräten verwenden, um mit AWS IoT Secure APIs Tunneling zu kommunizieren. Der lokale Proxy überträgt Daten, die von der Geräteanwendung gesendet werden, mithilfe von sicherem Tunneling über eine sichere Verbindung. WebSocket Der lokale Proxy kann im Modus `source` oder `destination` arbeiten. Im `source`-Modus läuft er auf demselben Gerät oder Netzwerk, das die TCP-Verbindung initiiert. Im `destination`-Modus wird der lokale Proxy zusammen mit der Zielanwendung auf dem Remote-Gerät ausgeführt. Weitere Informationen finden Sie unter Lokaler Proxy.

Der lokale Proxy muss eine direkte Verbindung zum Internet herstellen, um AWS IoT sicheres Tunneling verwenden zu können. Für eine langlebige TCP-Verbindung mit sicherem Tunneling aktualisiert der lokale Proxy die HTTPS-Anfrage, um eine Verbindung zu einem der WebSockets Verbindungsendpunkte für sichere Tunnelgeräte herzustellen.

Wenn sich Ihre Geräte in einem Netzwerk befinden, das einen Web-Proxy verwendet, kann der Web-Proxy die Verbindungen abfangen, bevor er sie an das Internet weiterleitet. Um eine dauerhafte Verbindung zu den Verbindungsendpunkten für Secure Tunneling-Geräte herzustellen, konfigurieren Sie Ihren lokalen Proxy so, dass er den Web-Proxy verwendet, wie in der Websocket-Spezifikation beschrieben.

> **Note**
>
> AWS IoT Geräteclient unterstützt keine Geräte, die einen Web-Proxy verwenden. Um mit dem Web-Proxy arbeiten zu können, müssen Sie einen lokalen Proxy verwenden und ihn so konfigurieren, dass er mit einem Web-Proxy funktioniert, wie unten beschrieben.

Die folgenden Schritte zeigen, wie der lokale Proxy mit einem Web-Proxy funktioniert.

1. Der lokale Proxy sendet eine HTTP `CONNECT`-Anfrage an den Web-Proxy, die die Remote-Adresse des Secure Tunneling-Service zusammen mit den Authentifizierungsinformationen für den Web-Proxy enthält.
2. Der Web-Proxy stellt dann eine langlebige Verbindung zu den Remote-Secure-Tunneling-Endpunkten her.
3. Die TCP-Verbindung ist hergestellt und der lokale Proxy funktioniert jetzt sowohl im Quell- als auch im Zielmodus für die Datenübertragung.

Führen Sie die folgenden Schritte aus, um dieses Verfahren abzuschließen.

- Erstellen Sie den lokalen Proxy
- Konfigurieren Sie Ihren Web-Proxy
- Konfigurieren und Starten des lokalen Proxys

## Erstellen Sie den lokalen Proxy

Öffnen Sie den lokalen Proxy-Quellcode im GitHub Repository und folgen Sie den Anweisungen zum Erstellen und Installieren des lokalen Proxys.

## Konfigurieren Sie Ihren Web-Proxy

Der lokale Proxy basiert auf dem HTTP-Tunneling-Mechanismus, der in der HTTP/1.1-Spezifikation beschrieben wird. Um den Spezifikationen zu entsprechen, muss Ihr Web-Proxy Geräten die Verwendung der `CONNECT`Methode ermöglichen.

Wie Sie Ihren Web-Proxy konfigurieren, hängt von dem von Ihnen verwendeten Web-Proxy und der Web-Proxy-Version ab. Um die korrekte Konfiguration des Web-Proxys sicherzustellen, lesen Sie die Anleitung Ihres Web-Proxys.

Zur Konfiguration Ihres Web-Proxys müssen Sie zunächst die URL Ihres Web-Proxys ermitteln und prüfen, ob Ihr Web-Proxy HTTP-Tunneling unterstützt. Die URL des Web-Proxys wird später verwendet, wenn Sie den lokalen Proxy konfigurieren und starten.

1. Identifizieren Sie Ihre URL des Web-Proxys

   Ihre URL für den Web-Proxy hat das folgende Format.

   ```
   protocol://web_proxy_host_domain:web_proxy_port
   ```

   AWS IoT Secure Tunneling unterstützt nur die Standardauthentifizierung für Web-Proxy. Um die Standardauthentifizierung zu verwenden, müssen Sie das **`username`** und **`password`** als Teil der URL des Web-Proxys angeben. Die URL für den Web-Proxy hat das folgende Format.

   ```
   protocol://username:password@web_proxy_host_domain:web_proxy_port
   ```

   - *`protocol`*kann oder sein. `http` `https` Wir empfehlen Ihnen, `https` zu verwenden.

- *web_proxy_host_domain*ist die IP-Adresse Ihres Webproxys oder ein DNS-Name, der in die IP-Adresse Ihres Webproxys aufgelöst wird.
- *web_proxy_port*ist der Port, auf dem der Web-Proxy lauscht.
- Der Web-Proxy verwendet dies **`username`** und **`password`**, um die Anfrage zu authentifizieren.

2. URL des Web-Proxys testen

   Um zu überprüfen, ob Ihr Web-Proxy TCP-Tunneling unterstützt, verwenden Sie einen `curl` Befehl und stellen Sie sicher, dass Sie eine Antwort `2xx` oder `3xx` erhalten.

   Wenn Ihre URL für den Web-Proxy beispielsweise lautet `https://server.com:1235`, verwenden Sie ein `proxy-insecure` Flag zusammen mit dem `curl` Befehl, da der Web-Proxy möglicherweise auf einem selbstsignierten Zertifikat basiert.

```
export HTTPS_PROXY=https://server.com:1235
curl -I https://aws.amazon.com --proxy-insecure
```

   Wenn Ihre URL für den Web-Proxy einen `http`-Port hat (z. B.`http://server.com:1234`), müssen Sie das `proxy-insecure`-Flag nicht verwenden.

```
export HTTPS_PROXY=http://server.com:1234
curl -I https://aws.amazon.com
```

## Konfigurieren und Starten des lokalen Proxys

Um den lokalen Proxy für die Verwendung eines Web-Proxys zu konfigurieren, müssen Sie die `HTTPS_PROXY` Umgebungsvariable entweder mit den DNS-Domain-Namen oder den IP-Adressen und Portnummern konfigurieren, die Ihr Web-Proxy verwendet.

Nachdem Sie den lokalen Proxy konfiguriert haben, können Sie den lokalen Proxy verwenden, wie in diesem README-Dokument beschrieben.

> **Note**
>
> Bei der Deklaration Ihrer Umgebungsvariablen wird die Groß-/Kleinschreibung beachtet. Wir empfehlen, jede Variable einmal zu definieren, indem Sie entweder nur Groß- oder Kleinbuchstaben verwenden. In den folgenden Beispielen wird die Umgebungsvariable

in Großbuchstaben angegeben. Wenn dieselbe Variable sowohl in Groß- als auch in Kleinbuchstaben angegeben wird, hat die in Kleinbuchstaben angegebene Variable Vorrang.

Die folgenden Befehle zeigen, wie Sie den lokalen Proxy, der auf Ihrem Ziel ausgeführt wird, so konfigurieren, dass er den Web-Proxy verwendet und den lokalen Proxy startet.

- `AWSIOT_TUNNEL_ACCESS_TOKEN`: Diese Variable enthält das Client-Zugriffstoken (CAT) für das Ziel.
- `HTTPS_PROXY`: Diese Variable enthält die URL des Web-Proxys oder die IP-Adresse für die Konfiguration des lokalen Proxys.

Die in den folgenden Beispielen gezeigten Befehle hängen vom verwendeten Betriebssystem ab und davon, ob der Web-Proxy einen HTTP- oder einen HTTPS-Port abhört.

Der Web-Proxy überwacht einen HTTP-Port

Wenn Ihr Web-Proxy einen HTTP-Port abhört, können Sie die URL des Web-Proxys oder IP-Adresse für die `HTTPS_PROXY` Variable angeben.

Linux/macOS

In Linux oder macOS führen Sie die folgenden Befehle im Terminal aus, um den lokalen Proxy auf Ihrem Ziel zu konfigurieren und zu starten, um einen Web-Proxy zu verwenden, der einen HTTP-Port abhört.

```
export AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
export HTTPS_PROXY=http:proxy.example.com:1234
./localproxy -r us-east-1 -d 22
```

Wenn Sie sich beim Proxy authentifizieren müssen, müssen Sie ein **`username`** und **`password`** als Teil der `HTTPS_PROXY`-Variablen angeben.

```
export AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
export HTTPS_PROXY=http://username:password@proxy.example.com:1234
./localproxy -r us-east-1 -d 22
```

Windows

In Windows konfigurieren Sie den lokalen Proxy ähnlich wie für Linux oder macOS, aber die Art und Weise, wie Sie die Umgebungsvariablen definieren, unterscheidet sich von den anderen Plattformen. Führen Sie die folgenden Befehle im cmd-Fenster aus, um den lokalen Proxy auf Ihrem Ziel so zu konfigurieren und zu starten, dass er einen Web-Proxy verwendet, der einen HTTP-Port abhört.

```
set AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
set HTTPS_PROXY=http://proxy.example.com:1234
.\localproxy -r us-east-1 -d 22
```

Wenn Sie sich beim Proxy authentifizieren müssen, müssen Sie ein **`username`** und **`password`** als Teil der HTTPS_PROXY-Variablen angeben.

```
set AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
set HTTPS_PROXY=http://username:password@10.15.20.25:1234
.\localproxy -r us-east-1 -d 22
```

Der Web-Proxy überwacht einen HTTPS-Port

Führen Sie die folgenden Befehle aus, wenn Ihr Web-Proxy einen HTTPS-Port abhört.

> **Note**
>
> Wenn Sie ein selbstsigniertes Zertifikat für den Web-Proxy verwenden oder wenn Sie den lokalen Proxy auf einem Betriebssystem ausführen, das keine native OpenSSL-Unterstützung und keine Standardkonfigurationen bietet, müssen Sie Ihre Web-Proxyzertifikate wie im Abschnitt Zertifikatseinrichtung im Repository beschrieben einrichten. GitHub

Die folgenden Befehle ähneln der Konfiguration Ihres Web-Proxys für einen HTTP-Proxy, mit der Ausnahme, dass Sie auch den Pfad zu den Zertifikatsdateien angeben, die Sie wie zuvor beschrieben installiert haben.

Linux/macOS

In Linux oder macOS führen Sie die folgenden Befehle im Terminal aus, um den lokalen Proxy auf Ihrem Ziel zu konfigurieren, um einen Web-Proxy zu verwenden, der einen HTTPS-Port abhört.

```
export AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
export HTTPS_PROXY=http:proxy.example.com:1234
./localproxy -r us-east-1 -d 22 -c /path/to/certs
```

Wenn Sie sich beim Proxy authentifizieren müssen, müssen Sie ein **`username`** und **`password`** als Teil der `HTTPS_PROXY`-Variablen angeben.

```
export AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
export HTTPS_PROXY=http://username:password@proxy.example.com:1234
./localproxy -r us-east-1 -d 22 -c /path/to/certs
```

Windows

In Windows führen Sie die folgenden Befehle im `cmd`-Fenster aus, um den lokalen Proxy auf Ihrem Ziel so zu konfigurieren und zu starten, dass er einen Web-Proxy verwendet, der einen HTTP-Port abhört.

```
set AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
set HTTPS_PROXY=http://proxy.example.com:1234
.\localproxy -r us-east-1 -d 22 -c \path\to\certs
```

Wenn Sie sich beim Proxy authentifizieren müssen, müssen Sie ein **`username`** und **`password`** als Teil der `HTTPS_PROXY`-Variablen angeben.

```
set AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
set HTTPS_PROXY=http://username:password@10.15.20.25:1234
.\localproxy -r us-east-1 -d 22 -c \path\to\certs
```

Beispielbefehl und Ausgabe

Das Folgende zeigt ein Beispiel für einen Befehl, den Sie auf einem Linux OS ausführen, und die entsprechende Ausgabe. Das Beispiel zeigt einen Web-Proxy, der einen HTTP-Port abhört, und wie der lokale Proxy so konfiguriert werden kann, dass er den Web-Proxy in beiden `source` `destination` Modi verwendet. Bevor Sie diese Befehle ausführen können, müssen Sie bereits einen Tunnel geöffnet und die Client-Zugriffstoken für die Quelle und das Ziel erhalten haben. Sie müssen auch den lokalen Proxy erstellt und Ihren Web-Proxy wie zuvor beschrieben konfiguriert haben.

Hier ist eine Übersicht über die Schritte, nachdem Sie den lokalen Proxy gestartet haben. Der lokale Proxy:

- Identifiziert die URL des Web-Proxys, so dass er die URL zur Verbindung mit dem Proxy-Server verwenden kann.
- Stellt eine TCP-Verbindung mit dem Web-Proxy her.
- Sendet eine `CONNECT` HTTP-Anfrage an den Web-Proxy und wartet auf die `HTTP/1.1 200`-Antwort, die darauf hinweist, dass die Verbindung hergestellt wurde.
- Führt ein Upgrade des HTTPS-Protokolls auf durch WebSockets , um eine langlebige Verbindung herzustellen.
- Beginnt mit der Übertragung von Daten über die Verbindung zu den Endpunkten der Secure-Tunneling-Geräte.

> **Note**
>
> Die folgenden Befehle, die in den Beispielen verwendet werden, verwenden das `verbosity`-Flag, um einen Überblick über die verschiedenen zuvor beschriebenen Schritte zu veranschaulichen, nachdem Sie den lokalen Proxy ausgeführt haben. Wir empfehlen, dass Sie das Flag nur für Tests verwenden.

Lokalen Proxy im Quellmodus betreiben

Die folgenden Befehle veranschaulichen die Ausführung des lokalen Proxys im Quellmodus.

```
export AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
export HTTPS_PROXY=http:username:password@10.15.10.25:1234
./localproxy -s 5555 -v 5 -r us-west-2
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe der Ausführung des lokalen Proxys im `source`-Modus.

```
...

Parsed basic auth credentials for the URL
Found Web proxy information in the environment variables, will use it to connect via
 the proxy.
```

```
...

Starting proxy in source mode
Attempting to establish web socket connection with endpoint wss://
data.tunneling.iot.us-west-2.amazonaws.com:443
Resolved Web proxy IP: 10.10.0.11
Connected successfully with Web Proxy
Successfully sent HTTP CONNECT to the Web proxy
Full response from the Web proxy:
HTTP/1.1 200 Connection established
TCP tunnel established successfully
Connected successfully with proxy server
Successfully completed SSL handshake with proxy server
Web socket session ID: 0a109afffee745f5-00001341-000b8138-cc6c878d80e8adb0-f186064b
Web socket subprotocol selected: aws.iot.securetunneling-2.0
Successfully established websocket connection with proxy server: wss://
data.tunneling.iot.us-west-2.amazonaws.com:443
Seting up web socket pings for every 5000 milliseconds
Scheduled next read:

...

Starting web socket read loop continue reading...
Resolved bind IP: 127.0.0.1
Listening for new connection on port 5555
```

Lokalen Proxy im Zielmodus betreiben

Die folgenden Befehle veranschaulichen die Ausführung des lokalen Proxys im Zielmodus.

```
export AWSIOT_TUNNEL_ACCESS_TOKEN=${access_token}
export HTTPS_PROXY=http:username:password@10.15.10.25:1234
./localproxy -d 22 -v 5 -r us-west-2
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe der Ausführung des lokalen Proxys im `destination`-Modus.

```
...

Parsed basic auth credentials for the URL
Found Web proxy information in the environment variables, will use it to connect via
 the proxy.
```

```
...

Starting proxy in destination mode
Attempting to establish web socket connection with endpoint wss://
data.tunneling.iot.us-west-2.amazonaws.com:443
Resolved Web proxy IP: 10.10.0.1
Connected successfully with Web Proxy
Successfully sent HTTP CONNECT to the Web proxy
Full response from the Web proxy:
HTTP/1.1 200 Connection established
TCP tunnel established successfully
Connected successfully with proxy server
Successfully completed SSL handshake with proxy server
Web socket session ID: 06717bfffed3fd05-00001355-000b8315-da3109a85da804dd-24c3d10d
Web socket subprotocol selected: aws.iot.securetunneling-2.0
Successfully established websocket connection with proxy server: wss://
data.tunneling.iot.us-west-2.amazonaws.com:443
Seting up web socket pings for every 5000 milliseconds
Scheduled next read:

...

Starting web socket read loop continue reading...
```

# Multiplex-Datenströme und gleichzeitige Verwendung von TCP-Verbindungen in einem sicheren Tunnel

Mithilfe der Multiplexing-Funktion für Secure Tunneling können Sie mehrere Datenströme pro Tunnel verwenden. Mit Multiplexing können Sie Fehler bei Geräten beheben, die mehrere Datenströme verwenden. Sie können auch Ihre Betriebslast reduzieren, indem Sie nicht mehr mehrere lokale Proxys erstellen, bereitstellen und starten oder mehrere Tunnel zum selben Gerät öffnen müssen. Multiplexing kann beispielsweise für einen Webbrowser verwendet werden, der das Senden mehrerer HTTP- und SSH-Datenströme erfordert.

AWS IoT Sicheres Tunneling unterstützt für jeden Datenstrom gleichzeitige TCP-Verbindungen. Durch die Verwendung gleichzeitiger Verbindungen wird das Risiko eines Timeouts bei mehreren Anfragen vom Client verringert. So kann beispielsweise die Ladezeit beim Fernzugriff auf einen Webserver reduziert werden, der sich lokal auf dem Zielgerät befindet.

In den folgenden Abschnitten werden weitere Informationen zum Multiplexing und zur Verwendung gleichzeitiger TCP-Verbindungen sowie deren verschiedenen Anwendungsfälle erläutert.

Themen

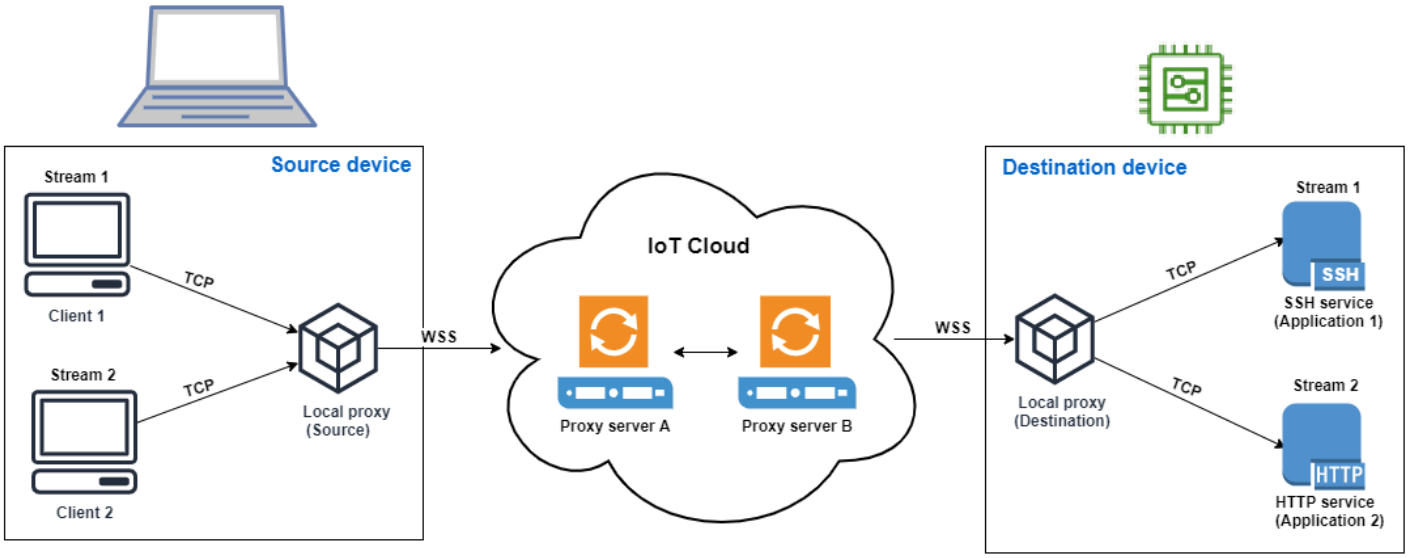

- Multiplexing mehrerer Datenströme in einem sicheren Tunnel
- Gleichzeitige TCP-Verbindungen in einem sicheren Tunnel verwenden


# Multiplexing mehrerer Datenströme in einem sicheren Tunnel

Sie können die Multiplexing-Funktion für Geräte verwenden, die mehrere Verbindungen oder Anschlüsse verwenden. Multiplexing kann auch verwendet werden, wenn Sie mehrere Verbindungen zu einem Remote-Gerät zur Behebung von Fehlern benötigen. Es kann beispielsweise für einen Webbrowser verwendet werden, der das Senden mehrerer HTTP- und SSH-Datenströme erfordert. Die Anwendungsdaten aus beiden Streams werden gleichzeitig über den Multiplex-Tunnel an das Gerät gesendet.

## Beispielanwendungsfall

Sagen wir, Sie müssen eine Verbindung zu einer geräteinternen Webanwendung zum Ändern einiger Netzwerkparameter herstellen und gleichzeitig Shell-Befehle über das Terminal eingeben, um die ordnungsgemäße Funktion des Geräts mit den neuen Netzwerkparametern zu überprüfen. In diesem Szenario müssen Sie möglicherweise sowohl über HTTP als auch über SSH eine Verbindung zum Gerät herstellen und zwei parallel Datenströme übertragen, um gleichzeitig auf die Webanwendung und das Terminal zuzugreifen. Mit der Multiplexing-Funktion können diese beiden unabhängigen Ströme gleichzeitig über denselben Tunnel übertragen werden.




## Wie man einen Multiplex-Tunnel einrichtet

Das folgende Verfahren führt Sie durch die Einrichtung eines Multiplex-Tunnels zur Fehlerbehebung bei Geräten mithilfe von Anwendungen, für die Verbindungen zu mehreren Ports erforderlich sind. Sie werden einen Tunnel mit zwei Multiplex-Streams einrichten: einen HTTP-Stream und einen SSH-Stream.

1. (Optional) Konfigurationsdateien erstellen

   Sie können das Quell- und Zielgerät optional mit Konfigurationsdateien konfigurieren. Verwenden Sie Konfigurationsdateien, wenn sich Ihre Portzuordnungen wahrscheinlich häufig ändern. Sie können diesen Schritt überspringen, wenn Sie die Portzuordnung lieber explizit über die CLI angeben möchten oder wenn Sie den lokalen Proxy nicht auf bestimmten Abhörports starten müssen. Weitere Informationen zur Verwendung von Konfigurationsdateien finden Sie unter Über --config festgelegte Optionen in GitHub.

   1. Erstellen Sie auf Ihrem Quellgerät in dem Ordner, in dem Ihr lokaler Proxy ausgeführt wird, einen Konfigurationsordner mit dem Namen`Config`. Erstellen Sie in diesem Ordner eine Datei mit dem Namen `SSHSource.ini` und dem folgenden Inhalt:

      ```
      HTTP1 = 5555
      SSH1 = 3333
      ```

2. Erstellen Sie auf Ihrem Zielgerät in dem Ordner, in dem Ihr lokaler Proxy ausgeführt wird, einen Konfigurationsordner mit dem Namen`Config`. Erstellen Sie in diesem Ordner eine Datei mit dem Namen `SSHDestination.ini` und dem folgenden Inhalt:

```
HTTP1 = 80
SSH1 = 22
```

2. Tunnel öffnen

Öffnen Sie einen Tunnel mit der `OpenTunnel` API-Funktion oder dem `open-tunnel` CLI-Befehl. Konfigurieren Sie das Ziel, indem Sie `SSH1` und `HTTP1` als Dienste und den Namen der AWS IoT Sache angeben, die Ihrem Remote-Gerät entspricht. Ihre SSH- und HTTP-Anwendungen werden auf diesem Remote-Gerät ausgeführt. Sie müssen das IoT-Ding bereits in der AWS IoT Registrierung erstellt haben. Weitere Informationen finden Sie unter Dinge mit der Registrierung verwalten.

```
aws iotsecuretunneling open-tunnel \
 --destination-config thingName=RemoteDevice1,services=HTTP1,SSH1
```

Wenn Sie diesen Befehl ausführen, werden die Quell- und Zielzugriffstoken generiert, mit denen Sie den lokalen Proxy ausführen.

```
{
 "tunnelId": "b2de92a3-b8ff-46c0-b0f2-afa28b00cecd",
 "tunnelArn": "arn:aws:iot:us-west-2:431600097591:tunnel/b2de92a3-b8ff-46c0-b0f2-
afa28b00cecd",
 "sourceAccessToken": source_client_access_token,
 "destinationAccessToken": destination_client_access_token
}
```

3. Konfigurieren und Starten des lokalen Proxys

Bevor Sie den lokalen Proxy ausführen können, müssen Sie entweder den AWS IoT Geräteclient einrichten oder den lokalen Proxy-Quellcode von der Plattform Ihrer Wahl herunterladen GitHubund ihn für die Plattform Ihrer Wahl erstellen. Anschließend können Sie das Ziel und den lokalen Quell-Proxy starten, um eine Verbindung zum sicheren Tunnel herzustellen. Weitere Informationen zum Konfigurieren und Verwenden des lokalen Proxys finden Sie unter Wie man den lokalen Proxy benutzt.

> **Note**
>
> Wenn Sie auf Ihrem Quellgerät keine Konfigurationsdateien verwenden oder die Portzuordnung mit der CLI angeben, können Sie trotzdem denselben Befehl verwenden, um den lokalen Proxy auszuführen. Der lokale Proxy im Quellmodus wählt automatisch die zu verwendenden Ports und deren Zuordnungen für Sie aus.

Start local proxy using configuration files

Führen Sie die folgenden Befehle aus, um den lokalen Proxy mithilfe von Konfigurationsdateien im Quell- und Zielmodus auszuführen.

```
// ----------------- Start the destination local proxy ----------------------
./localproxy -r us-east-1 -m dst -t destination_client_access_token

// ----------------- Start the source local proxy ---------------------------
// You also run the same command below if you want the local proxy to
// choose the mappings for you instead of using configuration files.
./localproxy -r us-east-1 -m src -t source_client_access_token
```

Start local proxy using CLI port mapping

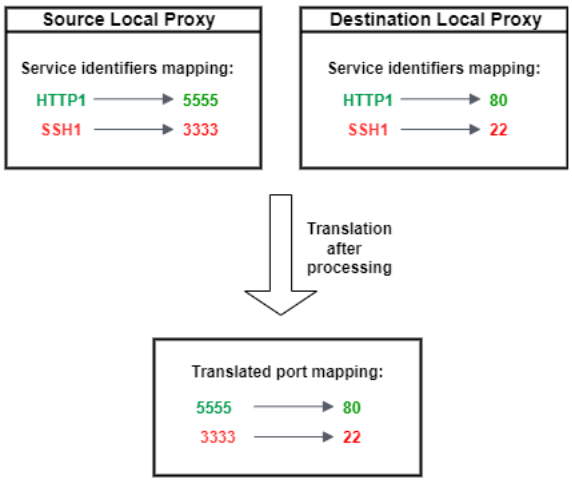
Führen Sie die folgenden Befehle aus, um den lokalen Proxy im Quell- und Zielmodus auszuführen, indem Sie die Portzuordnungen explizit mit der CLI angeben.

```
// ----------------- Start the destination local proxy
 ----------------------------------
./localproxy -r us-east-1 -d HTTP1=80,SSH1=22 -t destination_client_access_token

// ----------------- Start the source local proxy
 ---------------------------------------
./localproxy -r us-east-1 -s HTTP1=5555,SSH1=33 -t source_client_access_token
```

Die Anwendungsdaten aus der SSH- und HTTP-Verbindung können jetzt gleichzeitig über den Multiplex-Tunnel übertragen werden. Wie in der Abbildung unten zu sehen ist, dient die Service-ID als lesbares Format zur Übersetzung der Portzuweisung zwischen dem Quell- und dem Zielgerät. Bei dieser Konfiguration leitet sicheres Tunneling jeglichen eingehenden HTTP-Verkehr von Port *5555*

auf dem Quellgerät an Port *80* auf dem Zielgerät und jeglichen eingehenden SSH-Verkehr von Port *3333* zu Port *22* auf dem Zielgerät weiter.




## Gleichzeitige TCP-Verbindungen in einem sicheren Tunnel verwenden

AWS IoT Secure Tunneling unterstützt mehr als eine TCP-Verbindung gleichzeitig für jeden Datenstrom. Sie können diese Funktion verwenden, wenn Sie gleichzeitige Verbindungen zu einem Remote-Gerät benötigen. Durch die Verwendung gleichzeitiger TCP-Verbindungen wird das Risiko eines Timeouts bei mehreren Anfragen vom Client verringert. Wenn Sie beispielsweise auf einen Webserver zugreifen, auf dem mehrere Komponenten ausgeführt werden, können gleichzeitige TCP-Verbindungen die Zeit reduzieren, die zum Laden der Seite benötigt wird.

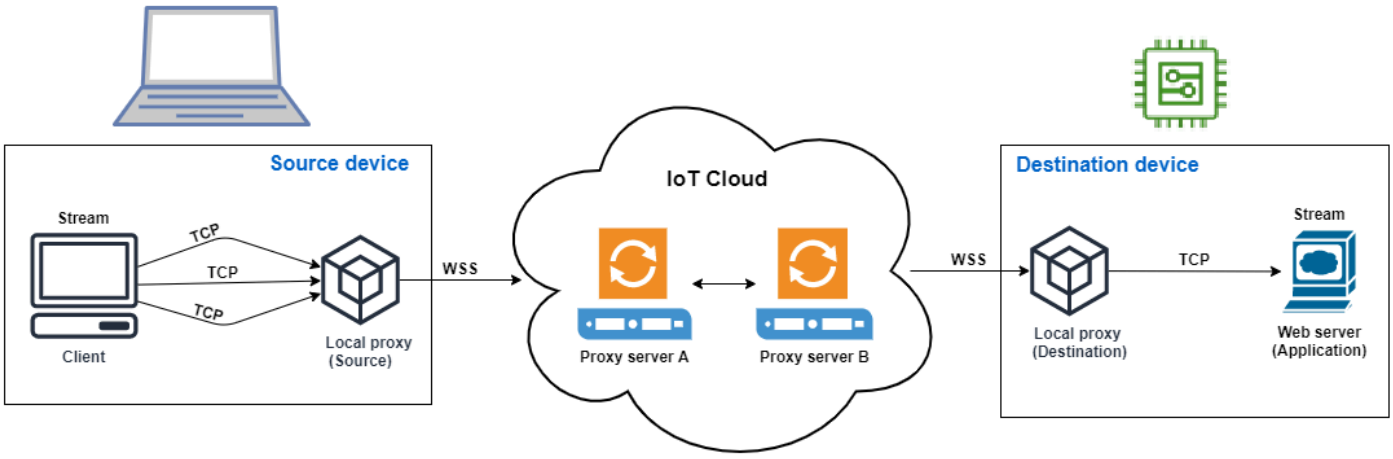
> **Note**
>
> Gleichzeitige TCP-Verbindungen haben eine Bandbreitenbeschränkung von jeweils 800 Kilobyte pro Sekunde. AWS-Konto AWS IoT Secure Tunneling kann dieses Limit je nach Anzahl der eingehenden Anfragen für Sie konfigurieren.

### Beispielanwendungsfall

Nehmen wir an, Sie müssen aus der Ferne auf einen Webserver zugreifen, der sich lokal auf dem Zielgerät befindet und auf dem mehrere Komponenten laufen. Bei einer einzigen TCP-Verbindung kann das sequenzielle Laden beim Zugriff auf den Webserver die Zeit verlängern, die zum Laden der Ressourcen auf der Seite benötigt wird. Die gleichzeitigen TCP-Verbindungen können die Ladezeit reduzieren, indem sie die Ressourcenanforderungen der Seite erfüllen, wodurch die Zugriffszeit reduziert wird. Das folgende Diagramm zeigt, wie gleichzeitige TCP-Verbindungen für den

Datenstrom zur Webserver-Anwendung unterstützt werden, die auf dem Remote-Gerät ausgeführt wird.

> **Note**
>
> Wenn Sie über den Tunnel auf mehrere Anwendungen zugreifen möchten, die auf dem Remote-Gerät ausgeführt werden, können Sie Tunnelmultiplexing verwenden. Weitere Informationen finden Sie unter Multiplexing mehrerer Datenströme in einem sicheren Tunnel.




## Wie verwendet man gleichzeitige TCP-Verbindungen

Im folgenden Verfahren wird beschrieben, wie Sie gleichzeitige TCP-Verbindungen für den Zugriff auf den Webbrowser auf dem entfernten Gerät verwenden können. Wenn mehrere Anfragen vom Client eingehen, richtet AWS IoT Secure Tunneling automatisch gleichzeitige TCP-Verbindungen ein, um die Anfragen zu bearbeiten, wodurch die Ladezeit reduziert wird.

1. Tunnel öffnen

   Öffnen Sie einen Tunnel mit der `OpenTunnel` API-Funktion oder dem `open-tunnel` CLI-Befehl. Konfigurieren Sie das Ziel, indem Sie `HTTP` als Dienst und den Namen des Objekts AWS IoT angeben, das Ihrem Remote-Gerät entspricht. Ihre Webserver-Anwendung wird auf diesem Remote-Gerät ausgeführt. Sie müssen das IoT-Ding bereits in der AWS IoT Registrierung erstellt haben. Weitere Informationen finden Sie unter Dinge mit der Registrierung verwalten.

   ```
   aws iotsecuretunneling open-tunnel \
   ```

```
 --destination-config thingName=RemoteDevice1,services=HTTP
```

Wenn Sie diesen Befehl ausführen, werden die Quell- und Zielzugriffstoken generiert, mit denen Sie den lokalen Proxy ausführen.

```
{
 "tunnelId": "b2de92a3-b8ff-46c0-b0f2-afa28b00cecd",
 "tunnelArn": "arn:aws:iot:us-west-2:431600097591:tunnel/b2de92a3-b8ff-46c0-b0f2-
afa28b00cecd",
 "sourceAccessToken": source_client_access_token,
 "destinationAccessToken": destination_client_access_token
}
```

2. Konfigurieren und Starten des lokalen Proxys

Bevor Sie den lokalen Proxy ausführen können, laden Sie den lokalen Proxy-Quellcode von herunter GitHubund erstellen Sie ihn für die Plattform Ihrer Wahl. Anschließend können Sie den lokalen Ziel- und Quell-Proxy starten, um eine Verbindung zum sicheren Tunnel herzustellen und die Remote-Web-Server-Anwendung zu verwenden.

> **Note**
>
> Für AWS IoT sicheres Tunneling mit gleichzeitigen TCP-Verbindungen müssen Sie ein Upgrade auf die neueste Version des lokalen Proxys durchführen. Diese Funktion ist nicht verfügbar, wenn Sie den lokalen Proxy mit dem AWS IoT Device Client konfigurieren.

```
// Start the destination local proxy
./localproxy -r us-east-1 -d HTTP=80 -t destination_client_access_token

// Start the source local proxy
./localproxy -r us-east-1 -s HTTP=5555 -t source_client_access_token
```

Weitere Informationen zum Konfigurieren und Verwenden des lokalen Proxys finden Sie unter Wie man den lokalen Proxy benutzt.

Sie können jetzt den Tunnel verwenden, um auf die Webserver-Anwendung zuzugreifen. AWS IoT Secure Tunneling richtet automatisch die gleichzeitigen TCP-Verbindungen ein und verarbeitet sie, wenn mehrere Anfragen vom Client eingehen.

# Ein Remote-Gerät konfigurieren und IoT-Agent verwenden

Der IoT-Agent wird verwendet, um die MQTT-Nachricht zu empfangen, die das Clientzugriffstoken enthält, und einen lokalen Proxy auf dem Remote-Gerät zu starten. Sie müssen den IoT-Agenten auf dem entfernten Gerät installieren und ausführen, wenn Sie das Client-Zugriffstoken über MQTT durch einen sicheren Tunnel übermitteln möchten. Der IoT-Agent muss das folgende reservierte IoT-MQTT-Thema abonnieren:

> **Note**
>
> Wenn Sie dem Remote-Gerät das Ziel-Client-Zugriffstoken über andere Methoden als durch das Abonnieren des reservierten MQTT-Topics zukommen lassen möchten, benötigen Sie möglicherweise einen Ziel-Client-Zugriffstoken-Listener (CAT) und einen lokalen Proxy. Der CAT-Listener muss mit dem von Ihnen gewählten Zustellungsmechanismus für Client-Zugangstoken arbeiten und in einen lokalen Proxy im Zielmodus starten können.

## IoT-Agent-Snippet

Der IoT-Agent muss das folgende reservierte IoT-MQTT-Topic abonnieren, damit er die MQTT-Nachricht empfangen und den lokalen Proxy starten kann:

`$aws/things/`*`thing-name`*`/tunnels/notify`

Wo `thing-name` ist der Name der AWS IoT Sache, die dem Remote-Gerät zugeordnet ist?

Im Folgenden finden Sie ein Beispiel für eine MQTT-Nachrichtennutzlast:

```
{
    "clientAccessToken": "destination-client-access-token",
    "clientMode": "destination",
    "region": "aws-region",
    "services": ["destination-service"]
}
```

Nach dem Empfang einer MQTT-Nachricht muss der IoT-Agent einen lokalen Proxy auf dem Remote-Gerät mit den entsprechenden Parametern starten.

Der folgende Java-Code zeigt, wie Sie mit dem AWS IoT Device SDK und ProcessBuilderder Java-Bibliothek einen einfachen IoT-Agenten für sicheres Tunneling erstellen.

```
// Find the IoT device endpoint for your AWS-Konto
final String endpoint = iotClient.describeEndpoint(new
 DescribeEndpointRequest().withEndpointType("iot:Data-ATS")).getEndpointAddress();

// Instantiate the IoT Agent with your AWS credentials
final String thingName = "RemoteDeviceA";
final String tunnelNotificationTopic = String.format("$aws/things/%s/tunnels/notify",
 thingName);
final AWSIotMqttClient mqttClient = new AWSIotMqttClient(endpoint, thingName,
                 "your_aws_access_key", "your_aws_secret_key");

try {
    mqttClient.connect();
    final TunnelNotificationListener listener = new
 TunnelNotificationListener(tunnelNotificationTopic);
    mqttClient.subscribe(listener, true);
}
finally {
    mqttClient.disconnect();
}

private static class TunnelNotificationListener extends AWSIotTopic {
    public TunnelNotificationListener(String topic) {
        super(topic);
    }

    @Override
    public void onMessage(AWSIotMessage message) {
        try {
            // Deserialize the MQTT message
            final JSONObject json = new JSONObject(message.getStringPayload());

            final String accessToken = json.getString("clientAccessToken");
            final String region = json.getString("region");

            final String clientMode = json.getString("clientMode");
            if (!clientMode.equals("destination")) {
```

```
                throw new RuntimeException("Client mode " + clientMode + " in the MQTT
 message is not expected");
            }

            final JSONArray servicesArray = json.getJSONArray("services");
            if (servicesArray.length() > 1) {
                throw new RuntimeException("Services in the MQTT message has more than
 1 service");
            }
            final String service = servicesArray.get(0).toString();
            if (!service.equals("SSH")) {
                throw new RuntimeException("Service " + service + " is not supported");
            }

            // Start the destination local proxy in a separate process to connect to
 the SSH Daemon listening port 22
            final ProcessBuilder pb = new ProcessBuilder("localproxy",
                        "-t", accessToken,
                        "-r", region,
                        "-d", "localhost:22");
            pb.start();
        }
        catch (Exception e) {
            log.error("Failed to start the local proxy", e);
        }
    }
}
```

# Steuern des Zugriffs auf Tunnel

DSecure Tunneling bietet dienstspezifische Aktionen, Ressourcen und Bedingungskontextschlüssel zur Verwendung in IAM-Berechtigungsrichtlinien.

## Voraussetzungen für den Tunnelzugriff

- Erfahren Sie, wie Sie AWS Ressourcen mithilfe von IAM-Richtlinien sichern können.
- Erfahren Sie, wie Sie IAM-Bedingungen erstellen und bewerten.
- Erfahren Sie, wie Sie AWS Ressourcen mithilfe von Ressourcen-Tags sichern.

# Richtlinien für den Tunnelzugriff

Sie müssen die folgenden Richtlinien verwenden, um Berechtigungen zur Verwendung der Secure Tunneling-API zu autorisieren. Weitere Informationen zur AWS IoT Sicherheit finden Sie unterIdentitäts- und Zugriffsmanagement für AWS IoT.

IoT: OpenTunnel

Die `iot:OpenTunnel`-Richtlinienaktion erteilt eine Prinzipalberechtigung zum Aufrufen von OpenTunnel.

Im `Resource` Element der IAM-Richtlinienerklärung:

- Geben Sie den Wildcard-Tunnel-ARN an:

  `arn:aws:iot:`*`aws-region`*`:`*`aws-account-id`*`:tunnel/*`
- Geben Sie einen Objekt-ARN an, um die `OpenTunnel` Berechtigung für bestimmte IoT-Objekte zu verwalten:

  `arn:aws:iot:`*`aws-region`*`:`*`aws-account-id`*`:thing/`*`thing-name`*

Mit der folgenden Richtlinienanweisung können Sie beispielsweise einen Tunnel für das IoT-Objekt mit der Bezeichnung `TestDevice` öffnen.

```
{
    "Effect": "Allow",
    "Action": "iot:OpenTunnel",
    "Resource": [
        "arn:aws:iot:aws-region:aws-account-id:tunnel/*",
        "arn:aws:iot:aws-region:aws-account-id:thing/TestDevice"
    ]
}
```

Die `iot:OpenTunnel`-Richtlinienaktion unterstützt die folgenden Bedingungsschlüssel:

- `iot:ThingGroupArn`
- `iot:TunnelDestinationService`
- `aws:RequestTag/`*`tag-key`*
- `aws:SecureTransport`

- `aws:TagKeys`

Mit der folgenden Richtlinienanweisung können Sie einen Tunnel zu dem Objekt öffnen, wenn das Objekt zu einer Objektgruppe mit einem Namen gehört, der mit `TestGroup` beginnt und im Tunnel der Zielservice SSH konfiguriert ist.

```
{
    "Effect": "Allow",
    "Action": "iot:OpenTunnel",
    "Resource": [
        "arn:aws:iot:aws-region:aws-account-id:tunnel/*"
    ],
    "Condition": {
        "ForAnyValue:StringLike": {
            "iot:ThingGroupArn": [
                "arn:aws:iot:aws-region:aws-account-id:thinggroup/TestGroup*"
            ]
        },
        "ForAllValues:StringEquals": {
            "iot:TunnelDestinationService": [
                "SSH"
            ]
        }
    }
}
```

Sie können auch Ressourcen-Tags verwenden, um die Berechtigung zum Öffnen von Tunneln zu steuern. Mit der folgenden Richtlinienanweisung kann beispielsweise ein Tunnel geöffnet werden, wenn der Tag-Schlüssel `Owner` mit dem Wert `Admin` vorhanden ist und keine anderen Tags angegeben werden. Allgemeine Informationen zur Verwendung von Tags finden Sie unter Verschlagworten Sie Ihre Ressourcen AWS IoT.

```
{
    "Effect": "Allow",
    "Action": "iot:OpenTunnel",
    "Resource": [
        "arn:aws:iot:aws-region:aws-account-id:tunnel/*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Owner": "Admin"
```

```
        },
        "ForAllValues:StringEquals": {
            "aws:TagKeys": "Owner"
        }
    }
}
```

IoT: RotateTunnelAccessToken

Die `iot:RotateTunnelAccessToken`-Richtlinienaktion erteilt eine Prinzipalberechtigung zum Aufrufen von RotateTunnelAccessToken.

Im `Resource` Element der IAM-Richtlinienerklärung:

- Geben Sie einen vollqualifizierten Tunnel-ARN an:

  `arn:aws:iot:`*`aws-region`*`: `*`aws-account-id`*`:tunnel/`*`tunnel-id`*

  Sie können auch den Wildcard-Tunnel-ARN verwenden:

  `arn:aws:iot:`*`aws-region`*`:`*`aws-account-id`*`:tunnel/*`
- Geben Sie einen Objekt-ARN an, um die `RotateTunnelAccessToken` Berechtigung für bestimmte IoT-Objekte zu verwalten:

  `arn:aws:iot:`*`aws-region`*`:`*`aws-account-id`*`:thing/`*`thing-name`*

Mit der folgenden Richtlinienanweisung können Sie beispielsweise entweder das Quellzugriffstoken eines Tunnels oder das Zielzugriffstoken eines Clients für das genannte IoT-Objekt namens`TestDevice` rotieren.

```
{
    "Effect": "Allow",
    "Action": "iot:RotateTunnelAccessToken",
    "Resource": [
        "arn:aws:iot:aws-region:aws-account-id:tunnel/*",
        "arn:aws:iot:aws-region:aws-account-id:thing/TestDevice"
    ]
}
```

Die `iot:RotateTunnelAccessToken`-Richtlinienaktion unterstützt die folgenden Bedingungsschlüssel:

- `iot:ThingGroupArn`
- `iot:TunnelDestinationService`
- `iot:ClientMode`
- `aws:SecureTransport`

Mit der folgenden Richtlinienanweisung können Sie das Zielzugriffstoken auf das Objekt rotieren, wenn das Objekt zu einer Objektgruppe mit einem Namen gehört, der mit `TestGroup` beginnt, der konfigurierte Zieldienst auf dem Tunnel SSH ist, und der Client sich im `DESTINATION`-Modus befindet.

```
{
    "Effect": "Allow",
    "Action": "iot:RotateTunnelAccessToken",
    "Resource": [
        "arn:aws:iot:aws-region:aws-account-id:tunnel/*"
    ],
    "Condition": {
        "ForAnyValue:StringLike": {
            "iot:ThingGroupArn": [
                "arn:aws:iot:aws-region:aws-account-id:thinggroup/TestGroup*"
            ]
        },
        "ForAllValues:StringEquals": {
            "iot:TunnelDestinationService": [
                "SSH"
            ],
            "iot:ClientMode": "DESTINATION"
        }
    }
}
```

IoT: DescribeTunnel

Die `iot:DescribeTunnel`-Richtlinienaktion erteilt eine Prinzipalberechtigung zum Aufrufen von DescribeTunnel.

Geben Sie im `Resource` Element der IAM-Richtlinienerklärung einen vollqualifizierten Tunnel-ARN an:

`arn:aws:iot:aws-region: aws-account-id:tunnel/tunnel-id`

Sie können auch den Wildcard-ARN verwenden:

`arn:aws:iot:aws-region:aws-account-id:tunnel/*`

Die `iot:DescribeTunnel`-Richtlinienaktion unterstützt die folgenden Bedingungsschlüssel:

- `aws:ResourceTag/tag-key`
- `aws:SecureTransport`

Mit der folgenden Richtlinienanweisung können Sie `DescribeTunnel` aufrufen, wenn der angeforderte Tunnel mit dem Schlüssel `Owner` mit dem Wert `Admin` gekennzeichnet ist.

```
{
    "Effect": "Allow",
    "Action": "iot:DescribeTunnel",
    "Resource": [
        "arn:aws:iot:aws-region:aws-account-id:tunnel/*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/Owner": "Admin"
        }
    }
}
```

IoT: ListTunnels

Die `iot:ListTunnels`-Richtlinienaktion erteilt eine Prinzipalberechtigung zum Aufrufen von ListTunnels.

Im `Resource` Element der IAM-Richtlinienerklärung:

- Geben Sie den Wildcard-Tunnel-ARN an:

  `arn:aws:iot:aws-region:aws-account-id:tunnel/*`
- Geben Sie einen Objekt-ARN an, um die `ListTunnels` Berechtigung für ausgewählte IoT-Objekte zu verwalten:

  `arn:aws:iot:aws-region:aws-account-id:thing/thing-name`

Die `iot:ListTunnels`-Richtlinienaktion unterstützt den Bedingungsschlüssel `aws:SecureTransport`.

Mit der folgenden Richtlinienanweisung können Sie Tunnel für das Objekt mit dem Namen `TestDevice` auflisten.

```
{
    "Effect": "Allow",
    "Action": "iot:ListTunnels",
    "Resource": [
        "arn:aws:iot:aws-region:aws-account-id:tunnel/*",
        "arn:aws:iot:aws-region:aws-account-id:thing/TestDevice"
    ]
}
```

IoT: ListTagsForResource

Die `iot:ListTagsForResource`-Richtlinienaktion erteilt eine Prinzipalberechtigung zum Aufrufen von `ListTagsForResource`.

Geben Sie im `Resource` Element der IAM-Richtlinienerklärung einen vollqualifizierten Tunnel-ARN an:

`arn:aws:iot:aws-region: aws-account-id:tunnel/tunnel-id`

Sie können auch den Wildcard-Tunnel-ARN verwenden:

`arn:aws:iot:aws-region:aws-account-id:tunnel/*`

Die `iot:ListTagsForResource`-Richtlinienaktion unterstützt den Bedingungsschlüssel `aws:SecureTransport`.

IoT: CloseTunnel

Die `iot:CloseTunnel`-Richtlinienaktion erteilt eine Prinzipalberechtigung zum Aufrufen von CloseTunnel.

Geben Sie im `Resource` Element der IAM-Richtlinienerklärung einen vollqualifizierten Tunnel-ARN an:

`arn:aws:iot:aws-region: aws-account-id:tunnel/tunnel-id`

Sie können auch den Wildcard-Tunnel-ARN verwenden:

`arn:aws:iot:aws-region:aws-account-id:tunnel/*`

Die `iot:CloseTunnel`-Richtlinienaktion unterstützt die folgenden Bedingungsschlüssel:

- `iot:Delete`
- `aws:ResourceTag/tag-key`
- `aws:SecureTransport`

Mit der folgenden Richtlinienanweisung können Sie `CloseTunnel` aufrufen, wenn der `Delete`-Parameter der Anforderung `false` ist und der angeforderte Tunnel mit dem Schlüssel `Owner` mit dem Wert `QATeam` gekennzeichnet ist.

```
{
    "Effect": "Allow",
    "Action": "iot:CloseTunnel",
    "Resource": [
        "arn:aws:iot:aws-region:aws-account-id:tunnel/*"
    ],
    "Condition": {
        "Bool": {
            "iot:Delete": "false"
        },
        "StringEquals": {
            "aws:ResourceTag/Owner": "QATeam"
        }
    }
}
```

IoT: TagResource

Die `iot:TagResource`-Richtlinienaktion erteilt eine Prinzipalberechtigung zum Aufrufen von `TagResource`.

Geben Sie im `Resource` Element der IAM-Richtlinienerklärung einen vollqualifizierten Tunnel-ARN an:

`arn:aws:iot:aws-region: aws-account-id:tunnel/tunnel-id`

Sie können auch den Wildcard-Tunnel-ARN verwenden:

`arn:aws:iot:aws-region:aws-account-id:tunnel/*`

Die `iot:TagResource`-Richtlinienaktion unterstützt den Bedingungsschlüssel `aws:SecureTransport`.

IoT: UntagResource

Die `iot:UntagResource`-Richtlinienaktion erteilt eine Prinzipalberechtigung zum Aufrufen von `UntagResource`.

Geben Sie im `Resource` Element der IAM-Richtlinienerklärung einen vollqualifizierten Tunnel-ARN an:

`arn:aws:iot:aws-region: aws-account-id:tunnel/tunnel-id`

Sie können auch den Wildcard-Tunnel-ARN verwenden:

`arn:aws:iot:aws-region:aws-account-id:tunnel/*`

Die `iot:UntagResource`-Richtlinienaktion unterstützt den Bedingungsschlüssel `aws:SecureTransport`.

# Lösung von Verbindungsproblemen beim AWS IoT sicheren Tunneling durch rotierende Client-Zugriffstoken

Wenn Sie AWS IoT Secure Tunneling verwenden, können Verbindungsprobleme auftreten, auch wenn der Tunnel geöffnet ist. Die folgenden Abschnitte zeigen einige mögliche Probleme und wie Sie diese durch Rotation der Client-Zugriffstoken lösen können. Um das Client Access Token (CAT) zu rotieren, verwenden Sie die RotateTunnelAccessTokenAPI oder die. rotate-tunnel-access-token AWS CLI Je nachdem, ob bei der Verwendung des Clients im Quell- oder Zielmodus ein Fehler auftritt, können Sie das CAT entweder im Quell- oder Zielmodus oder in beiden Modi rotieren.

> **Note**
>
> - Wenn Sie sich nicht sicher sind, ob das CAT an der Quelle oder am Ziel rotiert werden muss, können Sie das CAT sowohl an der Quelle als auch am Ziel rotieren, indem Sie `ClientMode` auf ALL setzen bei der Verwendung der `RotateTunnelAccessToken`-API.
> - Durch das Rotieren des CAT wird die Tunneldauer nicht verlängert. Nehmen wir zum Beispiel an, die Tunneldauer beträgt 12 Stunden und der Tunnel ist bereits seit 4 Stunden

geöffnet. Wenn Sie die Zugriffstoken rotieren, können die neu generierten Token nur für die verbleibenden 8 Stunden verwendet werden.

Themen


- Fehler beim ungültigen Client-Zugriffstoken
- Fehler bei Nichtübereinstimmung der Client-Tokens
- Verbindungsprobleme bei Remote-Geräten


## Fehler beim ungültigen Client-Zugriffstoken

Wenn Sie AWS IoT Secure Tunneling verwenden, kann es zu einem Verbindungsfehler kommen, wenn Sie dasselbe Clientzugriffstoken (CAT) verwenden, um die Verbindung zum gleichen Tunnel wiederherzustellen. In diesem Fall kann der lokale Proxy keine Verbindung zum Secure Tunneling-Proxyserver herstellen. Wenn Sie einen Client im Quellmodus verwenden, wird möglicherweise die folgende Fehlermeldung angezeigt:

```
Invalid access token: The access token was previously used and cannot be used again
```

Der Fehler tritt auf, weil das Client-Zugriffstoken (CAT) vom lokalen Proxy nur einmal verwendet werden kann und dann ungültig wird. Um diesen Fehler zu beheben, wechseln Sie das Client-Zugriffstoken in den `SOURCE` Modus, in dem ein neues CAT für die Quelle generiert wird. Ein Beispiel, das zeigt, wie Sie das Quell-CAT rotieren, finden Sie unter Beispiel für „Quell-CAT rotieren“.

## Fehler bei Nichtübereinstimmung der Client-Tokens

> **Note**
>
> Die Verwendung von Client-Tokens zur Wiederverwendung des CAT wird nicht empfohlen. Wir empfehlen, stattdessen die `RotateTunnelAccessToken`-API zu verwenden, um die Client-Zugriffstoken zu rotieren, um die Verbindung zum Tunnel wiederherzustellen.

Wenn Sie Client-Token verwenden, können Sie das CAT wiederverwenden, um die Verbindung zum Tunnel wiederherzustellen. Um die CAT wiederzuverwenden, müssen Sie dem Client-Token die CAT zur Verfügung stellen, wenn Sie zum ersten Mal eine Verbindung zu Secure Tunneling herstellen.

Secure Tunneling speichert das Client-Token, sodass für nachfolgende Verbindungsversuche mit demselben Token auch das Client-Token bereitgestellt werden muss. Weitere Informationen zur Verwendung von Client-Tokens finden Sie in der Referenzimplementierung für lokale Proxys unter. GitHub

Wenn Sie Client-Token verwenden und einen Client im Quellmodus verwenden, wird möglicherweise der folgende Fehler angezeigt:

```
Invalid client token: The provided client token does not match the client token
    that was previously set.
```

Der Fehler tritt auf, weil das bereitgestellte Client-Token nicht mit dem Client-Token übereinstimmt, das beim Zugriff auf den Tunnel mit dem CAT bereitgestellt wurde. Um diesen Fehler zu beheben, rotieren Sie den CAT in dem `SOURCE` Modus, um ein neues CAT für die Quelle zu erzeugen. Im Folgenden sehen Sie ein Beispiel:

Beispiel für „Quell-CAT rotieren“

Im Folgenden finden Sie ein Beispiel dafür, wie die `RotateTunnelAccessToken` API im `SOURCE`-Modus zum Generieren einer neuen CAT für die Quelle ausgeführt wird:

```
aws iotsecuretunneling rotate-tunnel-access-token \
    --region <region> \
    --tunnel-id <tunnel-id> \
    --client-mode SOURCE
```

Wenn Sie diesen Befehl ausführen, wird ein neues Quellzugriffstoken generiert und der ARN Ihres Tunnels zurückgegeben.

```
{
    "sourceAccessToken": "<source-access-token>",
    "tunnelArn": "arn:aws:iot:<region>:<account-id>:tunnel/<tunnel-id>"
}
```

Sie können jetzt das neue Quell-Token verwenden, um den lokalen Proxy im Quellmodus zu verbinden.

```
export AWSIOT_TUNNEL_ACCESS_TOKEN=<source-access-token>
./localproxy -r <region> -s <port>
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe der Ausführung des lokalen Proxys:

```
...

[info]    Starting proxy in source mode
...
[info]    Successfully established websocket connection with proxy server ...
[info]    Listening for new connection on port <port>
...
```

## Verbindungsprobleme bei Remote-Geräten

Bei Verwendung von AWS IoT Secure Tunneling wird die Verbindung zum Gerät möglicherweise unerwartet unterbrochen, selbst wenn der Tunnel geöffnet ist. Um festzustellen, ob ein Gerät noch mit dem Tunnel verbunden ist, können Sie die DescribeTunnelAPI oder den Describe-Tunnel verwenden. AWS CLI

Ein Gerät kann aus mehreren Gründen unterbrochen werden. Um das Verbindungsproblem zu beheben, können Sie das CAT auf das Zielgerät rotieren, falls die Verbindung zum Gerät aus den folgenden möglichen Gründen unterbrochen wurde:

- Das CAT auf dem Ziel wurde ungültig.
- Das Token wurde nicht über das für Secure Tunneling reservierte MQTT-Thema an das Gerät übermittelt:

  `$aws/things/<thing-name>/tunnels/notify`

Das folgende Beispiel veranschaulicht, wie dieses Problem gelöst werden kann:

Beispiel für die Rotation des Ziel-CAT

Man nehme ein Remote-Gerät, *<RemoteThing1>*. Um einen Tunnel für dieses Objekt zu öffnen, können Sie den folgenden Befehl verwenden:

```
aws iotsecuretunneling open-tunnel \
    --region <region> \
    --destination-config thingName=<RemoteThing1>,services=SSH
```

Wenn Sie diesen Befehl ausführen, werden die Tunneldetails und das CAT für Ihre Quelle und Ihr Ziel generiert.

```
{
    "sourceAccessToken": "<source-access-token>",
    "destinationAccessToken": "<destination-access-token>",
    "tunnelId": "<tunnel-id>",
    "tunnelArn": "arn:aws:iot:<region>:<account-id>:tunnel/tunnel-id"
}
```

Wenn Sie die DescribeTunnelAPI verwenden, zeigt die Ausgabe jedoch an, dass das Gerät getrennt wurde, wie unten dargestellt:

```
aws iotsecuretunneling describe-tunnel \
    --tunnel-id <tunnel-id> \
    --region <region>
```

Wenn Sie diesen Befehl ausführen, wird angezeigt, dass das Gerät immer noch nicht verbunden ist.

```
{
    "tunnel": {
        ...
        "destinationConnectionState": {
            "status": "DISCONNECTED"
        },
        ...
    }
}
```

Um diesen Fehler zu beheben, führen Sie die `RotateTunnelAccessToken` API mit dem Client im `DESTINATION`-Modus und den Konfigurationen für das Ziel aus. Wenn Sie diesen Befehl ausführen, wird das alte Zugriffstoken gesperrt, ein neues Token generiert und dieses Token erneut an das MQTT-Thema gesendet:

`$aws/things/<thing-name>/tunnels/notify`

```
aws iotsecuretunneling rotate-tunnel-access-token \
    --tunnel-id <tunnel-id> \
    --client-mode DESTINATION \
    --destination-config thingName=<RemoteThing1>,services=SSH \
    --region <region>
```

Durch die Ausführung dieses Befehls wird das neue Zugriffstoken wie unten dargestellt generiert. Das Token wird dann an das Gerät übermittelt, um eine Verbindung zum Tunnel herzustellen, sofern der Geräteagent korrekt eingerichtet ist.

```
{
    "destinationAccessToken": "destination-access-token",
    "tunnelArn": "arn:aws:iot:region:account-id:tunnel/tunnel-id"
}
```

# Gerätebereitstellung

AWS bietet verschiedene Möglichkeiten, ein Gerät bereitzustellen und eindeutige Client-Zertifikate darauf zu installieren. In diesem Abschnitt werden die einzelnen Möglichkeiten beschrieben und erläutert, wie Sie die beste für Ihre IoT-Lösung auswählen. Diese Optionen werden im Whitepaper mit dem Titel Herstellung und Bereitstellung von Geräten mit X.509-Zertifikaten in AWS IoT Core ausführlich beschrieben.

Wählen Sie die für Sie geeignete Option aus.

- Sie können Zertifikate auf IoT-Geräten installieren, bevor sie geliefert werden.

  Wenn Sie eindeutige Client-Zertifikate sicher auf Ihren IoT-Geräten installieren können, bevor sie dem Endbenutzer zur Verwendung bereitgestellt werden, sollten Sie just-in-timeProvisioning (JITP) oder just-in-timeRegistrierung (JITR) verwenden.

  Mithilfe von JITP und JITR wird die Zertifizierungsstelle (CA), die zum Signieren des Gerätezertifikats verwendet wird, registriert AWS IoT und erkannt, AWS IoT wenn das Gerät zum ersten Mal eine Verbindung herstellt. Das Gerät wird AWS IoT bei seiner ersten Verbindung mithilfe der Details seiner Bereitstellungsvorlage bereitgestellt.

  Weitere Informationen zur Single-Thing-, JITP-, JITR- und Massenbereitstellung von Geräten mit eindeutigen Zertifikaten finden Sie unter the section called “Bereitstellen von Geräten mit Gerätezertifikaten”.
- Endbenutzer oder Installateure können eine App verwenden, um Zertifikate auf ihren IoT-Geräten zu installieren.

  Wenn Sie eindeutige Client-Zertifikate nicht sicher auf Ihrem IoT-Gerät installieren können, bevor sie an die Endbenutzer geliefert werden, die Endbenutzer oder Installateure jedoch eine App verwenden können, um die Geräte zu registrieren und die eindeutigen Gerätezertifikate zu installieren, sollten Sie die Bereitstellung durch vertrauenswürdige Benutzer verwenden.

  Die Verwendung von vertrauenswürdigen Benutzern, z. B. Endbenutzern oder Installateuren mit bekanntem Konto, kann den Geräteherstellungsprozess vereinfachen. Anstatt eines eindeutigen Client-Zertifikats verfügen Geräte über ein temporäres Zertifikat, mit dem das Gerät nur 5 Minuten AWS IoT lang eine Verbindung herstellen kann. Während dieses 5-minütigen Zeitfensters erhalten vertrauenswürdige Benutzer ein eindeutiges Client-Zertifikat mit einer längeren Lebensdauer, das

sie auf dem Gerät installieren können. Durch die begrenzte Gültigkeitsdauer des Antragszertifikats wird das Risiko kompromittierter Zertifikate minimiert.

Weitere Informationen finden Sie unter the section called “Bereitstellung durch vertrauenswürdigen Benutzer”.

- Endbenutzer können KEINE App verwenden, um Zertifikate auf ihren IoT-Geräten zu installieren.

  Wenn keine der vorherigen Optionen in Ihrer IoT-Lösung funktioniert, ist für Sie die Bereitstellung durch Anspruch eine Option. Mit diesem Prozess verfügen Ihre IoT-Geräte über ein Antragszertifikat, das gemeinsam von anderen Geräten in der Flotte genutzt wird. Wenn ein Gerät zum ersten Mal eine Verbindung mit einem Antragszertifikat herstellt, AWS IoT registriert es das Gerät mithilfe seiner Bereitstellungsvorlage und stellt dem Gerät sein eindeutiges Client-Zertifikat für den späteren Zugriff AWS IoT aus.

  Diese Option ermöglicht die automatische Bereitstellung eines Geräts, wenn es eine Verbindung herstellt AWS IoT, könnte jedoch ein größeres Risiko darstellen, wenn das Antragszertifikat kompromittiert wird. Wenn ein Antragszertifikat kompromittiert wird, können Sie das Zertifikat deaktivieren. Durch die Deaktivierung des Antragszertifikats wird verhindert, dass in Zukunft Geräte mit diesem Antragszertifikat registriert werden. Durch die Deaktivierung des Antragszertifikats werden jedoch keine Geräte blockiert, die bereits bereitgestellt wurden.

  Weitere Informationen finden Sie unter the section called “Bereitstellung durch Anspruch”.

# Bereitstellung von Geräten in AWS IoT

Wenn Sie ein Gerät mit bereitstellen AWS IoT, müssen Sie Ressourcen einrichten, damit Ihre Geräte und Geräte sicher kommunizieren AWS IoT können. Weitere Ressourcen können erstellt werden, um Ihnen bei der Verwaltung Ihrer Geräteflotte zu helfen. Die folgenden Ressourcen können während des Bereitstellungsprozesses erstellt werden:

- Ein IoT-Objekt

  IoT-Dinge sind Einträge in der AWS IoT Geräteregistrierung. Jedes Objekt hat einen eindeutigen Namen und einen Satz von Attributen und ist mit einem physischen Gerät verbunden. Objekte können mit einem Objekttyp definiert oder in Objektgruppen gruppiert werden. Weitere Informationen finden Sie unter Geräte verwalten mit AWS IoT.

Obwohl nicht erforderlich, ermöglicht es das Erstellen eines Objekts, Ihre Geräteflotte effektiver zu verwalten, indem Sie Geräte nach Objekttyp, Objektgruppe und Objektattributen suchen. Weitere Informationen finden Sie unter -Flottenindizierung.

> **Note**
>
> Um die Konnektivitätsstatusdaten Ihres Dings zu indizieren, stellen Sie Ihr Ding bereit und konfigurieren Sie es so, dass der Name des Dings mit der Client-ID übereinstimmt, die in der Connect-Anfrage verwendet wurde.

- Ein X.509-Zertifikat.

  Geräte verwenden X.509-Zertifikate für die gegenseitige Authentifizierung mit AWS IoT. Sie können ein vorhandenes Zertifikat registrieren oder ein neues Zertifikat für Sie AWS IoT generieren und registrieren lassen. Sie ordnen einem Gerät ein Zertifikat zu, indem Sie es an das Objekt anhängen, das für das Gerät steht. Sie müssen auch das Zertifikat und den zugehörigen privaten Schlüssel auf das Gerät kopieren. Geräte legen das Zertifikat vor, wenn sie eine Verbindung herstellen AWS IoT. Weitere Informationen finden Sie unter Authentifizierung.

- Eine IoT-Richtlinie.

  IoT-Richtlinien definieren, welche Operationen ein Gerät in AWS IoT ausführen kann. IoT-Richtlinien sind an Gerätezertifikate angehängt. Wenn ein Gerät das Zertifikat vorlegt AWS IoT, werden ihm die in der Richtlinie angegebenen Berechtigungen gewährt. Weitere Informationen finden Sie unter Autorisierung. Jedes Gerät benötigt ein Zertifikat für die Kommunikation mit AWS IoT.

AWS IoT unterstützt die automatisierte Flottenbereitstellung mithilfe von Bereitstellungsvorlagen. Bereitstellungsvorlagen beschreiben die Ressourcen, die für die Bereitstellung AWS IoT Ihres Geräts erforderlich sind. Vorlagen enthalten Variablen, mit denen Sie eine Vorlage zum Bereitstellen mehrerer Geräte verwenden können. Wenn Sie ein Gerät bereitstellen, geben Sie Werte für die für das Gerät spezifischen Variablen mithilfe eines Wörterbuchs oder einer Karte an. Um ein anderes Gerät bereitzustellen, geben Sie neue Werte im Wörterbuch an.

Sie können die automatisierte Bereitstellung verwenden, unabhängig davon, ob Ihre Geräte über eindeutige Zertifikate (und den zugehörigen privaten Schlüssel) verfügen.

# Bereitstellung von Flotten APIs

Es gibt mehrere Kategorien, die bei der Flottenbereitstellung APIs verwendet werden:

- Diese Funktionen der Steuerungsebene erstellen und verwalten die Flottenbereitstellungsvorlagen und konfigurieren vertrauenswürdige Benutzerrichtlinien.
  - CreateProvisioningTemplate
  - CreateProvisioningTemplateVersion
  - DeleteProvisioningTemplate
  - DeleteProvisioningTemplateVersion
  - DescribeProvisioningTemplate
  - DescribeProvisioningTemplateVersion
  - ListProvisioningTemplates
  - ListProvisioningTemplateVersions
  - UpdateProvisioningTemplate
- Vertrauenswürdige Benutzer können diese Funktion der Steuerungsebene verwenden, um einen temporären Onboarding-Antrag zu generieren. Dieser temporäre Antrag wird während der WLAN-Konfiguration oder einer ähnlichen Methode an das Gerät übergeben.
  - CreateProvisioningClaim
- Die MQTT-API, die während des Bereitstellungsprozesses von Geräten verwendet wird, deren Bereitstellungsantragszertifikat in einem Gerät eingebettet ist oder von einem vertrauenswürdigen Benutzer an es übergeben wird.
  - the section called “CreateCertificateFromCsr”
  - the section called “CreateKeysAndCertificate”
  - the section called “RegisterThing”

# Bereitstellen von Geräten ohne Gerätezertifikate mithilfe der Flottenbereitstellung

Mithilfe von AWS IoT Fleet Provisioning AWS IoT können Gerätezertifikate und private Schlüssel generiert und sicher an Ihre Geräte gesendet werden, wenn diese AWS IoT zum ersten Mal eine Verbindung herstellen. AWS IoT stellt Client-Zertifikate bereit, die von der Amazon Root Certificate Authority (CA) signiert wurden.

Es gibt zwei Möglichkeiten, die Flottenbereitstellung zu verwenden:

- Bereitstellung durch Anspruch
- Bereitstellung durch vertrauenswürdigen Benutzer

## Bereitstellung durch Anspruch

Geräte können mit einem Bereitstellungsantragszertifikat und einem privaten Schlüssel (bei denen es sich um spezielle Anmeldeinformationen handelt) hergestellt werden. Wenn diese Zertifikate bei registriert sind AWS IoT, kann der Service sie gegen eindeutige Gerätezertifikate eintauschen, die das Gerät für den regulären Betrieb verwenden kann. Dieser Prozess umfasst die folgenden Schritte:

Vor der Geräteauslieferung

1. Rufen Sie `CreateProvisioningTemplate` auf, um eine Bereitstellungsvorlage zu erstellen. Diese API gibt einen Vorlagen-ARN zurück. Weitere Informationen finden Sie unter MQTT-API für die Gerätebereitstellung.

   Sie können in der AWS IoT Konsole auch eine Vorlage für die Flottenbereitstellung erstellen.

   a. Wählen Sie im Navigationsbereich die Dropdownliste Viele Geräte Connect aus. Wählen Sie dann „Viele Geräte Connect“.
   b. Wählen Sie Provisioning-Vorlage erstellen aus.
   c. Wählen Sie das Provisioning-Szenario, das am besten zu Ihren Installationsprozessen passt. Wählen Sie anschließend Weiter.
   d. Schließen Sie den Vorlagen-Workflow ab.
2. Erstellen Sie Zertifikate und zugehörige private Schlüssel, die als Bereitstellungsantragszertifikate verwendet werden sollen.
3. Registrieren Sie diese Zertifikate mit AWS IoT und verknüpfen Sie sie mit einer IoT-Richtlinie, die die Verwendung der Zertifikate einschränkt. Die folgende IoT-Beispielrichtlinie beschränkt die Verwendung des Zertifikats, das dieser Richtlinie zugeordnet ist, auf Bereitstellungsgeräte.

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

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": ["iot:Publish","iot:Receive"],
            "Resource": [
                "arn:aws:iot:aws-region:aws-account-id:topic/$aws/certificates/
create/*",
                "arn:aws:iot:aws-region:aws-account-id:topic/$aws/provisioning-
templates/templateName/provision/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iot:Subscribe",
            "Resource": [
                "arn:aws:iot:aws-region:aws-account-id:topicfilter/$aws/
certificates/create/*",
                "arn:aws:iot:aws-region:aws-account-id:topicfilter/$aws/
provisioning-templates/templateName/provision/*"
            ]
        }
    ]
}
```

4. Erteilen Sie dem AWS IoT Dienst die Erlaubnis, IoT-Ressourcen wie Dinge und Zertifikate in Ihrem Konto zu erstellen oder zu aktualisieren, wenn Sie Geräte bereitstellen. Fügen Sie dazu die `AWSIoTThingsRegistration` verwaltete Richtlinie einer IAM-Rolle (der sogenannten Bereitstellungsrolle) hinzu, die dem Dienstprinzipal vertraut. AWS IoT
5. Stellen Sie das Gerät mit dem sicher darin eingebetteten Bereitstellungsantragszertifikat her.

Das Gerät kann nun an den Ort geliefert werden, an dem es zur Verwendung installiert wird.

> **Important**
>
> Private Schlüssel für Bereitstellungsanträge sollten jederzeit gesichert werden, auch auf dem Gerät. Wir empfehlen Ihnen, anhand von AWS IoT CloudWatch Metriken und Protokollen nach Hinweisen auf Missbrauch zu suchen. Wenn Sie einen Missbrauch feststellen, deaktivieren Sie das Bereitstellungsantragszertifikat, damit es nicht für die Gerätebereitstellung verwendet werden kann.

So initialisieren Sie das Gerät für die Verwendung

1. Das Gerät verwendet dasAWS IoT Geräte SDKs - SDKs, Mobil- und AWS IoT Geräteclient, um sich AWS IoT mit dem auf dem Gerät installierten Provisioning Claim Certificate zu verbinden und sich damit zu authentifizieren.

   > **Note**
   >
   > Aus Sicherheitsgründen wird das `certificateOwnershipToken` von `CreateCertificateFromCsr` zurückgesendet und `CreateKeysAndCertificate` läuft nach einer Stunde ab. `RegisterThing` muss aufgerufen werden, bevor das `certificateOwnershipToken` abläuft. Wenn das von `CreateCertificateFromCsr` oder `CreateKeysAndCertificate` erstellte Zertifikat nicht aktiviert und bis zum Ablauf des Tokens noch nicht an eine Richtlinie oder ein Objekt angehängt wurde, wird das Zertifikat gelöscht. Wenn das Token abläuft, kann das Gerät `CreateCertificateFromCsr` oder `CreateKeysAndCertificate` erneut aufrufen, um ein neues Zertifikat zu generieren.

2. Das Gerät erhält ein permanentes Zertifikat und einen privaten Schlüssel mithilfe einer dieser Optionen. Das Gerät verwendet das Zertifikat und den Schlüssel für alle future Authentifizierungen mit AWS IoT.

   a. Rufen Sie `CreateKeysAndCertificate`an, um mithilfe der Zertifizierungsstelle ein neues Zertifikat und einen neuen privaten Schlüssel zu erstellen. AWS

      Oder

   b. Rufen Sie `CreateCertificateFromCsr` auf, um ein Zertifikat aus einer Zertifikatsignieranforderung zu generieren, das seinen privaten Schlüssel schützt.

3. Rufen Sie vom Gerät aus `RegisterThing` auf, um das Gerät in AWS IoT zu registrieren und Cloud-Ressourcen zu erstellen.

   Der Fleet-Provisioning-Service verwendet Bereitstellungsvorlagen, um Cloud-Ressourcen wie IoT-Objekte zu definieren und zu erstellen. Die Vorlage kann Attribute und Gruppen angeben, denen das Objekt angehört. Die Objektgruppen müssen vorhanden sein, damit das neue Objekt hinzugefügt werden kann.

4. Nach dem Speichern des permanenten Zertifikats auf dem Gerät muss das Gerät die Verbindung von der Sitzung trennen, die es mit dem Bereitstellungsantragszertifikat initiiert hat, und die Verbindung mit dem permanenten Zertifikat erneut herstellen.

Das Gerät ist jetzt bereit, normal mit dem Gerät zu kommunizieren AWS IoT.

## Bereitstellung durch vertrauenswürdigen Benutzer

In vielen Fällen stellt ein Gerät AWS IoT zum ersten Mal eine Verbindung her, wenn ein vertrauenswürdiger Benutzer, z. B. ein Endbenutzer oder Installationstechniker, eine mobile App verwendet, um das Gerät an seinem Einsatzort zu konfigurieren.

> **Important**
>
> Sie müssen den Zugriff und die Berechtigung des vertrauenswürdigen Benutzers verwalten, um dieses Verfahren auszuführen. Eine Möglichkeit besteht darin, vertrauenswürdigen Benutzern ein Konto bereitzustellen und für sie zu verwalten, mit dem sie authentifiziert werden und Zugriff auf die AWS IoT -Funktionen und API-Operationen erhalten, die für dieses Vorgehen erforderlich sind.

Vor der Geräteauslieferung

1. Rufen Sie `CreateProvisioningTemplate`auf, um eine Bereitstellungsvorlage zu erstellen, und geben Sie deren *`templateArn`* und *`templateName`* zurück.
2. Erstellen Sie eine IAM-Rolle, die von vertrauenswürdigen Benutzern verwendet wird, um den Bereitstellungsprozess zu initiieren. Mit der Bereitstellungsvorlage kann nur dieser Benutzer ein Gerät bereitstellen. Zum Beispiel:

   ```
   {
       "Effect": "Allow",
       "Action": [
           "iot:CreateProvisioningClaim"
       ],
       "Resource": [
           "arn:aws:iot:aws-region:aws-account-id:provisioningtemplate/templateName"
       ]
   }
   ```

3. Erteilen Sie dem AWS IoT Dienst die Erlaubnis, IoT-Ressourcen wie Dinge und Zertifikate in Ihrem Konto zu erstellen oder zu aktualisieren, wenn Sie Geräte bereitstellen. Dazu fügen Sie die `AWSIoTThingsRegistration` verwaltete Richtlinie einer IAM-Rolle (der sogenannten Bereitstellungsrolle) hinzu, die dem Dienstprinzipal vertraut. AWS IoT

4. Stellen Sie die Mittel zur Identifizierung Ihrer vertrauenswürdigen Benutzer bereit, indem Sie ihnen beispielsweise ein Konto zur Verfügung stellen, mit dem sie authentifiziert und ihre Interaktionen mit den AWS API-Vorgängen autorisiert werden können, die für die Registrierung ihrer Geräte erforderlich sind.

So initialisieren Sie das Gerät für die Verwendung

1. Der vertrauenswürdige Benutzer meldet sich bei der mobilen App oder dem Webservice für die Bereitstellung an.
2. Die mobile App oder Webanwendung verwendet die IAM-Rolle und ruft `CreateProvisioningClaim` auf, um ein temporäres Bereitstellungsantragszertifikat von AWS IoT abzurufen.

   > **Note**
   >
   > Aus Sicherheitsgründen läuft das von `CreateProvisioningClaim` zurückgegebene temporäre Bereitstellungsantragszertifikat nach fünf Minuten ab. Die folgenden Schritte müssen erfolgreich ein gültiges Zertifikat zurückgeben, bevor das temporäre Bereitstellungsantragszertifikat abläuft. Temporäre Bereitstellungsantragszertifikate werden nicht in der Zertifikatliste Ihres Kontos angezeigt.

3. Die mobile App oder Webanwendung stellt dem Gerät das temporäre Bereitstellungsantragszertifikat zusammen mit allen erforderlichen Konfigurationsinformationen, z. B. WLAN-Anmeldeinformationen, zur Verfügung.
4. Das Gerät verwendet das temporäre Bereitstellungsantragszertifikat, um eine Verbindung zu AWS IoT mit dem AWS IoT Geräte SDKs - SDKs, Mobil- und AWS IoT Geräteclient herzustellen.
5. Das Gerät erhält ein permanentes Zertifikat und einen privaten Schlüssel, indem es innerhalb von fünf Minuten nach der Verbindung AWS IoT mit dem temporären Bereitstellungsanforderungszertifikat eine dieser Optionen verwendet. Das Gerät verwendet das Zertifikat und den Schlüssel, mit dem diese Optionen zurückgegeben werden, für alle future Authentifizierungen AWS IoT.

   a. Rufen Sie `CreateKeysAndCertificate`an, um mithilfe der Zertifizierungsstelle ein neues Zertifikat und einen neuen privaten Schlüssel zu erstellen. AWS

      Oder

b. Rufen Sie `CreateCertificateFromCsr` auf, um ein Zertifikat aus einer Zertifikatsignieranforderung zu generieren, das seinen privaten Schlüssel schützt.

> **Note**
>
> Denken Sie daran, ein gültiges Zertifikat innerhalb von fünf Minuten nach dem Herstellen der Verbindung AWS IoT mit dem temporären Bereitstellungsanspruch zurückzugeben `CreateKeysAndCertificate`oder `CreateCertificateFromCsr`müssen Sie es zurückgeben.

6. Das Gerät ruft `RegisterThing`auf, um das Gerät bei Cloud-Ressourcen zu registrieren AWS IoT und diese zu erstellen.

   Der Fleet-Provisioning-Service verwendet Bereitstellungsvorlagen, um Cloud-Ressourcen wie IoT-Objekte zu definieren und zu erstellen. Die Vorlage kann Attribute und Gruppen angeben, denen das Objekt angehört. Die Objektgruppen müssen vorhanden sein, damit das neue Objekt hinzugefügt werden kann.

7. Nach dem Speichern des permanenten Zertifikats auf dem Gerät muss das Gerät die Verbindung von der Sitzung trennen, die es mit dem temporären Bereitstellungsantragszertifikat initiiert hat, und erneut eine Verbindung mit dem permanenten Zertifikat herstellen.

Das Gerät ist jetzt bereit, normal mit dem Gerät zu kommunizieren AWS IoT.

## Verwenden von Pre-Provisioning-Hooks mit der AWS -CLI

Im folgenden Verfahren wird eine Bereitstellungsvorlage mit Pre-Provisioning-Hooks erstellt. Die hier verwendete Lambda-Funktion ist ein Beispiel, das geändert werden kann.

So erstellen Sie Pre-Provisioning-Hooks und übernehmen Sie für eine Bereitstellungsvorlage

1. Erstellen Sie eine Lambda-Funktion mit definierter Eingabe und Ausgabe. Lambda-Funktionen sind hochgradig anpassbar. Für die Erstellung von Pre-Provisioning-Hooks sind `allowProvisioning` und `parameterOverrides` erforderlich. Weitere Informationen zum Erstellen von Lambda-Funktionen finden Sie unter AWS Lambda Mit der AWS Befehlszeilenschnittstelle verwenden.

   Im Folgenden sehen Sie ein Beispiel für eine Lambda-Funktionsausgabe:

```
{
  "allowProvisioning": True,
  "parameterOverrides": {
    "incomingKey0": "incomingValue0",
    "incomingKey1": "incomingValue1"
  }
}
```

2. AWS IoT verwendet ressourcenbasierte Richtlinien, um Lambda aufzurufen. Sie müssen also die AWS IoT Erlaubnis zum Aufrufen Ihrer Lambda-Funktion erteilen.

> **Important**
>
> Achten Sie darauf, das `source-arn` oder `source-account` in die globalen Bedingungskontextschlüssel der Richtlinien aufzunehmen, die mit Ihrer Lambda-Aktion verknüpft sind, damit Berechtigungen nicht manipuliert werden können. Weitere Informationen hierzu finden Sie unter Serviceübergreifende Confused-Deputy-Prävention.

Es folgt ein Beispiel dafür, wie Sie IoT mit add-permission die Berechtigung zum Aufrufen Ihrer Lambda-Funktion erteilen.

```
aws lambda add-permission \
    --function-name myLambdaFunction \
    --statement-id iot-permission \
    --action lambda:InvokeFunction \
    --principal iot.amazonaws.com
```

3. Fügen Sie einer Vorlage mit dem Befehl oder einen Pre-Provisioning-Hook hinzu. create-provisioning-templateupdate-provisioning-template

Das folgende CLI-Beispiel verwendet die create-provisioning-template, um eine Bereitstellungsvorlage mit Pre-Provisioning-Hooks zu erstellen:

```
aws iot create-provisioning-template \
    --template-name myTemplate \
    --provisioning-role-arn arn:aws:iam:us-east-1:1234564789012:role/myRole \
    --template-body file://template.json \
```

```
    --pre-provisioning-hook file://hooks.json
```

Die Ausgabe dieses Befehls sieht wie folgt aus:

```
{
    "templateArn": "arn:aws:iot:us-east-1:1234564789012:provisioningtemplate/
myTemplate",
    "defaultVersionId": 1,
    "templateName": myTemplate
}
```

Sie können einen Parameter auch aus einer Datei laden, statt ihn als Befehlszeilen-Parameterwert einzugeben, um Zeit zu sparen. Weitere Informationen finden Sie unter Laden von AWS CLI -Parametern aus einer Datei. Im Folgenden wird der Parameter `template` im erweiterten JSON-Format gezeigt:

```
{
    "Parameters" : {
        "DeviceLocation": {
            "Type": "String"
        }
    },
    "Mappings": {
        "LocationTable": {
            "Seattle": {
                "LocationUrl": "https://example.aws"
            }
        }
    },
    "Resources" : {
        "thing" : {
            "Type" : "AWS::IoT::Thing",
            "Properties" : {
                "AttributePayload" : {
                    "version" : "v1",
                    "serialNumber" : "serialNumber"
                },
                "ThingName" : {"Fn::Join":["",["ThingPrefix_",
{"Ref":"SerialNumber"}]]},
                "ThingTypeName" : {"Fn::Join":["",["ThingTypePrefix_",
{"Ref":"SerialNumber"}]]},
                "ThingGroups" : ["widgets", "WA"],
```

```
                "BillingGroup": "BillingGroup"
            },
            "OverrideSettings" : {
                "AttributePayload" : "MERGE",
                "ThingTypeName" : "REPLACE",
                "ThingGroups" : "DO_NOTHING"
            }
        },
        "certificate" : {
            "Type" : "AWS::IoT::Certificate",
            "Properties" : {
                "CertificateId": {"Ref": "AWS::IoT::Certificate::Id"},
                "Status" : "Active",
                "ThingPrincipalType" : "EXCLUSIVE_THING"
            }
        },
        "policy" : {
            "Type" : "AWS::IoT::Policy",
            "Properties" : {
                "PolicyDocument" : {
                    "Version": "2012-10-17",
                    "Statement": [{
                        "Effect": "Allow",
                        "Action":["iot:Publish"],
                        "Resource": ["arn:aws:iot:us-east-1:504350838278:topic/foo/
bar"]
                    }]
                }
            }
        }
    },
    "DeviceConfiguration": {
        "FallbackUrl": "https://www.example.com/test-site",
        "LocationUrl": {
            "Fn::FindInMap": ["LocationTable",{"Ref": "DeviceLocation"},
 "LocationUrl"]}
    }
}
```

Im Folgenden wird der Parameter `pre-provisioning-hook` im erweiterten JSON-Format gezeigt:

```
{
```

```
    "targetArn" : "arn:aws:lambda:us-
east-1:765219403047:function:pre_provisioning_test",
    "payloadVersion" : "2020-04-01"
}
```

# Bereitstellen von Geräten mit Gerätezertifikaten

AWS IoT bietet drei Möglichkeiten zur Bereitstellung von Geräten, auf denen bereits ein Gerätezertifikat (und ein zugehöriger privater Schlüssel) vorhanden sind:

- Bereitstellung einzelner Objekte mithilfe einer Bereitstellungsvorlage. Diese Option eignet sich gut, wenn Sie Geräte nur einzeln bereitstellen müssen.
- Just-in-time Bereitstellung (JITP) mit einer Vorlage, die ein Gerät bereitstellt, wenn es zum ersten Mal eine Verbindung herstellt. AWS IoT Diese Option eignet sich gut, wenn Sie eine große Anzahl von Geräten anmelden müssen, jedoch keine Informationen über sie besitzen, die Sie als Massenbereitstellungsliste zusammenstellen können.
- Massenregistrierung. Mit dieser Option können Sie eine Liste von Bereitstellungsvorlagenwerten für einzelne Objekte angeben, die in einer Datei in einem S3-Bucket gespeichert werden. Dieser Ansatz eignet sich gut, wenn eine große Anzahl bekannter Geräte vorhanden ist, deren gewünschten Merkmale in einer Liste zusammengestellt werden können.

Themen


- Bereitstellung eines einzelnen Objekts
- Just-in-time Bereitstellung
- Massenregistrierung


## Bereitstellung eines einzelnen Objekts

Verwenden Sie die RegisterThingAPI oder den `register-thing` CLI-Befehl, um etwas bereitzustellen. Der CLI-Befehl `register-thing` verwendet die folgenden Argumente:

--template-body

Die Bereitstellungsvorlage.

--parameters

Eine Liste von Name/Wert-Paaren für die in der Bereitstellungsvorlage verwendeten Parameter im JSON-Format (z. B. `{"ThingName" : "MyProvisionedThing", "CSR" : "csr-text"}`).

Siehe Bereitstellen von Vorlagen.

RegisterThingoder `register-thing` gibt das ARNs für die Ressourcen und den Text des erstellten Zertifikats zurück:

```
{
    "certificatePem": "certificate-text",
    "resourceArns": {
    "PolicyLogicalName": "arn:aws:iot:us-
west-2:123456789012:policy/2A6577675B7CD1823E271C7AAD8184F44630FFD7",
    "certificate": "arn:aws:iot:us-west-2:123456789012:cert/
cd82bb924d4c6ccbb14986dcb4f40f30d892cc6b3ce7ad5008ed6542eea2b049",
    "thing": "arn:aws:iot:us-west-2:123456789012:thing/MyProvisionedThing"
    }
}
```

Wenn ein Parameter im Lexikon weggelassen wird, wird der Standardwert verwendet. Wenn kein Standardwert angegeben ist, wird der Parameter nicht durch einen Wert ersetzt.

## Just-in-time Bereitstellung

Sie können just-in-time Provisioning (JITP) verwenden, um Ihre Geräte bereitzustellen, wenn sie zum ersten Mal versuchen, eine Verbindung herzustellen. AWS IoT Zur Bereitstellung des Geräts müssen Sie die automatische Registrierung aktivieren und dem CA-Zertifikat, mit dem das Gerätezertifikat signiert wurde, eine Bereitstellungsvorlage zuordnen. Erfolge und Fehler bei der Bereitstellung werden wie Gerätebereitstellungsmetriken bei Amazon CloudWatch protokolliert.

Themen

- Überblick über JITP
- Registrieren einer CA mithilfe der Bereitstellungsvorlage
- Registrieren einer CA anhand des Bereitstellungsvorlagennamens

## Überblick über JITP

Wenn ein Gerät versucht, AWS IoT mithilfe eines Zertifikats, das mit einem registrierten CA-Zertifikat signiert ist, eine Verbindung herzustellen, wird die Vorlage aus dem CA-Zertifikat AWS IoT geladen und zum Aufrufen RegisterThingverwendet. Der JITP-Workflow registriert zuerst ein Zertifikat mit dem Statuswert `PENDING_ACTIVATION`. Wenn die Gerätebereitstellung abgeschlossen ist, wird der Status des Zertifikats in `ACTIVE` geändert.

AWS IoT definiert die folgenden Parameter, die Sie in Bereitstellungsvorlagen deklarieren und referenzieren können:

- `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`

Die Werte für diese Bereitstellungsvorlagenparameter werden auf die Angaben beschränkt, die JITP aus dem Betreff-Feld des Zertifikats des bereitzustellenden Geräts extrahieren kann. Das Zertifikat muss Werte für alle Parameter im Vorlagentext enthalten. Der `AWS::IoT::Certificate::Id`-Parameter bezieht sich auf eine intern generierte ID und nicht auf eine ID, die im Zertifikat enthalten ist. Sie können den Wert dieser ID mithilfe der `principal()` Funktion in einer AWS IoT Regel abrufen.

> **Note**
>
> Sie können Geräte mithilfe der AWS IoT Core just-in-time Bereitstellungsfunktion (JITP) bereitstellen, ohne die gesamte Vertrauenskette bei der ersten Verbindung eines Geräts an senden zu müssen. AWS IoT Core Die Vorlage des CA-Zertifikats ist optional, aber das Gerät muss die SNI-Erweiterung (Server Name Indication) senden, wenn es eine Verbindung mit AWS IoT Core herstellt.

## Beispielvorlagentext

Die folgende JSON-Datei ist ein Beispieltext für eine vollständige JITP-Vorlage.

```
{
   "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"
         }
      },
      "policy":{
         "Type":"AWS::IoT::Policy",
         "Properties":{
            "PolicyDocument":"{ \"Version\": \"2012-10-17\", \"Statement\": [{ \"Effect
\": \"Allow\", \"Action\":[\"iot:Publish\"], \"Resource\": [\"arn:aws:iot:us-
east-1:123456789012:topic/foo/bar\"] }] }"
         }
      }
   }
}
```

Diese Beispielvorlage deklariert Werte für die Bereitstellungsparameter `AWS::IoT::Certificate::CommonName`, `AWS::IoT::Certificate::SerialNumber`, `AWS::IoT::Certificate::Country` und `AWS::IoT::Certificate::Id`, die aus dem Zertifikat extrahiert und im Abschnitt `Resources` verwendet werden. Der JITP-Workflow führt anhand dieser Vorlage die folgenden Aktionen aus:

- Ein Zertifikat registrieren und als seinen Status PENDING_ACTIVE einstellen.
- Eine Objekt-Ressource erstellen.
- Eine Richtlinien-Ressource erstellen.
- Dem Zertifikat die Richtlinie anfügen.
- Dem Objekt das Zertifikat anfügen.
- Den Status des Zertifikats auf ACTIVE aktualisieren.

Die Gerätebereitstellung schlägt fehl, wenn das Zertifikat nicht alle Eigenschaften aufweist, die im `Parameters` Abschnitt von aufgeführt sind. `templateBody` Wenn `AWS::IoT::Certificate::Country` es beispielsweise in der Vorlage enthalten ist, das Zertifikat jedoch keine `Country`-Eigenschaft besitzt, schlägt die Gerätebereitstellung fehl.

Sie können es auch CloudTrail zur Behebung von Problemen mit Ihrer JITP-Vorlage verwenden. Informationen zu den Metriken, die bei Amazon protokolliert werden CloudWatch, finden Sie unterGerätebereitstellungsmetriken. Weitere Informationen zur Bereitstellungsvorlagen finden Sie unter Bereitstellungsvorlagen.

> **Note**
>
> Während des Bereitstellungsprozesses ruft das just-in-time Provisioning (JITP) andere API-Operationen auf der AWS IoT Kontrollebene auf. Diese Aufrufe können die für Ihr Konto festgelegten AWS IoT -Drosselungskontingente überschreiten und zu gedrosselten Aufrufen führen. Wenden Sie sich an den AWS -Kundenservice, um Ihre Drosselungskontingente bei Bedarf zu erhöhen.

## Registrieren einer CA mithilfe der Bereitstellungsvorlage

Gehen Sie folgendermaßen vor, um eine CA mithilfe einer vollständigen Bereitstellungsvorlage zu registrieren:

1. Speichern Sie Ihre Bereitstellungsvorlage und die ARN-Informationen der Rolle wie im folgenden Beispiel als JSON-Datei:

```
{
     "templateBody" : "{\r\n    \"Parameters\" : {\r\n
 \"AWS::IoT::Certificate::CommonName\": {\r\n            \"Type\": \"String\"\r
\n        },\r\n        \"AWS::IoT::Certificate::SerialNumber\": {\r\n
  \"Type\": \"String\"\r\n        },\r\n        \"AWS::IoT::Certificate::Country
\": {\r\n            \"Type\": \"String\"\r\n        },\r\n
 \"AWS::IoT::Certificate::Id\": {\r\n            \"Type\": \"String\"\r
\n        }\r\n    },\r\n    \"Resources\": {\r\n        \"thing\": {\r
\n            \"Type\": \"AWS::IoT::Thing\",\r\n            \"Properties
\": {\r\n                \"ThingName\": {\r\n                    \"Ref\":
 \"AWS::IoT::Certificate::CommonName\"\r\n                },\r\n
    \"AttributePayload\": {\r\n                    \"version\": \"v1\",\r\n
                    \"serialNumber\": {\r\n                        \"Ref\":
 \"AWS::IoT::Certificate::SerialNumber\"\r\n                    }\r\n
    },\r\n                \"ThingTypeName\": \"lightBulb-versionA\",\r\n
       \"ThingGroups\": [\r\n                    \"v1-lightbulbs\",\r\n
          {\r\n                        \"Ref\": \"AWS::IoT::Certificate::Country
\"\r\n                    }\r\n                ]\r\n            },\r\n
  \"OverrideSettings\": {\r\n                \"AttributePayload\": \"MERGE\",\r\n
```

```
                \"ThingTypeName\": \"REPLACE\",\r\n                \"ThingGroups
\": \"DO_NOTHING\"\r\n            }\r\n        },\r\n        \"certificate\": {\r
\n            \"Type\": \"AWS::IoT::Certificate\",\r\n            \"Properties
\": {\r\n                \"CertificateId\": {\r\n                    \"Ref\":
 \"AWS::IoT::Certificate::Id\"\r\n                },\r\n                \"Status\":
 \"ACTIVE\"\r\n            },\r\n            \"OverrideSettings\": {\r\n
     \"Status\": \"DO_NOTHING\"\r\n            }\r\n        },\r\n        \"policy
\": {\r\n            \"Type\": \"AWS::IoT::Policy\",\r\n            \"Properties
\": {\r\n                \"PolicyDocument\": \"{ \\\"Version\\\": \\\"2012-10-17\
\\", \\\"Statement\\\": [{ \\\"Effect\\\": \\\"Allow\\\", \\\"Action\\\":[\\
\"iot:Publish\\\"], \\\"Resource\\\": [\\\"arn:aws:iot:us-east-1:123456789012:topic
\/foo\/bar\\\"] }] }\"\r\n            }\r\n        }\r\n    }\r\n}",
     "roleArn" : "arn:aws:iam::123456789012:role/JITPRole"
}
```

In diesem Beispiel muss der Wert des Feldes `templateBody` ein JSON-Objekt sein, das als Zeichenfolge mit Escapezeichen angegeben wird. Zulässig sind nur die Werte in der obigen Liste. Sie können eine Vielzahl von Tools verwenden, um die erforderliche JSON-Ausgabe zu erstellen, z. B. `json.dumps` (Python) oder `JSON.stringify` (Node). Der Wert von Feld `roleARN` muss der ARN einer Rolle sein, der `AWSIoTThingsRegistration` zugeordnet ist. Außerdem können Sie in Ihrer Vorlage `PolicyName` anstelle des Inline-`PolicyDocument` wie im Beispiel verwenden.

2. Registrieren Sie ein CA-Zertifikat mit der Operation Register CACertificate API oder dem `register-ca-certificate`CLI-Befehl. Geben Sie das Verzeichnis der Bereitstellungsvorlage und die ARN-Informationen der Rolle an, die Sie im vorherigen Schritt gespeichert haben:

   Im Folgenden finden Sie ein Beispiel für die Registrierung eines CA-Zertifikats im `DEFAULT`-Modus mithilfe von AWS CLI:

   ```
   aws iot register-ca-certificate --ca-certificate file://your-ca-cert --
   verification-cert file://your-verification-cert
                   --set-as-active --allow-auto-registration --registration-config
    file://your-template
   ```

   Im Folgenden finden Sie ein Beispiel für die Registrierung eines CA-Zertifikats im `SNI_ONLY`-Modus mithilfe von AWS CLI:

   ```
   aws iot register-ca-certificate --ca-certificate file://your-ca-cert --certificate-
   mode SNI_ONLY
   ```

```
                --set-as-active --allow-auto-registration --registration-config
 file://your-template
```

Weitere Informationen finden Sie unter Registrieren Ihres CA-Zertifikats.

3. (Optional) Aktualisieren Sie die Einstellungen für ein CA-Zertifikat mithilfe des CACertificateAPI-Aktualisierungsvorgangs oder des `update-ca-certificate`CLI-Befehls.

   Im Folgenden finden Sie ein Beispiel für die Aktualisierung eines CA-Zertifikats mithilfe von AWS CLI:

   ```
   aws iot update-ca-certificate --certificate-id caCertificateId
                   --new-auto-registration-status ENABLE --registration-config
    file://your-template
   ```

## Registrieren einer CA anhand des Bereitstellungsvorlagennamens

Gehen Sie folgendermaßen vor, um eine CA mit einem Bereitstellungsvorlagennamen zu registrieren:

1. Speichern Sie den Text Ihrer Bereitstellungsvorlage als JSON-Datei. Einen Beispielvorlagentext finden Sie unter Beispielvorlagentext.
2. Verwenden Sie die CreateProvisioningTemplateAPI oder den `create-provisioning-template`CLI-Befehl, um eine Bereitstellungsvorlage zu erstellen:

   ```
   aws iot create-provisioning-template --template-name your-template-name \
           --template-body file://your-template-body.json --type JITP \
           --provisioning-role-arn arn:aws:iam::123456789012:role/test
   ```

   > **Note**
   >
   > Für die just-in-time Bereitstellung (JITP) müssen Sie den Vorlagentyp angeben, der `JITP` bei der Erstellung der Bereitstellungsvorlage verwendet werden soll. Weitere Informationen zum Vorlagentyp finden Sie CreateProvisioningTemplatein der AWS API-Referenz.

3. Verwenden Sie die Register CACertificate API oder den `register-ca-certificate`CLI-Befehl, um CA mit dem Vorlagennamen zu registrieren:

```
aws iot register-ca-certificate --ca-certificate file://your-ca-cert --
verification-cert file://your-verification-cert \
        --set-as-active --allow-auto-registration --registration-config
 templateName=your-template-name
```

## Massenregistrierung

Mit dem Befehl `start-thing-registration-task` können Sie viele Objekte gemeinsam registrieren. Dieser Befehl verwendet eine Bereitstellungsvorlage, den Namen eines S3;-Buckets, einen Schlüsselnamen und einen Rollen-ARN, der den Zugriff auf die Datei in dem S3-Bucket ermöglicht. Die Datei in dem S3-Bucket enthält die Werte, die die Parameter in der Vorlage ersetzen. Dabei muss es sich um eine JSON-Datei mit Trennung durch neue Zeilen handeln. Jede Zeile enthält alle Parameterwerte für die Registrierung eines einzelnen Geräts. Zum Beispiel:

```
{"ThingName": "foo", "SerialNumber": "123", "CSR": "csr1"}
{"ThingName": "bar", "SerialNumber": "456", "CSR": "csr2"}
```

Folgende API-Operationen können im Zusammenhang mit der Massenregistrierung nützlich sein:

- ListThingRegistrationTasks: Führt die aktuellen Aufgaben zur Massenbereitstellung von Dingen auf.
- DescribeThingRegistrationTask: Stellt Informationen zu einer bestimmten Aufgabe zur Massenregistrierung von Dingen bereit.
- StopThingRegistrationTask: Stoppt eine Aufgabe zur Massenregistrierung von Dingen.
- ListThingRegistrationTaskReports: Wird verwendet, um die Ergebnisse und Fehler einer Aufgabe zur Massenregistrierung von Dingen zu überprüfen.

> **Note**
>
> - Es kann jeweils nur ein Massenregistrierungsvorgang gleichzeitig durchgeführt werden (pro Konto).
> - Bei der Massenregistrierung werden andere API-Operationen auf der AWS IoT Steuerungsebene aufgerufen. Diese Abrufe können die AWS IoT -Drosselungskontingente

in Ihrem Konto überschreiten und Drosselungsfehler verursachen. Wenden Sie sich bei Bedarf an den AWS Kundensupport, um Ihre AWS IoT Drosselungsquoten zu erhöhen.

# Bereitstellen von Vorlagen

Eine Bereitstellungsvorlage ist ein JSON-Dokument, das Parameter verwendet, um die Ressourcen zu beschreiben, die Ihr Gerät für die Interaktion verwenden muss. AWS IoT Eine Bereitstellungsvorlage besteht aus zwei Abschnitten: `Parameters` und `Resources`. Es gibt zwei Arten von Bereitstellungsvorlagen in. AWS IoT Eine wird für die just-in-time Bereitstellung (JITP) und die Massenregistrierung verwendet, die zweite für die Flottenbereitstellung.

Themen


- Bereich "Parameters"
- Bereich „Ressourcen“
- Vorlagenbeispiel für eine Massenregistrierung
- Beispiel für eine Vorlage für die just-in-time Bereitstellung (JITP)
- Flottenbereitstellung


## Bereich "Parameters"

Der Abschnitt `Parameters` deklariert die im Abschnitt `Resources` verwendeten Parameter. Jeder Parameter deklariert einen Namen, einen Typ und einen optionalen Standardwert. Der Standardwert wird verwendet, wenn das mit der Vorlage eingegebene Lexikon keinen Wert für den Parameter enthält. Der Abschnitt `Parameters` eines Vorlagendokuments sieht wie folgt aus:

```
{
    "Parameters" : {
        "ThingName" : {
            "Type" : "String"
        },
        "SerialNumber" : {
            "Type" : "String"
        },
        "Location" : {
            "Type" : "String",
            "Default" : "WA"
        },
```

```
        "CSR" : {
            "Type" : "String"
        }
    }
}
```

Dieses Vorlagentextfragment deklariert vier Parameter: `ThingName`, `SerialNumber`, `Location` und `CSR`. Alle diese Parameter sind vom Typ `String`. Der Parameter `Location` deklariert den Standardwert `"WA"`.

## Bereich „Ressourcen“

Im `Resources` Abschnitt des Vorlagentexts werden die Ressourcen deklariert, die für die Kommunikation Ihres Geräts erforderlich sind AWS IoT: eine Sache, ein Zertifikat und eine oder mehrere IoT-Richtlinien. Jede Ressource gibt einen logischen Namen, einen Typ und eine Reihe von Eigenschaften an.

Ein logischer Name ermöglicht den Verweis auf eine Ressource an einer anderen Stelle in der Vorlage.

Der Typ gibt die Art der Ressource an, die Sie deklarieren. Gültige Typen sind:

- `AWS::IoT::Thing`
- `AWS::IoT::Certificate`
- `AWS::IoT::Policy`

Die Eigenschaften, die Sie angeben, hängen vom Typ der Ressource ab, die Sie deklarieren.

### Objektressourcen

Objekt-Ressourcen werden mit den folgenden Eigenschaften deklariert:

- `ThingName`: Zeichenfolge.
- `AttributePayload`: Optional. Eine Liste von Name-Wert-Paaren.
- `ThingTypeName`: Optional. Zeichenfolge für einen zugehörigen Objekttyp für das Objekt.
- `ThingGroups`: Optional. Eine Liste der Gruppen, zu der das Objekt gehört.
- `BillingGroup`: Optional. Zeichenfolge für den Namen einer zugehörigen Fakturierungsgruppe.
- `PackageVersions`: Optional. Zeichenfolge für ein zugeordnetes Paket und Versionsnamen.

## Zertifikatressourcen

Sie können Zertifikate auf eine der folgenden Arten angeben:

- Eine Zertifikatssignierungsanforderung (Certificate Signing Request, CSR).
- Eine Zertifikat-ID eines vorhandenen Geräte-Zertifikats. (Nur ein Zertifikat IDs kann mit einer Flottenbereitstellungsvorlage verwendet werden.)
- Ein Geräte-Zertifikat mit einem für AWS IoT registrierten CA-Zertifikat. Wenn Sie über mehr als ein mit demselben Themafeld registriertes CA-Zertifikat verfügen, müssen Sie auch das verwendete CA-Zertifikat eingeben, um das Geräte-Zertifikat zu signieren.

> **Note**
>
> Wenn Sie ein Zertifikat in einer Vorlage deklarieren, verwenden Sie nur eine dieser Methoden. Wenn Sie z. B. eine Zertifikatsignierungsanforderung (CSR) verwenden, können Sie nicht auch eine Zertifikat-ID oder ein Geräte-Zertifikat angeben. Weitere Informationen finden Sie unter X.509-Clientzertifikate.

Weitere Informationen finden Sie unter Übersicht zum X.509-Zertifikat.

Zertifikat-Ressourcen werden mit den folgenden Eigenschaften deklariert:

- `CertificateSigningRequest`: Zeichenfolge.
- `CertificateId`: Zeichenfolge.
- `CertificatePem`: Zeichenfolge.
- `CACertificatePem`: Zeichenfolge.
- `Status`: Optional. Zeichenfolge, die `ACTIVE` oder `INACTIVE` sein kann. Der Standardwert ist ACTIVE.
- `ThingPrincipalType`: Optional. Zeichenfolge, die die Art der Beziehung zwischen dem Ding und dem Prinzipal (dem Zertifikat) angibt.
  - `EXCLUSIVE_THING`: Stellt eine exklusive Beziehung her. Der Schulleiter kann nur dieser bestimmten Sache zugeordnet werden und keiner anderen.
  - `NON_EXCLUSIVE_THING`: Ordnet den Dingen den angegebenen Prinzipal zu. Sie können mehrere Dinge an den Prinzipal anhängen. Dies ist der Standardwert, sofern er nicht angegeben ist.

> **Note**
>
> Sie können Geräte auch ohne Gerätezertifikate bereitstellen. Weitere Informationen finden Sie unter Bereitstellen von Geräten ohne Gerätezertifikate mithilfe der Flottenbereitstellung.

Beispiele:

- Zertifikat, das mit einer Zertifikatsignierungsanforderung (CSR) angegeben wird:

```
{
    "certificate" : {
        "Type" : "AWS::IoT::Certificate",
        "Properties" : {
            "CertificateSigningRequest": {"Ref" : "CSR"},
            "Status" : "ACTIVE"
        }
    }
}
```

- Zertifikat, das mit einer vorhandenen Zertifikat-ID angegeben wird:

```
{
    "certificate" : {
        "Type" : "AWS::IoT::Certificate",
        "Properties" : {
            "CertificateId": {"Ref" : "CertificateId"}
        }
    }
}
```

- Zertifikat, das mit der PEM-Datei eines vorhandenen Zertifikats und der PEM-Datei einer vorhandenen Zertifizierungsstelle angegeben wird:

```
{
    "certificate" : {
        "Type" : "AWS::IoT::Certificate",
        "Properties" : {
            "CACertificatePem": {"Ref" : "CACertificatePem"},
            "CertificatePem": {"Ref" : "CertificatePem"}
        }
```

```
    }
}
```

- Ordnen Sie einem Principal ausschließlich eine Sache zu:

```
{
    "certificate" : {
        "Type" : "AWS::IoT::Certificate",
        "Properties" : {
            "ThingPrincipalType" : "EXCLUSIVE_THING"
        }
    }
}
```

## Richtlinienressourcen

Richtlinien-Ressourcen werden mit einer der folgenden Eigenschaften deklariert:

- `PolicyName`: Optional. Zeichenfolge. Standardmäßig eine Prüfsumme des Richtliniendokuments. `PolicyName` kann nur auf AWS IoT -Richtlinien verweisen, nicht jedoch auf IAM-Richtlinien. Wenn Sie eine vorhandene AWS IoT -Richtlinie verwenden, geben Sie für die Eigenschaft `PolicyName` den Namen der Richtlinie ein. Verwenden Sie nicht die Eigenschaft `PolicyDocument`.
- `PolicyDocument`: Optional. Ein JSON-Objekt, das als Zeichenfolge mit Escapezeichen angegeben wird. Wenn `PolicyDocument` nicht angegeben wird, muss die Richtlinie bereits erstellt worden sein.

> **Note**
>
> Wenn ein `Policy`-Abschnitt vorhanden ist, muss `PolicyName` oder `PolicyDocument`, nicht aber beide, angegeben werden.

## Überschreibungseinstellungen

Wenn eine Vorlage eine Ressource angibt, die bereits vorhanden ist, ermöglicht der Abschnitt `OverrideSettings` die Angabe der durchzuführenden Aktion:

`DO_NOTHING`

Die Ressource unverändert lassen

`REPLACE`

Die Ressource durch die in der Vorlage angegebene Ressource ersetzen.

`FAIL`

Die Anfrage mit einer `ResourceConflictsException` fehlschlagen lassen.

`MERGE`

Dies gilt nur für die Eigenschaften `ThingGroups` und `AttributePayload` eines `thing`. Kombinieren der vorhandenen Attribute oder Gruppenmitgliedschaften des Objekts mit denjenigen, die in der Vorlage spezifiziert sind.

Wenn Sie eine Ding-Ressource deklarieren, können Sie `OverrideSettings` für die folgenden Eigenschaften angeben:

- `ATTRIBUTE_PAYLOAD`
- `THING_TYPE_NAME`
- `THING_GROUPS`

Wenn Sie eine Zertifikat-Ressource deklarieren, können Sie `OverrideSettings` für die `Status`-Eigenschaft angeben.

`OverrideSettings` stehen nicht für Richtlinienressourcen zur Verfügung.

## Ressourcenbeispiel

Das folgende Vorlagenfragment deklariert ein Objekt, ein Zertifikat und eine Richtlinie:

```
{
    "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"
            }
        },
        "policy" : {
            "Type" : "AWS::IoT::Policy",
            "Properties" : {
                "PolicyDocument" : "{ \"Version\": \"2012-10-17\", \"Statement
\": [{ \"Effect\": \"Allow\", \"Action\":[\"iot:Publish\"], \"Resource\":
 [\"arn:aws:iot:us-east-1:123456789012:topic/foo/bar\"] }] }"
            }
        }
    }
}
```

Das Objekt wird deklariert mit:

- Dem logischen Namen `"thing"`.
- Dem Typ `AWS::IoT::Thing`.
- Einer Reihe von Objekteigenschaften.

  Zu den Objekteigenschaften gehören der Name des Objekts, eine Reihe von Attributen, ein optionaler Name für den Objekttyp sowie eine optionale Liste von Objektgruppen, zu denen das Objekt gehört.

Parameter werden von `{"Ref":"`*`parameter-name`*`"}` referenziert. Wenn die Vorlage evaluiert wird, werden die Parameter durch den Parameterwert aus dem mit der Vorlage eingegebenen Lexikon ersetzt.

Das Zertifikat wird deklariert mit:

- Dem logischen Namen `"certificate"`.
- Dem Typ `AWS::IoT::Certificate`.
- Einer Reihe von Eigenschaften.

  Zu den Eigenschaften gehören die CSR für das Zertifikat und die Einstellung des Status auf `ACTIVE`. Der CSR-Text wird als Parameter in das mit der Vorlage eingegebene Lexikon eingegeben.

Die Richtlinie wird deklariert mit:

- Dem logischen Namen `"policy"`.
- Dem Typ `AWS::IoT::Policy`.
- Dem Namen einer vorhandenen Richtlinie oder dem Richtliniendokument.

## Vorlagenbeispiel für eine Massenregistrierung

Die folgende JSON-Datei ist ein Beispiel für eine vollständige Bereitstellungsvorlage, die das Zertifikat mit einer Zertifikatsignierungsanforderung angibt:

(Der Feldwert `PolicyDocument` muss ein JSON-Objekt sein, da als Zeichenfolge mit Escapezeichen angegeben wird.)

```
{
    "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",
                "ThingPrincipalType" : "EXCLUSIVE_THING"
            }
        },
        "policy" : {
            "Type" : "AWS::IoT::Policy",
            "Properties" : {
                "PolicyDocument" : "{ \"Version\": \"2012-10-17\", \"Statement
\": [{ \"Effect\": \"Allow\", \"Action\":[\"iot:Publish\"], \"Resource\":
 [\"arn:aws:iot:us-east-1:123456789012:topic/foo/bar\"] }] }"
            }
        }
    }
}
```

## Beispiel für eine Vorlage für die just-in-time Bereitstellung (JITP)

Die folgende JSON-Datei ist ein Beispiel für eine vollständige Bereitstellungsvorlage, die ein vorhandenes Zertifikat mit einer Zertifikat-ID angibt:

```
{
   "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",
               "ThingPrincipalType" : "EXCLUSIVE_THING"
            }
         },
         "policy":{
```

```
         "Type":"AWS::IoT::Policy",
         "Properties":{
            "PolicyDocument":"{ \"Version\": \"2012-10-17\", \"Statement\": [{ \"Effect
\": \"Allow\", \"Action\":[\"iot:Publish\"], \"Resource\": [\"arn:aws:iot:us-
east-1:123456789012:topic/foo/bar\"] }] }"
         }
      }
   }
}
```

> **Important**
>
> Sie müssen `CertificateId` in einer Vorlage verwenden, die für die JIT-Bereitstellung verwendet wird.

Weitere Informationen zum Typ einer Bereitstellungsvorlage finden Sie `CreateProvisioningTemplate`in der AWS API-Referenz.

Weitere Informationen zur Verwendung dieser Vorlage für die Bereitstellung finden Sie unter: J just-in-time ust-in-time Provisioning.

## Flottenbereitstellung

Vorlagen für die Flottenbereitstellung werden von verwendet AWS IoT , um die Cloud- und Gerätekonfiguration einzurichten. Diese Vorlagen verwenden dieselben Parameter und Ressourcen wie die JITP- und Massenregistrierungsvorlagen. Weitere Informationen finden Sie unter Bereitstellen von Vorlagen. Flottenbereitstellungsvorlagen können einen `Mapping`-Abschnitt und einen `DeviceConfiguration`-Abschnitt enthalten. Sie können intrinsische Funktionen innerhalb einer Flottenbereitstellungsvorlage verwenden, um die gerätespezifische Konfiguration zu generieren. Vorlagen für die Flottenbereitstellung werden als Ressourcen bezeichnet und sind gekennzeichnet durch ARNs (z. B.`arn:aws:iot:us-west-2:1234568788:provisioningtemplate/`*`templateName`*).

### Mappings

Im optionalen Abschnitt `Mappings` werden Schlüssel einem Satz benannter Werte zugewiesen. Wenn Sie beispielsweise Werte auf der Grundlage einer AWS Region festlegen möchten, können Sie eine Zuordnung erstellen, die den AWS-Region Namen als Schlüssel verwendet und die Werte

enthält, die Sie für jede spezifische Region angeben möchten. Zum Abrufen von Werten aus einer Karte nutzen Sie die intrinsische Funktion `Fn::FindInMap`.

Im Abschnitt `Mappings` dürfen keine Parameter, Pseudoparameter verwendet oder intrinsische Funktionen aufgerufen werden.

### Gerätekonfiguration

Der Abschnitt „Gerätekonfiguration“ enthält beliebige Daten, die Sie bei der Bereitstellung an Ihre Geräte senden möchten. Zum Beispiel:

```
{
    "DeviceConfiguration": {
        "Foo":"Bar"
    }
}
```

Wenn Sie Nachrichten mithilfe des Payload-Formats JavaScript Object Notation (JSON) an Ihre Geräte senden, AWS IoT Core formatieren Sie diese Daten als JSON. Wenn Sie das Payload-Format Concise Binary Object Representation (CBOR) verwenden, AWS IoT Core formatiert Sie diese Daten als CBOR. Der Abschnitt `DeviceConfiguration` unterstützt keine verschachtelten JSON-Objekte.

### Intrinsische Funktionen

Intrinsische Funktionen werden in jedem Abschnitt der Bereitstellungsvorlage mit Ausnahme des `Mappings`-Abschnitts verwendet.

`Fn::Join`

Fügt einem einzelnen Wert eine Gruppe von Werten getrennt durch das angegebene Trennzeichen an. Wenn das Trennzeichen eine leere Zeichenfolge ist, dann werden die Werte ohne Trennzeichen verkettet.

> **Important**
>
> `Fn::Join` wird nicht für the section called “Richtlinienressourcen” unterstützt.

`Fn::Select`

Gibt ein einzelnes Objekt aus einer Liste von Objekten nach Index zurück.

> **Important**
>
> `Fn::Select` überprüft nicht auf `null`-Werte oder ob sich der Index außerhalb des Arrays befindet. Beide Bedingungen führen zu einem Bereitstellungsfehler. Stellen Sie daher sicher, dass Sie einen gültigen Indexwert ausgewählt haben und die Liste Werte enthält, die nicht Null sind.

`Fn::FindInMap`

Gibt die Werte von Schlüsseln in einer Zwei-Ebenen-Karte zurück, die im Abschnitt `Mappings` deklariert ist.

`Fn::Split`

Teilt eine Zeichenfolge in eine Liste von Zeichenfolgenwerten auf, sodass Sie ein Element aus der Liste der Zeichenfolgen auswählen können. Sie geben ein Trennzeichen an, das bestimmt, wo die Zeichenfolge geteilt wird (z. B. ein Komma). Nachdem Sie eine Zeichenfolge geteilt haben, verwenden Sie `Fn::Select`, um ein Element auszuwählen.

Wenn beispielsweise eine durch Kommas getrennte Zeichenfolge eines Subnetzes in Ihre Stack-Vorlage importiert IDs wird, können Sie die Zeichenfolge bei jedem Komma aufteilen. Verwenden Sie diese Option aus der Liste der Subnetze IDs, `Fn::Select` um eine Subnetz-ID für eine Ressource anzugeben.

`Fn::Sub`

Sie können Variablen in einer Eingabezeichenfolge mit Werten ersetzen, die Sie angeben. Sie können diese Funktion verwenden, um Befehle oder Ausgaben mit Werten zu erstellen, die erst verfügbar sind, wenn Sie ein Stack erstellen oder aktualisieren.

## Beispiel einer Flottenbereitstellungsvorlage

```
{
    "Parameters" : {
        "ThingName" : {
            "Type" : "String"
        },
        "SerialNumber": {
            "Type": "String"
        },
```

```
        "DeviceLocation": {
            "Type": "String"
        }
    },
    "Mappings": {
        "LocationTable": {
            "Seattle": {
                "LocationUrl": "https://example.aws"
            }
        }
    },
    "Resources" : {
        "thing" : {
            "Type" : "AWS::IoT::Thing",
            "Properties" : {
                "AttributePayload" : {
                    "version" : "v1",
                    "serialNumber" : "serialNumber"
                },
                "ThingName" : {"Ref" : "ThingName"},
                "ThingTypeName" : {"Fn::Join":["",["ThingPrefix_",
{"Ref":"SerialNumber"}]]},
                "ThingGroups" : ["v1-lightbulbs", "WA"],
                "BillingGroup": "LightBulbBillingGroup"
            },
            "OverrideSettings" : {
                "AttributePayload" : "MERGE",
                "ThingTypeName" : "REPLACE",
                "ThingGroups" : "DO_NOTHING"
            }
        },
        "certificate" : {
            "Type" : "AWS::IoT::Certificate",
            "Properties" : {
                "CertificateId": {"Ref": "AWS::IoT::Certificate::Id"},
                "Status" : "Active",
                "ThingPrincipalType" : "EXCLUSIVE_THING"
            }
        },
        "policy" : {
            "Type" : "AWS::IoT::Policy",
            "Properties" : {
                "PolicyDocument" : {
                    "Version": "2012-10-17",
```

```
                    "Statement": [{
                        "Effect": "Allow",
                        "Action":["iot:Publish"],
                        "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/foo/
bar"]
                    }]
                }
            }
        }
    },
    "DeviceConfiguration": {
        "FallbackUrl": "https://www.example.com/test-site",
        "LocationUrl": {
            "Fn::FindInMap": ["LocationTable",{"Ref": "DeviceLocation"},
 "LocationUrl"]}
        }
}
```

> **Note**
>
> Eine vorhandene Bereitstellungsvorlage kann aktualisiert werden, um einen Pre-Provisioning-Hook hinzuzufügen.

## Pre-Provisioning-Hooks

AWS empfiehlt, bei der Erstellung von Provisioning-Vorlagen Hook-Funktionen vor der Bereitstellung zu verwenden, um mehr Kontrolle darüber zu haben, welche und wie viele Geräte Ihr Konto integriert. Pre-Provisioning-Hooks sind Lambda-Funktionen, die vom Gerät übergebene Parameter überprüfen, bevor das Gerät bereitgestellt werden kann. Diese Lambda-Funktion muss in Ihrem Konto vorhanden sein, bevor Sie ein Gerät bereitstellen, da sie jedes Mal aufgerufen wird, wenn ein Gerät eine Anfrage über the section called “RegisterThing” sendet.

> **Important**
>
> Achten Sie darauf, das `source-arn` oder `source-account` in die globalen Bedingungskontextschlüssel der Richtlinien aufzunehmen, die mit Ihrer Lambda-Aktion verknüpft sind, damit Berechtigungen nicht manipuliert werden können. Weitere Informationen hierzu finden Sie unter Serviceübergreifende Confused-Deputy-Prävention.

Damit Geräte bereitgestellt werden können, muss Ihre Lambda-Funktion das Eingabeobjekt akzeptieren und das in diesem Abschnitt beschriebene Ausgabeobjekt zurückgeben.
Die Bereitstellung wird nur fortgesetzt, wenn die Lambda-Funktion ein Objekt mit `"allowProvisioning": True` zurückgibt.

## Pre-Provisioning-Hook-Eingabe

AWS IoT sendet dieses Objekt an die Lambda-Funktion, wenn sich ein Gerät bei AWS IoT registriert.

```
{
    "claimCertificateId" : "string",
    "certificateId" : "string",
    "certificatePem" : "string",
    "templateArn" : "arn:aws:iot:us-east-1:1234567890:provisioningtemplate/MyTemplate",
    "clientId" : "221a6d10-9c7f-42f1-9153-e52e6fc869c1",
    "parameters" : {
        "string" : "string",
        ...
    }
}
```

Das an die Lambda-Funktion übergebene `parameters`-Objekt enthält die Eigenschaften im `parameters`-Argument, das in der the section called “RegisterThing”-Anforderungsnutzlast übergeben wird.

## Pre-Provisioning-Hook-Rückgabewert

Die Lambda-Funktion muss eine Antwort zurückgeben, die angibt, ob sie die Bereitstellungsanforderung und die Werte der zu überschreibenden Eigenschaften autorisiert hat.

Im Folgenden finden Sie ein Beispiel für eine erfolgreiche Antwort der Pre-Provisioning-Funktion.

```
{
    "allowProvisioning": true,
    "parameterOverrides" : {
        "Key": "newCustomValue",
        ...
    }
}
```

`"parameterOverrides"`-Werte werden dem Parameter `"parameters"` in der the section called “RegisterThing”-Anforderungsnutzlast hinzugefügt.

> **Note**
>
> - Wenn die Lambda-Funktion fehlschlägt, schlägt die Bereitstellungsanforderung fehl `ACCESS_DENIED` und ein Fehler wird in Logs protokolliert. CloudWatch
> - Wenn die Lambda-Funktion in der Antwort nicht `"allowProvisioning": "true"` zurückgibt, schlägt die Bereitstellungsanforderung mit `ACCESS_DENIED` fehl.
> - Die Lambda-Funktion muss die Ausführung beenden und innerhalb von 5 Sekunden zurückgeben, andernfalls schlägt die Bereitstellungsanforderung fehl.

## Lambda-Beispiel für einen Pre-Provisioning-Hook

Python

Ein Beispiel für einen Pre-Provisioning-Hook ist Lambda in Python.

```
import json

def pre_provisioning_hook(event, context):
    print(event)

    return {
        'allowProvisioning': True,
        'parameterOverrides': {
            'DeviceLocation': 'Seattle'
        }
    }
```

Java

Ein Beispiel für einen Pre-Provisioning-Hook ist Lambda in Java.

Handler-Klasse

```
package example;

import java.util.Map;
```

```
import java.util.HashMap;
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;

public class PreProvisioningHook implements
 RequestHandler<PreProvisioningHookRequest, PreProvisioningHookResponse> {

    public PreProvisioningHookResponse handleRequest(PreProvisioningHookRequest
 object, Context context) {
        Map<String, String> parameterOverrides = new HashMap<String, String>();
        parameterOverrides.put("DeviceLocation", "Seattle");

        PreProvisioningHookResponse response = PreProvisioningHookResponse.builder()
                .allowProvisioning(true)
                .parameterOverrides(parameterOverrides)
                .build();

        return response;
    }

}
```

Anforderungsklasse:

```
package example;

import java.util.Map;
import lombok.Builder;
import lombok.Data;
import lombok.AllArgsConstructor;
import lombok.NoArgsConstructor;

@Data
@Builder
@AllArgsConstructor
@NoArgsConstructor
public class PreProvisioningHookRequest {
    private String claimCertificateId;
    private String certificateId;
    private String certificatePem;
    private String templateArn;
    private String clientId;
    private Map<String, String> parameters;
```

```
}
```

Response-Klasse:

```
package example;

import java.util.Map;
import lombok.Builder;
import lombok.Data;
import lombok.AllArgsConstructor;
import lombok.NoArgsConstructor;


@Data
@Builder
@AllArgsConstructor
@NoArgsConstructor
public class PreProvisioningHookResponse {
    private boolean allowProvisioning;
    private Map<String, String> parameterOverrides;
}
```

JavaScript

Ein Beispiel für einen Pre-Provisioning-Hook Lambda in. JavaScript

```
exports.handler = function(event, context, callback) {
    console.log(JSON.stringify(event, null, 2));
    var reply = {
        allowProvisioning: true,
        parameterOverrides: {
            DeviceLocation: 'Seattle'
        }
     };
     callback(null, reply);
}
```

# Selbstverwaltete Zertifikatsignierung mithilfe des Zertifikatsanbieters AWS IoT Core

Sie können einen AWS IoT Core Zertifikatsanbieter erstellen, um Zertifikatssignieranfragen (CSRs) bei der AWS IoT Flottenbereitstellung zu signieren. Ein Zertifikatsanbieter verweist auf eine Lambda-Funktion und die `CreateCertificateFromCsr`MQTT-API für die Flottenbereitstellung. Die Lambda-Funktion akzeptiert eine CSR und gibt ein signiertes Client-Zertifikat zurück.

Wenn Sie keinen Zertifikatsanbieter bei sich haben AWS-Konto, wird die CreateCertificateFromCsr MQTT-API bei der Flottenbereitstellung aufgerufen, um das Zertifikat aus einer CSR zu generieren. Nachdem Sie einen Zertifikatsanbieter erstellt haben, ändert sich das Verhalten der CreateCertificateFromCsr MQTT-API und alle Aufrufe dieser MQTT-API rufen den Zertifikatsanbieter auf, um das Zertifikat auszustellen.

Mit dem AWS IoT Core Zertifikatsanbieter können Sie Lösungen implementieren, die private Zertifizierungsstellen (CAs) wie AWS Private CAandere öffentlich vertrauenswürdige oder Ihre eigene Public Key Infrastructure (PKI) verwenden CAs, um die CSR zu signieren. Darüber hinaus können Sie den Zertifikatsanbieter verwenden, um die Felder Ihres Client-Zertifikats wie Gültigkeitszeiträume, Signaturalgorithmen, Aussteller und Erweiterungen anzupassen.

> **Important**
>
> Sie können jeweils nur einen Zertifikatsanbieter erstellen. AWS-Konto Die Änderung des Signierverhaltens gilt für die gesamte Flotte, die die CreateCertificateFromCsr MQTT-API aufruft, bis Sie den Zertifikatsanbieter aus Ihrem AWS-Konto löschen.

In diesem Thema:


- So funktioniert die selbstverwaltete Zertifikatsignierung bei der Flottenbereitstellung
- Eingabe der Lambda-Funktion des Zertifikatsanbieters
- Rückgabewert der Lambda-Funktion des Zertifikatsanbieters
- Beispiel-Lambda-Funktion
- Selbstverwaltete Zertifikatsignierung für die Flottenbereitstellung
- AWS CLI Befehle für den Zertifikatsanbieter

# So funktioniert die selbstverwaltete Zertifikatsignierung bei der Flottenbereitstellung

## Die wichtigsten Konzepte

Die folgenden Konzepte enthalten Einzelheiten, anhand derer Sie verstehen können, wie die selbstverwaltete Zertifikatsignierung bei der Flottenbereitstellung funktioniert. AWS IoT Weitere Informationen finden Sie unter Bereitstellen von Geräten ohne Gerätezertifikate mithilfe von Fleet Provisioning.

AWS IoT Flottenbereitstellung

> Mit AWS IoT Fleet Provisioning (kurz für Fleet Provisioning) werden Gerätezertifikate AWS IoT Core generiert und sicher an Ihre Geräte gesendet, wenn diese AWS IoT Core zum ersten Mal eine Verbindung herstellen. Sie können Fleet Provisioning verwenden, um Geräte, für die keine Gerätezertifikate vorliegen, miteinander zu verbinden. AWS IoT Core

Anfrage zum Signieren eines Zertifikats (CSR)

> Bei der Flottenbereitstellung stellt ein Gerät eine Anfrage an das MQTT für die AWS IoT Core Flottenbereitstellung. APIs Diese Anfrage beinhaltet eine Certificate Signing Request (CSR), die signiert wird, um ein Client-Zertifikat zu erstellen.

AWS verwaltete Zertifikatsignierung bei der Flottenbereitstellung

> AWS managed ist die Standardeinstellung für das Signieren von Zertifikaten bei der Flottenbereitstellung. Bei AWS verwalteter Zertifikatsignierung AWS IoT Core wird die Signatur CSRs mit eigener CAs Signatur signiert.

Selbstverwaltetes Signieren von Zertifikaten bei der Flottenbereitstellung

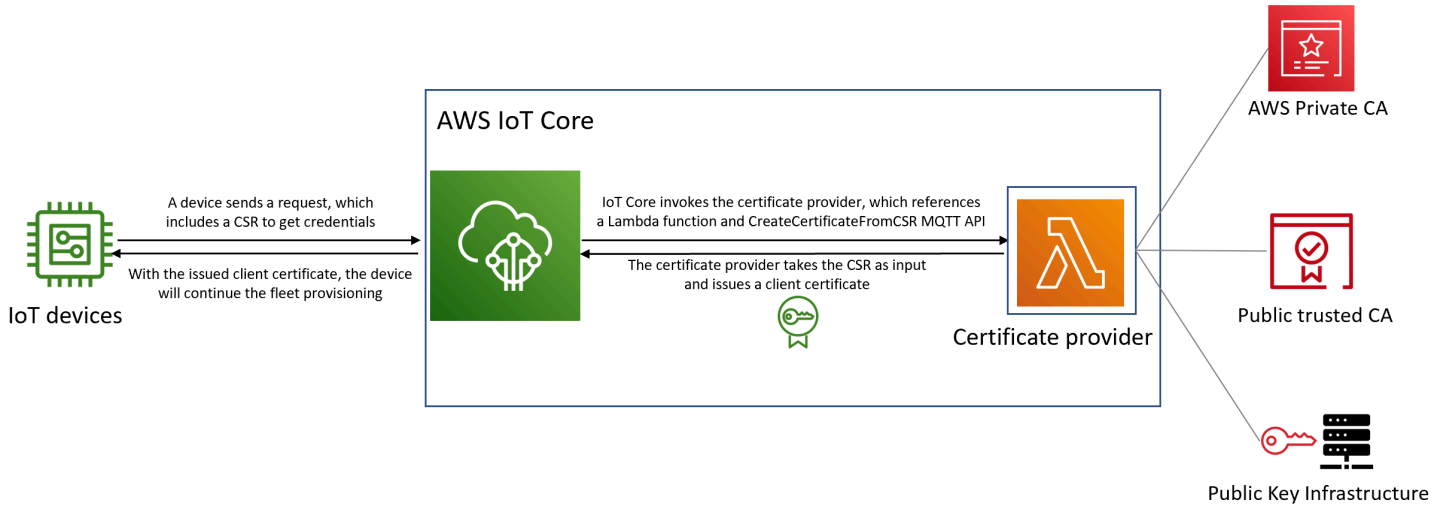
> Selbstverwaltung ist eine weitere Option für die Zertifikatsignierung bei der Flottenbereitstellung. Mit der selbstverwalteten Zertifikatsignierung erstellen Sie einen AWS IoT Core Zertifikatsanbieter zum Signieren. CSRs Sie können die selbstverwaltete Zertifikatsignierung verwenden, um CSRs mit einer Zertifizierungsstelle zu signieren, die von einer AWS privaten Zertifizierungsstelle, einer anderen öffentlich vertrauenswürdigen Zertifizierungsstelle oder Ihrer eigenen Public Key Infrastructure (PKI) generiert wurde.

## AWS IoT Core Zertifikatsanbieter

AWS IoT Core Der Zertifikatsanbieter (kurz für Certificate Provider) ist eine vom Kunden verwaltete Ressource, die für die selbstverwaltete Signierung von Zertifikaten bei der Flottenbereitstellung verwendet wird.

## Diagramm

Das folgende Diagramm zeigt in vereinfachter Form, wie das Signieren von Selbstzertifikaten bei der AWS IoT Flottenbereitstellung funktioniert.




- Wenn ein neues IoT-Gerät hergestellt oder in die Flotte eingeführt wird, benötigt es Kundenzertifikate, mit AWS IoT Core denen es sich authentifizieren kann.
- Im Rahmen des Flottenbereitstellungsprozesses fordert das Gerät über das AWS IoT Core Flottenbereitstellungs-MQTT Kundenzertifikate an. APIs Diese Anfrage beinhaltet eine Certificate Signing Request (CSR).
- AWS IoT Core ruft den Zertifikatsanbieter auf und übergibt die CSR als Eingabe an den Anbieter.
- Der Zertifikatsanbieter verwendet die CSR als Eingabe und stellt ein Client-Zertifikat aus.

  Signiert beim Signieren AWS verwalteter Zertifikate die CSR mit AWS IoT Core einer eigenen Zertifizierungsstelle und stellt ein Client-Zertifikat aus.
- Mit dem ausgestellten Client-Zertifikat setzt das Gerät die Flottenbereitstellung fort und stellt eine sichere Verbindung mit her. AWS IoT Core

## Eingabe der Lambda-Funktion des Zertifikatsanbieters

AWS IoT Core sendet das folgende Objekt an die Lambda-Funktion, wenn sich ein Gerät bei ihr registriert. Der Wert von `certificateSigningRequest` ist die CSR im PEM-Format (Privacy-Enhanced Mail), die in der Anfrage angegeben ist. `CreateCertificateFromCsr` Das `principalId` ist die ID des Prinzipals, mit dem bei der Anfrage eine Verbindung hergestellt wurde. AWS IoT Core `CreateCertificateFromCsr` `clientId`ist die Client-ID, die für die MQTT-Verbindung festgelegt wurde.

```
{
 "certificateSigningRequest": "string",
 "principalId": "string",
 "clientId": "string"
}
```

## Rückgabewert der Lambda-Funktion des Zertifikatsanbieters

Die Lambda-Funktion muss eine Antwort zurückgeben, die den `certificatePem` Wert enthält. Das Folgende ist ein Beispiel für eine erfolgreiche Antwort. AWS IoT Core verwendet den Rückgabewert (`certificatePem`), um das Zertifikat zu erstellen.

```
{
 "certificatePem": "string"
}
```

Wenn die Registrierung erfolgreich ist, `CreateCertificateFromCsr` wird dasselbe `certificatePem` in der `CreateCertificateFromCsr` Antwort zurückgegeben. Weitere Informationen finden Sie im Beispiel für die Antwort-Payload von CreateCertificateFromCsr.

## Beispiel-Lambda-Funktion

Bevor Sie einen Zertifikatsanbieter erstellen, müssen Sie eine Lambda-Funktion erstellen, um eine CSR zu signieren. Im Folgenden finden Sie ein Beispiel für eine Lambda-Funktion in Python. Diese Funktion ruft AWS Private CA auf, um die Eingabe-CSR unter Verwendung einer privaten Zertifizierungsstelle und des `SHA256WITHRSA` Signaturalgorithmus zu signieren. Das zurückgegebene Client-Zertifikat ist ein Jahr lang gültig. Weitere Informationen zu AWS Private CA und zum Erstellen einer privaten Zertifizierungsstelle finden Sie unter Was ist eine AWS private Zertifizierungsstelle? und Eine private CA erstellen.

```
import os
import time
import uuid
import boto3

def lambda_handler(event, context):
    ca_arn = os.environ['CA_ARN']
    csr = (event['certificateSigningRequest']).encode('utf-8')

    acmpca = boto3.client('acm-pca')
    cert_arn = acmpca.issue_certificate(
        CertificateAuthorityArn=ca_arn,
        Csr=csr,
        Validity={"Type": "DAYS", "Value": 365},
        SigningAlgorithm='SHA256WITHRSA',
        IdempotencyToken=str(uuid.uuid4())
    )['CertificateArn']

    # Wait for certificate to be issued
    time.sleep(1)
    cert_pem = acmpca.get_certificate(
        CertificateAuthorityArn=ca_arn,
        CertificateArn=cert_arn
    )['Certificate']

    return {
        'certificatePem': cert_pem
    }
```

**Important**

- Von der Lambda-Funktion zurückgegebene Zertifikate müssen denselben Betreffnamen und denselben öffentlichen Schlüssel haben wie die Certificate Signing Request (CSR).
- Die Lambda-Funktion muss in 5 Sekunden fertig ausgeführt werden.
- Die Lambda-Funktion muss sich in derselben AWS-Konto Region wie die Ressource des Zertifikatsanbieters befinden.
- Dem AWS IoT Dienstprinzipal muss die Aufrufberechtigung für die Lambda-Funktion erteilt werden. Um verwirrende Probleme mit Stellvertretern zu vermeiden, empfehlen wir Ihnen, die Zugriffsberechtigungen `sourceArn` und `sourceAccount` für das Aufrufen

festzulegen. Weitere Informationen finden Sie unter Vermeidung des dienstübergreifenden Confused-Deputy-Problems.

Das folgende Beispiel für eine ressourcenbasierte Richtlinie für Lambda gewährt AWS IoT die Erlaubnis, die Lambda-Funktion aufzurufen:

```
{
 "Version": "2012-10-17",
 "Id": "InvokePermission",
 "Statement": [
  {
   "Sid": "LambdaAllowIotProvider",
   "Effect": "Allow",
   "Principal": {
    "Service": "iot.amazonaws.com"
   },
   "Action": "lambda:InvokeFunction",
   "Resource": "arn:aws:lambda:us-east-1:123456789012:function:my-function",
   "Condition": {
    "StringEquals": {
     "AWS:SourceAccount": "123456789012"
    },
    "ArnLike": {
     "AWS:SourceArn": "arn:aws:iot:us-east-1:123456789012:certificateprovider:my-
certificate-provider"
    }
   }
  }
 ]
}
```

## Selbstverwaltete Zertifikatsignierung für die Flottenbereitstellung

Sie können die selbstverwaltete Zertifikatssignierung für die Flottenbereitstellung mithilfe von oder auswählen. AWS CLI AWS Management Console

AWS CLI

Um sich für die selbstverwaltete Zertifikatsignierung zu entscheiden, müssen Sie einen AWS IoT Core Zertifikatsanbieter für die Anmeldung CSRs bei Fleet Provisioning erstellen. AWS IoT

Core ruft den Zertifikatsanbieter auf, der eine CSR als Eingabe verwendet und ein Client-Zertifikat zurückgibt. Verwenden Sie den `CreateCertificateProvider` API-Vorgang oder den `create-certificate-provider` CLI-Befehl, um einen Zertifikatsanbieter zu erstellen.

> **Note**
>
> Nachdem Sie einen Zertifikatsanbieter erstellt haben, ändert sich das Verhalten der `CreateCertificateFromCsr`API für die Flottenbereitstellung, sodass bei allen Aufrufen von der Zertifikatsanbieter zur Erstellung der Zertifikate aufgerufen `CreateCertificateFromCsr` wird. Es kann einige Minuten dauern, bis sich dieses Verhalten ändert, nachdem ein Zertifikatsanbieter erstellt wurde.

```
aws iot create-certificate-provider \
                --certificateProviderName my-certificate-provider \
                --lambdaFunctionArn arn:aws:lambda:us-east-1:123456789012:function:my-
function-1 \
                --accountDefaultForOperations CreateCertificateFromCsr
```

Im Folgenden wird eine Beispielausgabe für diesen Befehl gezeigt:

```
{
 "certificateProviderName": "my-certificate-provider",
 "certificateProviderArn": "arn:aws:iot:us-east-1:123456789012:certificateprovider:my-
certificate-provider"
}
```

Weitere Informationen finden Sie in `CreateCertificateProvider` der AWS IoTAPI-Referenz.

AWS Management Console

Gehen Sie wie folgt vor AWS Management Console, um die selbstverwaltete Zertifikatsignierung mithilfe von auszuwählen:

1. Rufen Sie die AWS IoT -Konsole auf.
2. Wählen Sie in der linken Navigationsleiste unter Sicherheit die Option Zertifikatsignierung aus.
3. Wählen Sie auf der Seite Zertifikatsignierung unter Details zur Zertifikatsignierung die Option Zertifikatsignierungsmethode bearbeiten aus.

4. Wählen Sie auf der Seite Zertifikatsignierungsmethode bearbeiten unter Zertifikatsignierungsmethode die Option Selbstverwaltet aus.
5. Geben Sie im Abschnitt Selbstverwaltete Einstellungen einen Namen für den Zertifikatsanbieter ein und erstellen Sie dann eine Lambda-Funktion oder wählen Sie sie aus.
6. Wählen Sie Zertifikatsignatur aktualisieren aus.

## AWS CLI Befehle für den Zertifikatsanbieter

### Zertifikatsanbieter erstellen

Verwenden Sie den `CreateCertificateProvider` API-Vorgang oder den `create-certificate-provider` CLI-Befehl, um einen Zertifikatsanbieter zu erstellen.

> **Note**
>
> Nachdem Sie einen Zertifikatsanbieter erstellt haben, ändert sich das Verhalten der `CreateCertificateFromCsr`API für die Flottenbereitstellung, sodass bei allen Aufrufen von der Zertifikatsanbieter zur Erstellung der Zertifikate aufgerufen `CreateCertificateFromCsr` wird. Es kann einige Minuten dauern, bis sich dieses Verhalten ändert, nachdem ein Zertifikatsanbieter erstellt wurde.

```
aws iot create-certificate-provider \
                --certificateProviderName my-certificate-provider \
                --lambdaFunctionArn arn:aws:lambda:us-east-1:123456789012:function:my-
function-1 \
                --accountDefaultForOperations CreateCertificateFromCsr
```

Im Folgenden wird eine Beispielausgabe für diesen Befehl gezeigt:

```
{
 "certificateProviderName": "my-certificate-provider",
 "certificateProviderArn": "arn:aws:iot:us-east-1:123456789012:certificateprovider:my-
certificate-provider"
}
```

Weitere Informationen finden Sie in `CreateCertificateProvider` der AWS IoTAPI-Referenz.

## Aktualisieren Sie den Zertifikatsanbieter

Verwenden Sie den `UpdateCertificateProvider` API-Vorgang oder den `update-certificate-provider` CLI-Befehl, um einen Zertifikatsanbieter zu aktualisieren.

```
aws iot update-certificate-provider \
                --certificateProviderName my-certificate-provider \
                --lambdaFunctionArn arn:aws:lambda:us-east-1:123456789012:function:my-function-2 \
                --accountDefaultForOperations CreateCertificateFromCsr
```

Im Folgenden wird eine Beispielausgabe für diesen Befehl gezeigt:

```
{
 "certificateProviderName": "my-certificate-provider",
 "certificateProviderArn": "arn:aws:iot:us-east-1:123456789012:certificateprovider:my-certificate-provider"
}
```

Weitere Informationen finden Sie in `UpdateCertificateProvider` der AWS IoTAPI-Referenz.

## Beschreiben Sie den Zertifikatsanbieter

Verwenden Sie die `DescribeCertificateProvider` API-Operation oder den `describe-certificate-provider` CLI-Befehl, um einen Zertifikatsanbieter zu beschreiben.

```
aws iot describe-certificate-provider --certificateProviderName my-certificate-provider
```

Im Folgenden wird eine Beispielausgabe für diesen Befehl gezeigt:

```
{
 "certificateProviderName": "my-certificate-provider",
 "lambdaFunctionArn": "arn:aws:lambda:us-east-1:123456789012:function:my-function",
 "accountDefaultForOperations": [
  "CreateCertificateFromCsr"
 ],
 "creationDate": "2022-11-03T00:15",
 "lastModifiedDate": "2022-11-18T00:15"
}
```

Weitere Informationen finden Sie in `DescribeCertificateProvider` der AWS IoTAPI-Referenz.

### Löschen Sie den Zertifikatsanbieter

Verwenden Sie den `DeleteCertificateProvider` API-Vorgang oder den `delete-certificate-provider` CLI-Befehl, um einen Zertifikatsanbieter zu löschen. Wenn Sie die Ressource des Zertifikatsanbieters löschen, `CreateCertificateFromCsr` wird das Verhalten von wieder aufgenommen und AWS IoT es werden Zertifikate erstellt, die AWS IoT von einer CSR signiert wurden.

```
aws iot delete-certificate-provider --certificateProviderName my-certificate-provider
```

Dieser Befehl liefert keine Ausgabe.

Weitere Informationen finden Sie in `DeleteCertificateProvider` der AWS IoTAPI-Referenz.

### Zertifikatsanbieter auflisten

Verwenden Sie die `ListCertificateProviders` API-Operation oder den `list-certificate-providers` CLI-Befehl AWS-Konto, um die Zertifikatsanbieter in Ihrem aufzulisten.

```
aws iot list-certificate-providers
```

Im Folgenden wird eine Beispielausgabe für diesen Befehl gezeigt:

```
{
 "certificateProviders": [
  {
   "certificateProviderName": "my-certificate-provider",
   "certificateProviderArn": "arn:aws:iot:us-
east-1:123456789012:certificateprovider:my-certificate-provider"
  }
 ]
}
```

Weitere Informationen finden Sie in `ListCertificateProvider`der AWS IoTAPI-Referenz.

# Erstellen von IAM-Richtlinien und -Rollen für Benutzer, die ein Gerät installieren

> **Note**
>
> Diese Verfahren dürfen nur verwendet werden, wenn Sie von der AWS IoT Konsole dazu aufgefordert werden.
> Öffnen Sie Neue Bereitstellungsvorlage erstellen, um von der Konsole aus zu dieser Seite zu gelangen.

## Warum ist das nicht in der AWS IoT -Konsole möglich?

IAM-Aktionen werden aus Sicherheitsgründen in der IAM-Konsole ausgeführt. Die Verfahren in diesem Abschnitt führen Sie durch die Schritte zum Erstellen der IAM-Rollen und -Richtlinien, die für die Verwendung der Bereitstellungsvorlage erforderlich sind.

## Erstellen einer IAM-Richtlinie für Benutzer, die ein Gerät installieren werden

In diesem Verfahren wird beschrieben, wie Sie eine IAM-Richtlinie erstellen, die Benutzer autorisiert, ein Gerät mithilfe einer Bereitstellungsvorlage zu installieren.

Während Sie dieses Verfahren ausführen, wechseln Sie zwischen der IAM-Konsole und der AWS IoT Konsole. Wir empfehlen, während dieses Verfahrens beide Konsolen gleichzeitig zu öffnen.

Erstellen einer IAM-Richtlinie für Benutzer, die ein Gerät installieren werden

1. Öffnen Sie das Richtlinien-Hub in der IAM-Konsole.
2. Wählen Sie Richtlinie erstellen aus.
3. Wählen Sie auf der Seite Richtlinie erstellen die Registerkarte JSON aus.
4. Wechseln Sie zu der Seite in der AWS IoT Konsole, auf der Sie Benutzerrichtlinie und Rolle konfigurieren ausgewählt haben.
5. Wählen Sie in der Beispiel-Bereitstellungsrichtlinie die Option Kopieren.
6. Wechseln Sie zurück zur IAM-Konsole.
7. Fügen Sie im JSON-Editor die Richtlinie ein, die Sie aus der AWS IoT Konsole kopiert haben. Diese Richtlinie ist spezifisch für die Vorlage, die Sie in der AWS IoT Konsole erstellen.

8. Wählen Sie Weiter: Tags, um fortzufahren.
9. Wählen Sie auf der Seite Tags hinzufügen (optional) für jedes Tag, das Sie zu dieser Richtlinie hinzufügen möchten, die Option Tag hinzufügen aus. Diesen Schritt können Sie überspringen, wenn Sie keine Tags hinzufügen möchten.
10. Wählen Sie Weiter: Überprüfung, um fortzufahren.
11. Führen Sie auf der Seite Richtlinie überprüfen die folgenden Schritte aus:

    a. Geben Sie unter Name* einen Namen für die Richtlinie ein, der Sie an den Zweck der Richtlinie erinnert.

       Notieren Sie sich den Namen, den Sie dieser Richtlinie geben, da Sie ihn im nächsten Verfahren benötigen werden.

    b. Optional können Sie eine Beschreibung für die Richtlinie eingeben, die Sie erstellen.

    c. Lesen Sie sich den Rest dieser Richtlinie und ihrer Tags durch.
12. Wählen Sie Richtlinie erstellen, um Ihre Richtlinie zu erstellen.

Nachdem Sie Ihre neue Richtlinie erstellt haben, fahren Sie mit the section called “Erstellen einer IAM-Rolle für Benutzer, die ein Gerät installieren werden” fort, um den Rolleneintrag der Benutzer zu erstellen, denen Sie diese Richtlinie anhängen.

## Erstellen einer IAM-Rolle für Benutzer, die ein Gerät installieren werden

In diesen Schritten wird beschrieben, wie Sie eine IAM-Rolle erstellen, die die Benutzer authentifiziert, die ein Gerät mithilfe einer Bereitstellungsvorlage installieren.

Erstellen einer IAM-Richtlinie für Benutzer, die ein Gerät installieren werden

1. Öffnen Sie die Seite Rollen-Hub in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Wählen Sie unter Vertrauenswürdige Entität auswählen den Typ der vertrauenswürdigen Entität aus, der Sie Zugriff auf die von Ihnen erstellte Vorlage gewähren möchten.
4. Wählen Sie die ID der vertrauenswürdigen Entität, der Sie Zugriff gewähren möchten, oder geben Sie sie ein, und klicken Sie dann auf Weiter.
5. Geben Sie auf der Seite Berechtigungen hinzufügen unter Berechtigungsrichtlinien im Suchfeld den Namen der Richtlinie ein, die Sie im vorherigen Verfahren erstellt haben.

6. Wählen Sie für die Richtlinienliste die Richtlinie aus, die Sie im vorherigen Verfahren erstellt haben, und klicken Sie anschließend auf Weiter.
7. Gehen Sie im Abschnitt Name, prüfen und erstellen wie folgt vor:

    a. Geben Sie unter Rollenname einen Rollennamen ein, der Sie an den Zweck dieser Rolle erinnert.

    b. Unter Beschreibung können Sie optional eine Beschreibung der Rolle eingeben. Dies ist nicht erforderlich, um fortzufahren.

    c. Überprüfen Sie die Werte in Schritt 1 und Schritt 2.

    d. Unter Tags hinzufügen (optional) können Sie auswählen, ob Sie dieser Rolle Tags hinzufügen möchten. Dies ist nicht erforderlich, um fortzufahren.

    e. Vergewissern Sie sich, dass die Informationen auf dieser Seite vollständig und korrekt sind, und wählen Sie dann Rolle erstellen.

Nachdem Sie die neue Rolle erstellt haben, kehren Sie zur AWS IoT Konsole zurück, um mit der Erstellung der Vorlage fortzufahren.

## Aktualisieren einer vorhandenen Richtlinie, um eine neue Vorlage zu autorisieren

In den folgenden Schritten wird beschrieben, wie Sie einer IAM-Richtlinie eine neue Vorlage hinzufügen, die Benutzer autorisiert, ein Gerät mithilfe einer Bereitstellungsvorlage zu installieren.

Hinzufügen einer neuen Vorlage zu einer bestehenden IAM-Richtlinie

1. Öffnen Sie das Richtlinien-Hub in der IAM-Konsole.
2. Geben Sie im Suchfeld den Namen der zu aktualisierenden Richtlinie ein.
3. Suchen Sie in der Liste unter dem Suchfeld die Richtlinie, die Sie aktualisieren möchten, und wählen Sie den Richtliniennamen aus.
4. Wählen Sie für die Richtlinienübersicht die Registerkarte JSON, falls dieser Bereich noch nicht sichtbar ist.
5. Wählen Sie Richtlinie bearbeiten, um das Richtliniendokument zu bearbeiten.
6. Wählen Sie im Editor die Registerkarte JSON, falls dieser Bereich noch nicht sichtbar ist.
7. Suchen Sie im Richtliniendokument nach der Richtlinienerklärung, die die `iot:CreateProvisioningClaim`-Aktion enthält.

Wenn das Richtliniendokument keine Richtlinienanweisung mit der `iot:CreateProvisioningClaim`-Aktion enthält, kopieren Sie den folgenden Anweisungsausschnitt und fügen Sie ihn als zusätzlichen Eintrag in das `Statement`-Array im Richtliniendokument ein.

> **Note**
>
> Dieser Ausschnitt muss vor dem letzten `]`-Zeichen im `Statement`-Array stehen. Möglicherweise müssen Sie vor oder nach diesem Ausschnitt ein Komma setzen, um Syntaxfehler zu korrigieren.

```
{
    "Effect": "Allow",
    "Action": [
        "iot:CreateProvisioningClaim"
    ],
    "Resource": [
        "--PUT YOUR NEW TEMPLATE ARN HERE--"
    ]
}
```

8. Wechseln Sie zu der Seite in der AWS IoT Konsole, auf der Sie Benutzerrollenberechtigungen ändern ausgewählt haben.
9. Suchen Sie den Ressourcen-ARN der Vorlage und wählen Sie Kopieren.
10. Wechseln Sie zurück zur IAM-Konsole.
11. Fügen Sie den kopierten Amazon-Ressourcennamen (ARN) oben in der Vorlagenliste ARNs im `Statement` Array ein, sodass er der erste Eintrag ist.

    Wenn dies der einzige ARN im Array ist, entfernen Sie das Komma am Ende des Werts, den Sie gerade eingefügt haben.
12. Lesen Sie die aktualisierte Richtlinienanweisung und korrigieren Sie alle vom Editor angegebenen Fehler.
13. Wählen Sie Richtlinie überprüfen, um das aktualisierte Richtliniendokument zu speichern.
14. Überprüfen Sie die Richtlinie und wählen Sie anschließend Änderungen speichern.
15. Kehren Sie zur AWS IoT Konsole zurück.

# MQTT-API für die Gerätebereitstellung

Der Fleet Provisioning Service unterstützt die folgenden MQTT-API-Operationen:

- the section called “CreateCertificateFromCsr”
- the section called “CreateKeysAndCertificate”
- the section called “RegisterThing”

Diese API unterstützt je nach Thema Antwortpuffer im Format Concise Binary Object Representation (CBOR) und JavaScript Object Notation (JSON). *payload-format* Aus Gründen der Übersichtlichkeit werden die Antworten- und Anforderungsbeispiele in diesem Abschnitt im JSON-Format dargestellt.

| ***payload-format*** | Datentyp des Antwortformats |
|---|---|
| cbor | Concise Binary Object Representation (CBOR) |
| json | JavaScript Objektnotation (JSON) |

> **Important**
>
> Bevor Sie ein Anforderungsnachrichtenthema veröffentlichen, abonnieren Sie die Antwortthemen, um die Antwort zu erhalten. Die Nachrichten, die von dieser API verwendet werden, stellen mithilfe des Protokolls zum Veröffentlichen/Abonnieren von MQTT eine Anforderungs- und Antwort-Interaktion bereit.
> Wenn Sie die Antwortthemen nicht abonnieren, bevor Sie eine Anfrage veröffentlichen, erhalten Sie möglicherweise keine Ergebnisse dieser Anfrage.

## CreateCertificateFromCsr

Erstellt ein Zertifikat aus einer Zertifikatsignieranforderung (CSR). AWS IoT stellt Client-Zertifikate bereit, die von der Amazon Root Certificate Authority (CA) signiert wurden. Das neue Zertifikat hat den Status `PENDING_ACTIVATION`. Wenn Sie `RegisterThing` aufrufen, um ein Objekt mit diesem Zertifikat bereitzustellen, ändert sich der Zertifikatstatus in `ACTIVE` oder `INACTIVE`, wie in der Vorlage beschrieben.

Weitere Informationen zum Erstellen eines Client-Zertifikats mit Ihrem Zertifizierungsstellenzertifikat und einer Zertifikatsignierungsanforderung finden Sie unter Erstellen eines Clientzertifikats mit Ihrem CA-Zertifikat.

> **Note**
>
> Aus Sicherheitsgründen läuft das von `CreateCertificateFromCsr` ausgegebene `certificateOwnershipToken` zurückgesendet nach einer Stunde ab. `RegisterThing` muss aufgerufen werden, bevor `certificateOwnershipToken` abläuft. Wenn das von erstellte Zertifikat `CreateCertificateFromCsr` bis zum Ablauf des Tokens nicht aktiviert und an eine Richtlinie oder ein Objekt angehängt wurde, wird das Zertifikat gelöscht. Wenn das Token abläuft, kann das Gerät `CreateCertificateFromCsr` erneut aufrufen, um ein neues Zertifikat zu generieren.

## CreateCertificateFromCsr-Anfrage

Veröffentlichen Sie eine Nachricht mit dem Thema `$aws/certificates/create-from-csr/`*`payload-format`*.

`payload-format`

Das Nachrichtennutzlastformat ist `cbor` oder `json`.

CreateCertificateFromCsrPayload anfordern

```
{
    "certificateSigningRequest": "string"
}
```

`certificateSigningRequest`

Die CSR im PEM-Format.

## CreateCertificateFromCsr-Antwort

Abonnieren Sie `$aws/certificates/create-from-csr/`*`payload-format`*`/accepted`.

`payload-format`

Das Nachrichtennutzlastformat ist `cbor` oder `json`.

CreateCertificateFromCsrNutzlast der Antwort

```
{
    "certificateOwnershipToken": "string",
    "certificateId": "string",
    "certificatePem": "string"
}
```

`certificateOwnershipToken`

Das Token, um den Besitz des Zertifikats während der Bereitstellung nachzuweisen.

`certificateId`

Die ID des Zertifikats. Zertifikatsverwaltungsoperationen verwenden nur eine certificateId.

`certificatePem`

Die Zertifikatdaten im PEM-Format.

## CreateCertificateFromCsr Fehler

Um Fehlerantworten zu empfangen, abonnieren Sie `$aws/certificates/create-from-csr/`*`payload-format`*`/rejected`.

`payload-format`

Das Nachrichtennutzlastformat ist `cbor` oder `json`.

CreateCertificateFromCsrFehler Payload

```
{
    "statusCode": int,
    "errorCode": "string",
    "errorMessage": "string"
}
```

`statusCode`

Welcher Statuscode gesendet wird

`errorCode`

Der Fehlercode.

`errorMessage`

Die Fehlermeldung.

## CreateKeysAndCertificate

Erzeugt neue Schlüssel und ein Zertifikat. AWS IoT stellt Client-Zertifikate bereit, die von der Amazon Root Certificate Authority (CA) signiert wurden. Das neue Zertifikat hat den Status `PENDING_ACTIVATION`. Wenn Sie `RegisterThing` aufrufen, um ein Objekt mit diesem Zertifikat bereitzustellen, ändert sich der Zertifikatstatus in `ACTIVE` oder `INACTIVE`, wie in der Vorlage beschrieben.

> **Note**
>
> Aus Sicherheitsgründen läuft das von `CreateKeysAndCertificate` ausgegebene `certificateOwnershipToken` zurückgesendet nach einer Stunde ab. `RegisterThing` muss aufgerufen werden, bevor `certificateOwnershipToken` abläuft. Wenn das von erstellte Zertifikat `CreateKeysAndCertificate` bis zum Ablauf des Tokens nicht aktiviert und an eine Richtlinie oder ein Objekt angehängt wurde, wird das Zertifikat gelöscht. Wenn das Token abläuft, kann das Gerät `CreateKeysAndCertificate` erneut aufrufen, um ein neues Zertifikat zu generieren.

### CreateKeysAndCertificate-Anfrage

Veröffentlichen Sie eine Nachricht unter `$aws/certificates/create/`*`payload-format`* mit einer leeren Nachrichtennutzlast.

`payload-format`

Das Nachrichtennutzlastformat ist `cbor` oder `json`.

## CreateKeysAndCertificate-Antwort

Abonnieren Sie `$aws/certificates/create/`*`payload-format`*`/accepted`.

`payload-format`

Das Nachrichtennutzlastformat ist `cbor` oder `json`.

CreateKeysAndCertificate-Antwort

```
{
    "certificateId": "string",
    "certificatePem": "string",
    "privateKey": "string",
    "certificateOwnershipToken": "string"
}
```

`certificateId`

Die ID des Zertifikats.

`certificatePem`

Die Zertifikatdaten im PEM-Format.

`privateKey`

Der private Schlüssel.

`certificateOwnershipToken`

Das Token, um den Besitz des Zertifikats während der Bereitstellung nachzuweisen.

## CreateKeysAndCertificate Fehler

Um Fehlerantworten zu empfangen, abonnieren Sie `$aws/certificates/create/`*`payload-format`*`/rejected`.

`payload-format`

Das Nachrichtennutzlastformat ist `cbor` oder `json`.

CreateKeysAndCertificateFehler Payload

```
{
    "statusCode": int,
    "errorCode": "string",
    "errorMessage": "string"
}
```

`statusCode`

Welcher Statuscode gesendet wird

`errorCode`

Der Fehlercode.

`errorMessage`

Die Fehlermeldung.

## RegisterThing

Stellt ein Objekt anhand einer vordefinierten Vorlage bereit.

### RegisterThing Anfrage

Veröffentlichen Sie eine Nachricht unter `$aws/provisioning-templates/`*`templateName`*`/provision/`*`payload-format`*.

`payload-format`

Das Nachrichtennutzlastformat ist `cbor` oder `json`.

`templateName`

Der Name der Bereitstellungsvorlage.

RegisterThing Nutzlast anfordern

```
{
    "certificateOwnershipToken": "string",
    "parameters": {
```

```
        "string": "string",
        ...
    }
}
```

`certificateOwnershipToken`

Das Token zum Nachweis der Inhaberschaft des Zertifikats. AWS IoT generiert das Token, wenn Sie ein Zertifikat über MQTT erstellen.

`parameters`

Optional. Schlüssel-Wert-Paare vom Gerät, die von den Pre-Provisioning-Hooks verwendet werden, um die Registrierungsanforderung auszuwerten.

## RegisterThing Antwort

Abonnieren Sie `$aws/provisioning-templates/`*`templateName`*`/provision/`*`payload-format`*`/accepted`.

`payload-format`

Das Nachrichtennutzlastformat ist `cbor` oder `json`.

`templateName`

Der Name der Bereitstellungsvorlage.

### RegisterThing Nutzlast der Antwort

```
{
    "deviceConfiguration": {
        "string": "string",
        ...
    },
    "thingName": "string"
}
```

`deviceConfiguration`

Die in der Vorlage definierte Gerätekonfiguration.

`thingName`

Der Name des IoT-Objekts, das während der Bereitstellung erstellt wurde.

## RegisterThing Fehlerantwort

Um Fehlerantworten zu empfangen, abonnieren Sie `$aws/provisioning-templates/`*`templateName`*`/provision/`*`payload-format`*`/rejected`.

`payload-format`

Das Nachrichtennutzlastformat ist `cbor` oder `json`.

`templateName`

Der Name der Bereitstellungsvorlage.

RegisterThing Payload für die Fehlerantwort

```
{
    "statusCode": int,
    "errorCode": "string",
    "errorMessage": "string"
}
```

`statusCode`

Welcher Statuscode gesendet wird

`errorCode`

Der Fehlercode.

`errorMessage`

Die Fehlermeldung.

# -Flottenindizierung

Sie können die Flottenindizierung verwenden, um die Daten Ihrer Geräte aus den folgenden Quellen zu indizieren, zu durchsuchen und zu aggregieren: AWS IoT Registrierung, AWS IoT Device Shadow, AWS IoT Konnektivität, AWS IoT Geräteverwaltungs-Softwarepaketkatalog und AWS IoT Device DefenderVerstöße. Sie können eine Gruppe von Geräten abfragen und Statistiken zu Gerätedatensätzen aggregieren, die auf verschiedenen Kombinationen von Geräteattributen basieren, darunter Status, Konnektivität und Geräteverstöße. Mit der Flottenindizierung können Sie Ihre Geräteflotte organisieren, untersuchen und Fehler beheben.

Die Flottenindizierung bietet die folgenden Funktionen.

## Verwalten von Indexaktualisierungen

Sie können einen Flottenindex einrichten, um Updates für Ihre Objektgruppen, Objektregister, Geräteschatten, Gerätekonnektivität und Geräteverletzungen zu indexieren. Wenn Sie die Flottenindizierung aktivieren, wird AWS IoT ein Index für Ihre Objekte oder Objektgruppen erstellen. `AWS_Things` ist der Index, der für all Ihre Objekte erstellt wurde. `AWS_ThingGroups` ist der Index, der all Ihre Objektgruppen enthält. Wenn dies aktiviert ist, können Sie Abfragen für Ihren Index ausführen. Sie können beispielsweise alle Geräte finden, die in der Hand gehalten werden und eine Akkulaufzeit von mehr als 70 Prozent haben. AWS IoT aktualisiert den Index kontinuierlich mit Ihren neuesten Daten. Weitere Informationen finden Sie unter Verwalten der Flottenindexierung.

## Verbindungsstatus für ein bestimmtes Gerät abfragen

Dies API ermöglicht den Zugriff auf die neuesten gerätespezifischen Konnektivitätsinformationen mit niedriger Latenz und hohem Durchsatz. Weitere Informationen finden Sie unter Status der Gerätekonnektivität.

## Datenquellenübergreifende Suche

Sie können eine Abfragezeichenfolge auf der Grundlage einer Abfragesprache erstellen und diese für die datenquellenübergreifende Suche verwenden. Sie müssen auch Datenquellen in der Flottenindizierungseinstellung so konfigurieren, dass die Indizierungskonfiguration die Datenquellen enthält, aus denen Sie suchen möchten. Die Abfragezeichenfolge beschreibt die Objekte, die Sie suchen möchten. Sie können Abfragen mithilfe von AWS verwalteten Feldern, benutzerdefinierten Feldern und beliebigen Attributen aus Ihren indizierten Datenquellen erstellen. Weitere Informationen

zu Datenquellen, die die Flottenindizierung unterstützen, finden Sie unter Verwaltung der Indexierung von Objekten.

## Abfragen von Aggregatdaten

Sie können Ihre Geräte nach aggregierten Daten durchsuchen und Statistiken, Perzentile, Kardinalität oder eine Liste von Objekten mit Suchanfragen zu bestimmten Feldern zurückgeben. Sie können Aggregationen für AWS verwaltete Felder oder beliebige Attribute ausführen, die Sie in den Einstellungen für die Flottenindizierung als benutzerdefinierte Felder konfigurieren. Weitere Informationen zur Aggregationsabfrage finden Sie unter Abfragen aggregierter Daten.

## Überwachung aggregierter Daten und Erstellung von Alarmen mithilfe von Flottenkennzahlen

Sie können Flottenkennzahlen verwenden, um aggregierte Daten CloudWatch automatisch an zu senden, Trends zu analysieren und Alarme zu erstellen, um den Gesamtstatus Ihrer Flotte auf der Grundlage vordefinierter Schwellenwerte zu überwachen. Weitere Informationen zu Metriken erhalten Sie unter Ressourcenmetriken.

## Verwalten der Flottenindizierung

Flottenindizierung verwaltet zwei Arten von Indizes für Sie: die Objektindizierung und die Objektgruppenindizierung.

### Objektindizierung

`AWS_Things` ist der Index für all Ihre Objekte. Die Objektindizierung unterstützt die folgenden Datenquellen: AWS IoT Registrierungsdaten, AWS IoT Device Schatten-Daten, AWS IoT Konnektivitätsdaten und Daten zu AWS IoT Device DefenderVerstößen. Indem Sie diese Datenquellen zu Ihrer Flottenindexierungskonfiguration hinzufügen, können Sie nach Objekten suchen, aggregierte Daten abfragen und dynamische Objektgruppen und Flottenmetriken auf der Grundlage Ihrer Suchanfragen erstellen.

Registry —AWS IoT bietet ein Register, mit dem Sie Dinge verwalten können. Sie können die Registrierungsdaten zu Ihrer Flottenindexierungskonfiguration hinzufügen, um anhand der Objektnamen, Beschreibungen und anderen Registrierungsattributen nach Geräten zu suchen. Weitere Informationen zur -Registrierung finden Sie unter Verwalten von Aufgaben mit der -Registrierung.

Schatten — Der AWS IoT Device Schatten-Dienst bietet Schatten, mit denen Sie Ihre Gerätestatusdaten speichern können. Die Indizierung von Objekten unterstützt sowohl klassische unbenannte Schatten als auch benannte Schatten. Um benannte Schatten zu indizieren, aktivieren Sie Ihre Einstellungen für benannte Schatten und geben Sie Ihre Schattennamen in der Konfiguration für die Objektindizierung an. Standardmäßig können Sie bis zu 10 Schattennamen pro Datei hinzufügen AWS-Konto. Informationen darüber, wie Sie die Obergrenze für die Anzahl der Schattennamen erhöhen können, finden Sie in der AWS allgemeinen Referenz unter AWS IoT Device Management Kontingente.

So fügen Sie benannte Schatten für die Indizierung hinzu:

- Wenn Sie die AWS IoT Konsole verwenden, aktivieren Sie die Objektindizierung, wählen Sie Benannte Schatten hinzufügen und fügen Sie Ihre Schattennamen über die Auswahl benannter Schatten hinzu.
- Wenn Sie das AWS Command Line Interface (AWS CLI) verwenden, setzen Sie `namedShadowIndexingMode` es auf und geben Sie Schattennamen in an `IndexingFilter`. `ON` CLIBeispielbefehle finden Sie unter Dingindizierung verwalten.

> **Important**
>
> Am 20. Juli 2022 erscheint die Version General Availability (GA) der AWS IoT Device Management-Flottenindexierungsintegration mit AWS IoT Core Named Shadows und AWS IoT Device Defender Detect Violations. Mit dieser GA-Version können Sie bestimmte benannte Schatten indizieren, indem Sie Schattennamen angeben. Wenn Sie Ihre benannten Schatten während der öffentlichen Vorschauphase dieser Funktion vom 30. November 2021 bis 19. Juli 2022 für die Indizierung hinzugefügt haben, empfehlen wir Ihnen, Ihre Einstellungen für die Flottenindizierung neu zu konfigurieren und spezifische Schattennamen auszuwählen, um die Indexierungskosten zu senken und die Leistung zu optimieren.

Weitere Informationen zu Schatten finden Sie unter AWS IoT Device Schatten-Service.

Konnektivität — Mithilfe der Daten zur Gerätekonnektivität können Sie den Verbindungsstatus Ihrer Geräte ermitteln. Diese Konnektivitätsdaten werden durch Lebenszyklusereignisse bestimmt. Wenn ein Client eine Verbindung herstellt oder die Verbindung trennt, AWS IoT veröffentlicht er Lebenszyklusereignisse mit Nachrichten zu MQTT Themen. Bei einer Meldung zum Herstellen oder Trennen kann es sich um eine Liste von JSON Elementen handeln, die Einzelheiten zum

Verbindungsstatus enthalten. Weitere Informationen zur Gerätekonnektivität finden Sie unter Lebenszyklusereignisse.

Verstöße gegen Device Defender — Daten zu AWS IoT Device Defender Verstößen helfen dabei, ungewöhnliches Geräteverhalten im Vergleich zu den normalen Verhaltensweisen zu identifizieren, die Sie in einem Sicherheitsprofil definieren. Ein Sicherheitsprofil enthält eine Reihe von Verhaltensweisen. Für jedes Verhalten wird eine Metrik verwendet, die das normale Verhalten Ihrer Geräte angibt. Weitere Informationen zu Device Defender-Verstößen finden AWS IoT Device Defender Sie unter Erkennen.

Weitere Informationen finden Sie unter Verwalten der Objektindizierung.

## Modus für die Objektgruppenindizierung.

`AWS_ThingGroups` ist der Index, die alle Ihre Objektgruppen enthält. Dieser Index ermöglicht Ihnen die Suche nach Gruppen basierend auf Gruppennamen, Beschreibung, Attributen und allen übergeordneten Gruppennamen.

Weitere Informationen finden Sie unter Verwalten der Objektgruppenindizierung.

## Verwaltete Felder

Verwaltete Felder enthalten Daten, die mit Dingen, Dinggruppen, Geräteschatten, Gerätekonnektivität und Device Defender-Verstößen verknüpft sind. AWS IoT definiert den Datentyp in verwalteten Feldern. Sie geben die Werte jedes verwalteten Felds an, wenn Sie ein AWS IoT Ding erstellen. Beispielsweise sind Objektnamen, Objektgruppen und Objektbeschreibungen alles verwaltete Felder. Der Flottenindizierungsservice indiziert verwaltete Felder basierend auf dem von Ihnen angegebenen Indizierungsmodus: Verwaltete Felder können nicht geändert oder in `customFields` angezeigt werden. Weitere Informationen finden Sie unter Benutzerdefinierte Felder.

Im Folgenden sind verwaltete Felder für die Indizierung von Objekten aufgeführt:

- Verwaltete Felder für die Registrierung

```
"managedFields" : [
  {name:thingId, type:String},
  {name:thingName, type:String},
  {name:registry.version, type:Number},
  {name:registry.thingTypeName, type:String},
  {name:registry.thingGroupNames, type:String},
```

```
]
```

- Verwaltete Felder für klassische unbenannte Schatten

```
"managedFields" : [
  {name:shadow.version, type:Number},
  {name:shadow.hasDelta, type:Boolean}
]
```

- Verwaltete Felder für benannte Schatten

```
"managedFields" : [
  {name:shadow.name.shadowName.version, type:Number},
  {name:shadow.name.shadowName.hasDelta, type:Boolean}
]
```

- Verwaltete Felder für die Objektkonnektivität

```
"managedFields" : [
  {name:connectivity.timestamp, type:Number},
  {name:connectivity.version, type:Number},
  {name:connectivity.connected, type:Boolean},
  {name:connectivity.disconnectReason, type:String}
]
```

- Verwaltete Felder für Device Defender

```
"managedFields" : [
  {name:deviceDefender.violationCount, type:Number},
  {name:deviceDefender.securityprofile.behaviorname.metricName, type:String},
  {name:deviceDefender.securityprofile.behaviorname.lastViolationTime, type:Number},
  {name:deviceDefender.securityprofile.behaviorname.lastViolationValue, type:String},
  {name:deviceDefender.securityprofile.behaviorname.inViolation, type:Boolean}
]
```

- Verwaltete Felder für Objektgruppen

```
"managedFields" : [
  {name:description, type:String},
  {name:parentGroupNames, type:String},
  {name:thingGroupId, type:String},
  {name:thingGroupName, type:String},
  {name:version, type:Number},
```

```
]
```

In der folgenden Tabelle sind verwaltete Felder aufgeführt, die nicht durchsucht werden können.

| Datenquelle | Verwaltetes Feld, das nicht durchsucht werden kann |
| --- | --- |
| Registrierung | `registry.version` |
| Unbenannte Schatten | `shadow.version` |
| Benannter Schatten | `shadow.name.*.version` |
| Device Defender | `deviceDefender.version` |
| Objektgruppen | `version` |

## Benutzerdefinierte Felder

Sie können Objekt-Attribute, Device Schatten-Daten und Daten zu Device Defender-Verstößen aggregieren, indem Sie benutzerdefinierte Felder erstellen, um sie zu indizieren. Das Attribut `customFields` ist eine Liste von Feld- und Datentyppaaren. Sie können Aggregationsabfragen auf der Grundlage des Datentyps durchführen. Der von Ihnen gewählte Indizierungsmodus wirkt sich auf Felder aus, in denen Sie angeben können. `customFields` Wenn Sie beispielsweise den Indizierungsmodus `REGISTRY` angeben, können Sie kein Feld aus einem Schattenobjekt angeben. Sie können den update-indexing-configurationCLIBefehl verwenden, um die benutzerdefinierten Felder zu erstellen oder zu aktualisieren (einen Beispielbefehl finden Sie unter Beispiele zur Aktualisierung der Indexierungskonfiguration).

- Namen benutzerdefinierter Felder

Benutzerdefinierte Feldnamen für Objekt- und Objektgruppenattribute beginnen mit `attributes.`, gefolgt vom Attributnamen. Wenn die unbenannte Schattenindizierung aktiviert ist, können Objekte benutzerdefinierte Feldnamen haben, die mit `shadow.desired` oder`shadow.reported` beginnen, gefolgt vom Namen des unbenannten Schattendatenwerts. Wenn die benannte Schattenindizierung aktiviert ist, können Objekte benutzerdefinierte Feldnamen haben, die mit `shadow.name.*.desired.` oder `shadow.name.*.reported.` beginnen, gefolgt vom benannten

Schattendatenwert. Wenn die Device Defender-Indizierung für Verstöße aktiviert ist, können Objekte benutzerdefinierte Feldnamen haben, die mit `deviceDefender.`, gefolgt vom Datenwert Device Defender-Verletzungen beginnen.

Der Name des Attributs oder Datenwerts, der auf das Präfix folgt, darf nur aus alphanumerischen Zeichen, Bindestrichen und Unterstrichen bestehen. Er darf keine Leerzeichen enthalten.

Wenn zwischen einem benutzerdefinierten Feld in der Konfiguration und dem indizierten Wert eine Typinkonsistenz besteht, ignoriert der Flottenindizierungsservice den inkonsistenten Wert für Aggregationsabfragen. -Protokolle sind hilfreich bei der Behebung von Problemen mit Aggregationsabfragen. CloudWatch Protokolle sind hilfreich bei der Behebung von Problemen mit Aggregationsabfragen. Weitere Informationen finden Sie unter Fehlerbehebung bei Aggregationsabfragen für den Flottenindizierungsservice.

- Benutzerdefinierte Feldtypen

Benutzerdefinierte Feldtypen haben die folgenden unterstützten Werte: `NumberString`, und`Boolean`.

## Verwalten der Objektindizierung

`AWS_Things` ist der Index für all Ihre Objekte. Sie können aus den folgenden Datenquellen steuern, was indexiert werden soll: AWS IoT Registrierungsdaten, AWS IoT Device Schatten-Daten, AWS IoT Konnektivitätsdaten und Daten zu AWS IoT Device DefenderVerstößen.

In diesem Thema:

- Aktivieren der Objektindizierung
- Beschreiben eines Objektindex
- Abfragen des Objektindex
- Beschränkungen und Einschränkungen
- Autorisierung

### Aktivieren der Objektindizierung

Sie verwenden den update-indexing-configurationCLIBefehl oder die UpdateIndexingConfigurationAPIOperation, um den `AWS_Things` Index zu erstellen und seine Konfiguration zu steuern. Mit dem Parameter `--thing-indexing-configuration`

(`thingIndexingConfiguration`) können Sie steuern, welche Art von Daten indiziert werden (z. B. Registrierungs-, Schatten- und Gerätekonnektivitätsdaten).

Der Parameter `--thing-indexing-configuration` nimmt eine Zeichenfolge mit der folgenden Struktur an:

```
{
  "thingIndexingMode": "OFF"|"REGISTRY"|"REGISTRY_AND_SHADOW",
  "thingConnectivityIndexingMode": "OFF"|"STATUS",
  "deviceDefenderIndexingMode": "OFF"|"VIOLATIONS",
  "namedShadowIndexingMode": "OFF"|"ON",
  "managedFields": [
    {
      "name": "string",
      "type": "Number"|"String"|"Boolean"
    },
    ...
  ],
  "customFields": [
    {
      "name": "string",
      "type": "Number"|"String"|"Boolean"
    },
    ...
  ],
  "filter": {
     "namedShadowNames": [ "string" ],
     "geoLocations": [
        {
            "name": "String",
            "order": "LonLat|LatLon"
        }
    ]
  }
}
```

Objektindizierungsmodus.

Sie können in Ihrer Indizierungskonfiguration verschiedene Indizierungsmodi angeben, je nachdem, aus welchen Datenquellen Sie Geräte indizieren und durchsuchen möchten:

- `thingIndexingMode`: Steuert, ob Registry oder Schatten indexiert ist. Wenn `thingIndexingMode` auf `OFF` eingestellt ist, ist die Indizierung von Objekten deaktiviert.

- `thingConnectivityIndexingMode`: Gibt an, ob die Objektkonnektivitätsdaten indiziert sind.

- `deviceDefenderIndexingMode`: Gibt an, ob Device Defender-Daten, die Verstöße verletzen, indexiert werden.
- `namedShadowIndexingMode`: Gibt an, ob benannte Schatten-Daten indexiert werden. Um benannte Schatten auszuwählen, die zu Ihrer Flottenindizierungskonfiguration hinzugefügt werden sollen, legen Sie `namedShadowIndexingMode` als `ON` fest und geben Sie Ihre benannten Schattennamen unter `filter` an.

Die folgende Tabelle zeigt die gültigen Werte für jeden Indizierungsmodus und die Datenquelle, die für jeden Wert indexiert ist.

| Attribut | Zulässige Werte | Registrierung | Shadow | Konnektivität | DD-Verstöße | Benannter Schatten |
|---|---|---|---|---|---|---|
| `thingIndexingMode` | OFF | | | | | |
| | REGISTRY | ✓ | | | | |
| | REGISTRY_AND_SHADOW | ✓ | ✓ | | | |
| `thingConnectivityIndexingMode` | Nicht angegeben. | | | | | |
| | OFF | | | | | |
| | STATUS | | | ✓ | | |
| `deviceDefenderIndexingMode` | Nicht angegeben. | | | | | |
| | OFF | | | | | |
| | VIOLATIONS | | | | ✓ | |

| Attribut | Zulässige Werte | Registrierung | Shadow | Konnektivität | DD-Verstöße | Benannter Schatten |
|---|---|---|---|---|---|---|
| `namedShadowIndexingMode` | Nicht angegeben. | | | | | |
| | OFF | | | | | |
| | ON | | | | | ✓ |

Verwaltete Felder und benutzerdefinierte Felder

Verwaltete Felder

Verwaltete Felder enthalten Daten, die mit Dingen, Dinggruppen, Geräteschatten, Gerätekonnektivität und Device Defender-Verstößen verknüpft sind. AWS IoT definiert den Datentyp in verwalteten Feldern. Beim Erstellen eines IoT-Objekts geben Sie die Werte jedes verwalteten Felds an. Beispielsweise sind Objektnamen, Objektgruppen und Objektbeschreibungen alles verwaltete Felder. Der Flottenindizierungsservice indiziert verwaltete Felder basierend auf dem von Ihnen angegebenen Indizierungsmodus: Verwaltete Felder können nicht geändert oder in `customFields` angezeigt werden.

Benutzerdefinierte Felder

Sie können Attribute, Device Schatten-Daten und Daten zu Device Defender-Verstößen aggregieren, indem Sie benutzerdefinierte Felder erstellen, um sie zu indizieren. Das Attribut `customFields` ist eine Liste von Feld- und Datentyppaaren. Sie können Aggregationsabfragen auf der Grundlage des Datentyps durchführen. Der von Ihnen gewählte Indizierungsmodus wirkt sich auf Felder aus, in denen Sie angeben können. `customFields` Wenn Sie beispielsweise den Indizierungsmodus `REGISTRY` angeben, können Sie kein Feld aus einem Schattenobjekt angeben. Sie können den update-indexing-configurationCLIBefehl verwenden, um die benutzerdefinierten Felder zu erstellen oder zu aktualisieren (einen Beispielbefehl finden Sie unter Beispiele zur Aktualisierung der Indexierungskonfiguration). Weitere Informationen zu RDS CUstom finden Sie unter .

Indizierungsfilter

Der Indexfilter bietet zusätzliche Auswahlmöglichkeiten für benannte Schatten und Geolokalisierungsdaten.

**`namedShadowNames`**

Um Ihrer Flottenindizierungskonfiguration benannte Schatten hinzuzufügen, legen Sie `namedShadowIndexingMode` als `ON` fest und geben Sie Ihre benannten Schattennamen im `namedShadowNames`-Filter an.

Beispiel

```
"filter": {
     "namedShadowNames": [ "namedShadow1", "namedShadow2" ]
}
```

**`geoLocations`**

So fügen Sie Ihrer Flottenindexierungskonfiguration Geolokalisierungsdaten hinzu:

- Wenn Ihre Geolokalisierungsdaten in einem klassischen (unbenannten) Schatten gespeichert sind, legen Sie den Wert `thingIndexingMode` auf REGISTRY _ AND _ SHADOW fest und geben Sie Ihre Geolokalisierungsdaten im Filter an. `geoLocations`

  Der folgende Beispielfilter spezifiziert ein geoLocation Objekt in einem klassischen (unbenannten) Schatten:

  ```
  "filter": {
       "geoLocations": [
          {
              "name": "shadow.reported.location",
              "order": "LonLat"
          }
       ]
    }
  ```

- Wenn Ihre Geolokalisierungsdaten in einem benannten Schatten gespeichert sind, setzen Sie `namedShadowIndexingMode` auf ON, fügen Sie den Schattennamen im `namedShadowNames`-Filter hinzu und geben Sie Ihre Geolokalisierungsdaten im `geoLocations`-Filter an.

  Der folgende Beispielfilter spezifiziert ein geoLocation Objekt in einem benannten Schatten (`nameShadow1`):

  ```
  "filter": {
       "namedShadowNames": [ "namedShadow1" ],
       "geoLocations": [
  ```

```
        {
            "name": "shadow.name.namedShadow1.reported.location",
            "order": "LonLat"
        }
    ]
}
```

Weitere Informationen finden Sie in IndexingFilterder AWS IoT APIReferenz.

Aktualisieren von Konfigurationsbeispielen für die Indexierung

Verwenden Sie den AWS IoT update-indexing-configuration CLI Befehl, um Ihre Indizierungskonfiguration zu aktualisieren. Im folgenden Beispiel wird gezeigt, wie update-indexing-configuration verwendet wird.

Kurze Syntax:

```
aws iot update-indexing-configuration --thing-indexing-configuration \
'thingIndexingMode=REGISTRY_AND_SHADOW, deviceDefenderIndexingMode=VIOLATIONS,
namedShadowIndexingMode=ON,filter={namedShadowNames=[thing1shadow]},
 thingConnectivityIndexingMode=STATUS,
customFields=[{name=attributes.version,type=Number},
{name=shadow.name.thing1shadow.desired.DefaultDesired, type=String},
 {name=shadow.desired.power, type=Boolean},
{name=deviceDefender.securityProfile1.NUMBER_VALUE_BEHAVIOR.lastViolationValue.number,
 type=Number}]'
```

JSONSyntax:

```
aws iot update-indexing-configuration --cli-input-json \ '{
          "thingIndexingConfiguration": { "thingIndexingMode": "REGISTRY_AND_SHADOW",
          "thingConnectivityIndexingMode": "STATUS",
          "deviceDefenderIndexingMode": "VIOLATIONS",
          "namedShadowIndexingMode": "ON",
          "filter": { "namedShadowNames": ["thing1shadow"]},
          "customFields": [ { "name": "shadow.desired.power", "type": "Boolean" },
          {"name": "attributes.version", "type": "Number"},
          {"name": "shadow.name.thing1shadow.desired.DefaultDesired", "type":
 "String"},
```

```
          {"name":
 "deviceDefender.securityProfile1.NUMBER_VALUE_BEHAVIOR.lastViolationValue.number",
 "type": Number} ] } }'
```

Dieser Befehl liefert keine Ausgabe.

Führen Sie den folgenden `describe-index` CLI Befehl aus, um den Status des Dingindexes zu überprüfen:

```
aws iot describe-index --index-name "AWS_Things"
```

Die Ausgabe des Befehls `describe-index` sieht wie folgt aus:

```
{
    "indexName": "AWS_Things",
    "indexStatus": "ACTIVE",
    "schema": "MULTI_INDEXING_MODE"
}
```

> **Note**
>
> Es kann einen Moment dauern, bis der Flottenindex bei der Flottenindizierung aktualisiert ist. Wir empfehlen, mit der Verwendung zu warten, bis die `indexStatus` Show angezeigt ACTIVE wird. Je nachdem, welche Datenquellen Sie konfiguriert haben, können Sie im Schemafeld unterschiedliche Werte angeben. Weitere Informationen finden Sie unter Beschreiben eines Objektindizents.

Führen Sie den `get-indexing-configuration` CLI folgenden Befehl aus, um die Konfigurationsdetails für die Indexierung Ihres Dings abzurufen:

```
aws iot get-indexing-configuration
```

Die Ausgabe des Befehls `get-indexing-configuration` sieht wie folgt aus:

```
{
    "thingIndexingConfiguration": {
        "thingIndexingMode": "REGISTRY_AND_SHADOW",
        "thingConnectivityIndexingMode": "STATUS",
        "deviceDefenderIndexingMode": "VIOLATIONS",
```

```
        "namedShadowIndexingMode": "ON",
        "managedFields": [
            {
                "name": "connectivity.disconnectReason",
                "type": "String"
            },
            {
                "name": "registry.version",
                "type": "Number"
            },
            {
                "name": "thingName",
                "type": "String"
            },
            {
                "name": "deviceDefender.violationCount",
                "type": "Number"
            },
            {
                "name": "shadow.hasDelta",
                "type": "Boolean"
            },
            {
                "name": "shadow.name.*.version",
                "type": "Number"
            },
            {
                "name": "shadow.version",
                "type": "Number"
            },
            {
                "name": "connectivity.version",
                "type": "Number"
            },
            {
                "name": "connectivity.timestamp",
                "type": "Number"
            },
            {
                "name": "shadow.name.*.hasDelta",
                "type": "Boolean"
            },
            {
                "name": "registry.thingTypeName",
```

```
                "type": "String"
            },
            {
                "name": "thingId",
                "type": "String"
            },
            {
                "name": "connectivity.connected",
                "type": "Boolean"
            },
            {
                "name": "registry.thingGroupNames",
                "type": "String"
            }
        ],
        "customFields": [
            {
                "name": "shadow.name.thing1shadow.desired.DefaultDesired",
                "type": "String"
            },

            {
                "name":
"deviceDefender.securityProfile1.NUMBER_VALUE_BEHAVIOR.lastViolationValue.number",
                "type": "Number"
            },
            {
                "name": "shadow.desired.power",
                "type": "Boolean"
            },
            {
                "name": "attributes.version",
                "type": "Number"
            }
        ],
        "filter": {
              "namedShadowNames": [
                  "thing1shadow"
              ]
          }
      },
    "thingGroupIndexingConfiguration": {
        "thingGroupIndexingMode": "OFF"
    }
```

```
}
```

Um die benutzerdefinierten Felder zu aktualisieren, können Sie den `update-indexing-configuration` Befehl ausführen. Das Beispiel ist wie folgt:

```
aws iot update-indexing-configuration --thing-indexing-configuration

 'thingIndexingMode=REGISTRY_AND_SHADOW,customFields=[{name=attributes.version,type=Number},
{name=attributes.color,type=String},{name=shadow.desired.power,type=Boolean},
{name=shadow.desired.intensity,type=Number}]'
```

Dieser Befehl hat der Indizierungskonfiguration `shadow.desired.intensity` hinzugefügt.

> **Note**
>
> Beim Aktualisieren der benutzerdefinierten Felder in der Indizierungskonfiguration werden alle vorhandenen benutzerdefinierten Felder überschrieben. Achten Sie darauf, beim Aufrufen von update-indexing-configuration alle benutzerdefinierten Felder anzugeben.

Nachdem der Index neu erstellt wurde, können Sie Aggregationsabfrage für die neu hinzugefügten Felder, Registrierungsdaten, Schattendaten und Statusdaten der Objektkonnektivität verwenden.

Stellen Sie beim Ändern des Indizierungsmodus sicher, dass alle benutzerdefinierten Felder im neuen Indizierungsmodus gültig sind. Wenn Sie beispielsweise im Modus `REGISTRY_AND_SHADOW` mit dem benutzerdefinierten Feld `shadow.desired.temperature` beginnen, müssen Sie das benutzerdefinierte Feld `shadow.desired.temperature` löschen, bevor Sie den Indizierungsmodus in `REGISTRY` ändern. Wenn Ihre Indizierungskonfiguration benutzerdefinierte Felder enthält, die nicht vom Indizierungsmodus indiziert werden, schlägt die Aktualisierung fehl.

## Beschreiben eines Objektindex

Der folgende Befehl zeigt Ihnen, wie Sie den describe-index CLI Befehl verwenden, um den aktuellen Status des Dingindexes abzurufen.

```
aws iot describe-index --index-name "AWS_Things"
```

Die Ausgabe des Befehls sieht wie folgt aus:

```
{
    "indexName": "AWS_Things",
    "indexStatus": "BUILDING",
    "schema": "REGISTRY_AND_SHADOW_AND_CONNECTIVITY_STATUS"
}
```

Wenn Sie zum ersten Mal eine Fleet-Indizierung durchführen, wird Ihr Index AWS IoT erstellt. Sie können den Index nicht abfragen, wenn sich `indexStatus` im Status `BUILDING` befindet. Das `schema` für den Objektindex zeigt an, welche Art von Daten (`REGISTRY_AND_SHADOW_AND_CONNECTIVITY_STATUS`) indiziert werden.

Wenn die Konfiguration für Ihren Index geändert wird, wird der Index neu erstellt. Der `indexStatus` während dieses Vorgangs lautet `REBUILDING`. Sie können Abfragen für Daten im Objektindex ausführen, während er erstellt wird. Wenn Sie beispielsweise die Indexkonfiguration von `REGISTRY` in `REGISTRY_AND_SHADOW` ändern, während der Index neu erstellt wird, können Sie Registrierungsdaten abfragen, einschließlich der aktuellen Updates. Sie können die Schattendaten jedoch erst abfragen, wenn die Wiederherstellung abgeschlossen ist. Die benötigte Zeit zum Erstellen oder Neuerstellen des Index hängt von der Menge an Daten ab.

Abhängig von den Datenquellen, die Sie konfiguriert haben, können Sie im Schemafeld unterschiedliche Werte sehen. Die folgende Tabelle zeigt die verschiedenen Schemawerte und die entsprechenden Beschreibungen:

| Schema | Beschreibung |
| --- | --- |
| OFF | Es sind keine Datenquellen konfiguriert oder indexiert. |
| REGISTRY | (Nur Registrierungsdaten werden indiziert.) |
| REGISTRY_AND_SHADOW | (Registrierungsdaten und Schatten-Daten werden indiziert.) |
| REGISTRY_AND_CONNECTIVITY | Registrierungsdaten und Konnektivitätsdaten sind indexiert. |
| REGISTRY_AND_SHADOW_AND_CONNECTIVITY_STATUS | Registrierungsdaten, unbenannte (klassische) Schattendaten und Konnektivitätsdaten werden indexiert. |

| Schema | Beschreibung |
| --- | --- |
| MULTI_INDEXING_MODE | Daten zu Verletzungen durch benannte Schatten- oder Device Defender-Angriffe werden zusätzlich zu Registrierungsdaten, unbenannten (klassischen) Schatten- oder Konnektivitätsdaten indexiert. |

## Abfragen des Objektindex

Verwenden Sie den search-index CLI Befehl, um Daten im Index abzufragen.

```
aws iot search-index --index-name "AWS_Things" --query-string
          "thingName:mything*"
```

```
{
    "things":[{
         "thingName":"mything1",
         "thingGroupNames":[
            "mygroup1"
         ],
         "thingId":"a4b9f759-b0f2-4857-8a4b-967745ed9f4e",
         "attributes":{
            "attribute1":"abc"
         },
         "connectivity": {
            "connected":false,
            "timestamp":1556649874716,
            "disconnectReason": "CONNECTION_LOST"
         }
    },
    {
        "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":{
                "location":"new york",
                "myvalues":[1, 2, 3],
                "stats":{
                    "battery":78
                }
            },
            "metadata":{
                 "desired":{
                       "location":{
                            "timestamp":123456789
                        },
                       "myvalues":{
                             "timestamp":123456789
                       }
                  },
                  "reported":{
                        "location":{
                             "timestamp":34535454
                         },
                        "myvalues":{
                             "timestamp":34535454
                        },
                        "stats":{
                             "battery":{
                                   "timestamp":34535454
                             }
                        }
                 }
            },
            "version":10,
            "timestamp":34535454
        },
        "connectivity": {
            "connected":true,
            "timestamp":1556649855046
```

```
        }
    }],
    "nextToken":"AQFCuvk7zZ3D9pOYMbFCeHbdZ+h=G"
}
```

In der JSON Antwort werden `"connectivity"` (wie durch die `thingConnectivityIndexingMode=STATUS` Einstellung aktiviert) ein boolescher Wert, ein Zeitstempel und ein Wert angegeben, der disconnectReason angibt, ob das Gerät angeschlossen ist. AWS IoT Core Die Verbindung zum Gerät `"mything1"` wurde aufgrund von unterbrochen (`false`). POSIX `1556649874716` `CONNECTION_LOST` Weitere Informationen zu den Gründen für die Unterbrechung der Verbindung finden Sie unter Lifecycle-Ereignisse.

```
"connectivity": {
    "connected":false,
    "timestamp":1556649874716,
    "disconnectReason": "CONNECTION_LOST"
}
```

Das Gerät `"mything2"` ist zu der POSIX Zeit `1556649855046` verbunden (`true`):

```
"connectivity": {
    "connected":true,
    "timestamp":1556649855046
}
```

Zeitstempel werden in Millisekunden seit der Epoche angegeben, `1556649855046` entspricht also 18:44:15.046 Uhr am Dienstag, 30. April 2019 (). UTC

> **Important**
>
> Wenn ein Gerät etwa eine Stunde lang getrennt war, fehlt möglicherweise der `"timestamp"`-Wert und der `"disconnectReason"`-Wert des Konnektivitätsstatus.

## Beschränkungen und Einschränkungen

Dies sind die Einschränkungen und Begrenzungen für `AWS_Things`.

### Schatten-Felder mit komplexen Typen

Ein Schattenfeld wird nur indexiert, wenn der Wert des Felds ein einfacher Typ ist, z. B. ein JSON Objekt, das kein Array enthält, oder ein Array, das ausschließlich aus einfachen Typen besteht. Mit „einfacher Typ“ ist eine Zeichenfolge, eine Zahl oder eines der Literale `true` oder `false` gemeint. Beispielsweise angesichts des folgenden Schattenzustands wird der Wert des Feldes `"palette"` nicht indiziert, da es sich um ein Array handelt, das Elemente komplexen Typs enthält. Der Wert des Feldes `"colors"` wird indiziert, da jeder Wert im Array eine Zeichenfolge ist.

```
{
    "state": {
        "reported": {
            "switched": "ON",
            "colors": [ "RED", "GREEN", "BLUE" ],
            "palette": [
                {
                    "name": "RED",
                    "intensity": 124
                },
                {
                    "name": "GREEN",
                    "intensity": 68
                },
                {
                    "name": "BLUE",
                    "intensity": 201
                }
            ]
        }
    }
}
```

### Verschachtelte Schattenfeldnamen

Die Namen verschachtelter Schattenfelder werden als Zeichenfolge mit Punkt als Trennzeichen (.) gespeichert. Beispielsweise bei einem Schattendokument:

```
{
  "state": {
    "desired": {
      "one": {
```

```
        "two": {
          "three": "v2"
        }
      }
    }
  }
}
```

Der Name des Feldes `three` wird als `desired.one.two.three` gespeichert. Wenn Sie auch ein Schattendokument wie das folgende haben:

```
{
  "state": {
    "desired": {
      "one.two.three": "v2"
    }
  }
}
```

Beide entsprechen einer Abfrage für `shadow.desired.one.two.three:v2`. Eine bewährte Methode besteht darin, keine Punkte in Schattenfeldnamen zu verwenden.

Schatten-Metadaten

Ein Feld in einem Schatten-Metadatenbereich wird indiziert, aber nur dann, wenn das entsprechende Feld in dem `"state"`-Abschnitt des Shadow indiziert ist. (Im vorherigen Beispiel wird das Feld `"palette"` im Metadatenbereich des Schattens auch nicht indiziert.)

Alle nicht registrierten Geräte

Die Flottenindizierung indexiert den Konnektivitätsstatus für ein Gerät, dessen Verbindung `clientId` mit der eines in `thingName` der Registrierung registrierten Geräts übereinstimmt.

Nicht registrierte Schatten

Wenn Sie UpdateThingShadoweinen Schatten mit einem Dingnamen erstellen, der nicht in Ihrem AWS IoT Konto registriert wurde, werden Felder in diesem Schatten nicht indexiert. Dies gilt sowohl für den klassischen unbenannten Schatten als auch für den benannten Schatten.

Numerische Werte

Wenn Registrierungs- oder Schattendaten von dem Service als numerischer Wert erkannt werden, werden sie als solche indiziert. Sie können Abfragen erstellen, die Bereiche und

Vergleichsoperatoren für numerische Werte umfassen (beispielsweise `"attribute.foo<5"` oder `"shadow.reported.foo:[75 TO 80]"`). Um als numerisch erkannt zu werden, muss es sich bei dem Wert der Daten um eine gültige, buchstäbliche Zahl handeln. JSON Um als numerisch erkannt zu werden, muss der Wert der Daten ein gültiges JSON-Literal des Typs „Zahl“ (eine Ganzzahl von -2^53...2^53-1 oder ein Gleitkomma mit doppelter Genauigkeit und optionaler Exponentialnotation) oder Teil eines Arrays sein, das ausschließlich solche Werte enthält.

Null-Werte

Null-Werte werden nicht indiziert.

Maximale Werte

Maximale Anzahl von benutzerdefinierten Felder für Aggregationsabfragen ist 5.

Maximale Anzahl von angeforderten Perzentilen für Aggregationsabfragen ist 100.

## Autorisierung

Sie können den Things-Index in einer AWS IoT Richtlinienaktion wie folgt als Amazon-Ressourcennamen (ARN) angeben.

| Aktion | Ressource |
| --- | --- |
| `iot:SearchIndex` | Ein Index ARN (zum Beispiel`arn:aws:iot: your-aws-region your-aws-account :index/AWS_Things` ). |
| `iot:DescribeIndex` | Ein Index ARN (zum Beispiel`arn:aws:iot: your-aws-region :index/AWS_Things` ). |

> **Note**
>
> Wenn Sie über die Berechtigungen verfügen, den Flottenindex abzufragen, können Sie auf Daten zu Objekten über die gesamte Flotte hinweg zugreifen.

# Verwalten der Objektgruppenindizierung

`AWS_ThingGroups` ist der Index, die alle Ihre Objektgruppen enthält. Dieser Index ermöglicht Ihnen die Suche nach Gruppen basierend auf Gruppennamen, Beschreibung, Attributen und allen übergeordneten Gruppennamen.

## Aktivieren der Objektgruppenindizierung

Sie können die `thing-group-indexing-configuration` Einstellung in verwenden UpdateIndexingConfigurationAPI, um den `AWS_ThingGroups` Index zu erstellen und seine Konfiguration zu steuern. Sie können den verwenden GetIndexingConfigurationAPI, um die aktuelle Indizierungskonfiguration abzurufen.

Führen Sie den folgenden Befehl aus, um die Indexierungskonfigurationen für Dinggruppen zu aktualisieren: update-indexing-configuration CLI

```
aws iot update-indexing-configuration --thing-group-indexing-configuration
 thingGroupIndexingMode=ON
```

Sie können Konfigurationen für sowohl die Objekt- als auch die Objektgruppenindizierung wie folgt auch in einem einzigen Befehl aktualisieren.

```
aws iot update-indexing-configuration --thing-indexing-configuration
 thingIndexingMode=REGISTRY --thing-group-indexing-configuration
 thingGroupIndexingMode=ON
```

Im Folgenden sehen Sie gültige Werte für `thingGroupIndexingMode`.

OFF

Keine Indizierung/Index löschen

ON

Den `AWS_ThingGroups`-Index erstellen oder konfigurieren.

Führen Sie den folgenden Befehl aus, um die aktuellen Konfigurationen für die Indizierung von Dingen und Dinggruppen abzurufen: get-indexing-configuration CLI

```
aws iot get-indexing-configuration
```

Die Ausgabe des Befehls sieht wie folgt aus:

```
{
   "thingGroupIndexingConfiguration": {
        "thingGroupIndexingMode": "ON"
    }
}
```

## Beschreiben von Gruppenindizes

Verwenden Sie den describe-index CLI folgenden Befehl, um den aktuellen Status des `AWS_ThingGroups` Indexes abzurufen:

```
aws iot describe-index --index-name "AWS_ThingGroups"
```

Die Ausgabe des Befehls sieht wie folgt aus:

```
{
   "indexStatus": "ACTIVE",
   "indexName": "AWS_ThingGroups",
   "schema": "THING_GROUPS"
}
```

AWS IoT erstellt Ihren Index, wenn Sie ihn zum ersten Mal indizieren. Es ist nicht möglich, den Index abzufragen, wenn `indexStatus` auf `BUILDING` eingestellt ist.

## Abfragen eines Objektgruppenindex

Verwenden Sie den search-index CLI folgenden Befehl, um Daten im Index abzufragen:

```
aws iot search-index --index-name "AWS_ThingGroups" --query-string
 "thingGroupName:mythinggroup*"
```

## Autorisierung

Sie können den Dinggruppen-Index wie folgt als Ressource ARN in einer AWS IoT Richtlinienaktion angeben.

| Aktion | Ressource |
| --- | --- |
| `iot:SearchIndex` | Ein Index ARN (zum Beispiel`arn:aws:iot: your-aws-region :index/AWS_ThingGroups` ). |
| `iot:DescribeIndex` | Ein Index ARN (zum Beispiel`arn:aws:iot: your-aws-region :index/AWS_ThingGroups` ). |

# Abfragen zum Status der Gerätekonnektivität

AWS IoT Fleet Indexing unterstützt die Abfrage der Konnektivität einzelner Geräte, sodass Sie den Konnektivitätsstatus und die zugehörigen Metadaten für bestimmte Geräte effizient abrufen können. Diese Funktion ergänzt die bestehenden flottenweiten Indizierungs- und Abfragefunktionen.

## Funktionsweise

Die Unterstützung von Abfragen zur Gerätekonnektivität kann für den optimierten Abruf des Verbindungsstatus einzelner Geräte verwendet werden. Dies API ermöglicht den Zugriff auf die neuesten gerätespezifischen Konnektivitätsinformationen mit niedriger Latenz und hohem Durchsatz. Sobald Sie die Konnektivitätsindizierung aktiviert haben, haben Sie Zugriff auf diese Abfrage, API die als Standardabfragen berechnet wird. Weitere Informationen finden Sie unter AWS IoT Device Management — Preise

## Features

Mit der Unterstützung von Abfragen zur Gerätekonnektivität können Sie:

1. Fragen Sie den aktuellen Konnektivitätsstatus (verbunden oder getrennt) für ein bestimmtes Gerät ab, indem Sie ihn verwenden. `thingName`
2. Rufen Sie zusätzliche Konnektivitätsmetadaten ab, darunter:
   a. Grund für das Trennen der Verbindung
   b. Zeitstempel für das letzte Verbindungs- oder Trennungsereignis.

> **Note**
>
> Die Flottenindizierung indexiert den Konnektivitätsstatus für ein Gerät, dessen Verbindung `clientId` mit der eines in `thingName` der Registrierung registrierten Geräts übereinstimmt.

## Vorteile

1. Niedrige Latenz: Spiegelt den neuesten Status der Gerätekonnektivität wider und bietet eine geringe Latenz, um Änderungen des Verbindungsstatus von IoT Core widerzuspiegeln. IoT Core bestimmt, dass ein Gerät entweder getrennt ist, sobald es eine Verbindungsabbruchanfrage vom Gerät erhält, oder wenn ein Gerät die Verbindung trennt, ohne eine Trennungsanfrage zu senden. Der IoT-Core wartet das 1,5-fache der konfigurierten Keep-Alive-Zeit, bevor festgestellt wird, dass der Client getrennt wird. Der Konnektivitätsstatus spiegelt API diese Änderungen in der Regel weniger als eine Sekunde wider, nachdem IoT Core die Änderung des Verbindungsstatus eines Geräts festgestellt hat.
2. Hoher Durchsatz: Unterstützt standardmäßig 350 Transaktionen pro Sekunde (TPS) und kann auf Anfrage auf einen höheren Wert eingestellt werden.
3. Datenspeicherung: Speichert Ereignisdaten auf unbestimmte Zeit, wenn der Fleet Indexing (FI) ConnectivityIndexing -Modus aktiviert ist und das Ding nicht gelöscht wird. Wenn Sie die Konnektivitätsindizierung deaktivieren, werden die Datensätze nicht aufbewahrt.

> **Note**
>
> Wenn die Indizierung des Konnektivitätsstatus vor dem Start aktiviert warAPI, beginnt Fleet Indexing mit der Verfolgung von Änderungen des Konnektivitätsstatus nach dem API Start und spiegelt den aktualisierten Status auf der Grundlage dieser Änderungen wider.

## Voraussetzungen

So verwenden Sie die Unterstützung für Gerätekonnektivitätsabfragen:

1. Richten Sie ein AWS Konto ein
2. Geräte AWS IoT Core in Ihrer bevorzugten Region einbinden und registrieren
3. Aktivieren Sie die Flottenindizierung mit der Konnektivitätsindizierung

> **Note**
>
> Es ist keine zusätzliche Einrichtung erforderlich, wenn Sie die Konnektivitätsindizierung bereits aktiviert haben

Ausführliche Anweisungen zur Einrichtung finden Sie im AWS IoT Entwicklerhandbuch

## Beispiele

```
aws iot get-thing-connectivity-data --thing-name myThingName
```

```
{
   "connected": true,
   "disconnectReason": "NONE",
   "thingName": "myThingName",
   "timestamp": "2024-12-19T10:00:00.000000-08:00"
}
```

- `thingName`: Der Name des Geräts, wie er in der Anfrage angegeben ist. Dies entspricht auch dem, mit clientId dem die Verbindung hergestellt wurde AWS IoT Core.
- `disconnectReason`: Grund für die Verbindung. Gilt NONE für ein angeschlossenes Gerät.
- `connected`: Der boolesche Wert true gibt an, dass dieses Gerät derzeit verbunden ist.
- `timestamp`: Der Zeitstempel, der die letzte Unterbrechung des Geräts in Millisekunden darstellt.

```
aws iot get-thing-connectivity-data --thing-name myThingName
```

```
{
   "connected": false,
   "disconnectReason": "CLIENT_INITIATED_DISCONNECT",
   "thingName": "myThingName",
   "timestamp": "2024-12-19T10:30:00.000000-08:00"
}
```

- `thingName`: Der Name des Geräts, wie er in der Anfrage angegeben ist. Dies entspricht auch dem, mit clientId dem die Verbindung hergestellt wurde AWS IoT Core.
- `disconnectReason`: Der Grund für die Verbindung ist CLIENT _ INITIATED _, DISCONNECT was bedeutet, dass der Client angegeben hat, AWS IoT Core dass er die Verbindung trennen würde.
- `connected`: Der boolesche Wert false gibt an, dass dieses Gerät derzeit nicht verbunden ist.
- `timestamp`: Der Zeitstempel, der die letzte Unterbrechung des Geräts in Millisekunden darstellt.

```
aws iot get-thing-connectivity-data --thing-name neverConnectedThing
```

```
{
   "connected": false,
   "disconnectReason": "UNKNOWN",
   "thingName": "neverConnectedThing"
}
```

- `thingName`: Der Name des Geräts, wie er in der Anfrage angegeben ist. Dies entspricht auch dem, mit clientId dem die Verbindung hergestellt wurde AWS IoT Core.
- `disconnectReason`: Grund für die Verbindung. Steht für „UNKNOWN“ für ein Gerät, das noch nie verbunden war oder für das Fleet Indexing nicht den letzten Grund für die Unterbrechung der Verbindung gespeichert hat.
- `connected`: Der boolesche Wert false gibt an, dass dieses Gerät derzeit nicht angeschlossen ist.
- `timestamp`: Der Zeitstempel wird nicht für ein Gerät zurückgegeben, das noch nie verbunden war oder für das Fleet Indexing nicht den letzten Zeitstempel gespeichert hat.

## Abfragen von Aggregatdaten

AWS IoT bietet vier APIs (`GetStatistics`,`GetCardinality`, und`GetBucketsAggregation`)`GetPercentiles`, mit denen Sie Ihre Geräteflotte nach aggregierten Daten durchsuchen können.

> **Note**
>
> Bei Problemen mit fehlenden oder unerwarteten Werten für die Aggregation APIs lesen Sie den Leitfaden zur Fehlerbehebung bei der Fleet-Indexierung.

## GetStatistics

Der Befehl GetStatisticsAPIund der get-statistics CLI Befehl geben die Anzahl, den Durchschnitt, die Summe, das Minimum, das Maximum, die Summe der Quadrate, die Varianz und die Standardabweichung für das angegebene aggregierte Feld zurück.

Der get-statistics-Befehl CLI verwendet die folgenden Parameter:

`index-name`

Der Name des zu durchsuchenden Indexes. Der Standardwert ist `AWS_Things`.

`query-string`

Die zur Abfrage des Indexes verwendete Abfrage. Sie können angeben`"*"`, dass die Anzahl aller indizierten Objekte in Ihrem abgerufen werden soll. AWS-Konto

`aggregationField`

(Optional) Das zu aggregierende Feld. Dieses Feld muss ein verwaltetes oder benutzerdefiniertes Feld sein, das beim Aufruf von update-indexing-configuration definiert wird. Wenn Sie kein Aggregationsfeld angeben, wird `registry.version` als Aggregationsfeld verwendet.

`query-version`

Die Version der Abfrage, die verwendet werden soll. Der Standardwert ist `2017-09-30`.

Der Typ des Aggregationsfelds kann sich auf die zurückgegebenen Statistiken auswirken.

### GetStatistics mit Zeichenkettenwerten

Wenn Sie in einem Zeichenfolgenfeld aggregieren, gibt der Aufruf von `GetStatistics` eine Anzahl von Geräten zurück, die Attribute aufweisen, die der Abfrage entsprechen. Beispielsweise:

```
aws iot get-statistics --aggregation-field 'attributes.stringAttribute'
            --query-string '*'
```

Dieser Befehl gibt die Anzahl der Geräte zurück, die ein Attribut mit dem Namen `stringAttribute` enthalten:

```
{
  "statistics": {
    "count": 3
  }
}
```

## GetStatistics mit booleschen Werten

Wenn Sie `GetStatistics` mit einem booleschen Aggregationsfeld aufrufen:

- AVERAGEist der Prozentsatz der Geräte, die der Abfrage entsprechen.
- MINIMUMist gemäß den folgenden Regeln 0 oder 1:
  - Wenn alle Werte für das Aggregationsfeld gleich sind`false`, MINIMUM ist 0.
  - Wenn alle Werte für das Aggregationsfeld gleich sind`true`, MINIMUM ist 1.
  - Wenn die Werte für das Aggregationsfeld eine Mischung aus `false` und sind`true`, MINIMUM ist 0.
- MAXIMUMist 0 oder 1 gemäß den folgenden Regeln:
  - Wenn alle Werte für das Aggregationsfeld gleich sind`false`, MAXIMUM ist 0.
  - Wenn alle Werte für das Aggregationsfeld gleich sind`true`, MAXIMUM ist 1.
  - Wenn die Werte für das Aggregationsfeld eine Mischung aus `false` und sind`true`, MAXIMUM ist 1.
- SUMist die Summe der ganzzahligen Entsprechungen der booleschen Werte.
- COUNTist die Anzahl der Elemente, die den Kriterien der Abfragezeichenfolge entsprechen und einen gültigen Aggregationsfeldwert enthalten.

## GetStatistics mit numerischen Werten

Wenn Sie `GetStatistics` aufrufen und ein Aggregationsfeld vom Typ `Number` angeben, gibt `GetStatistics` die folgenden Werte zurück:

count

Die Anzahl der Elemente, die den Kriterien der Abfragezeichenfolge entsprechen und einen gültigen Aggregationsfeldwert enthalten.

Durchschnitt

Der Durchschnitt der numerischen Werte, die der Abfrage entsprechen.

sum

Die Summe der numerischen Werte, die der Abfrage entsprechen.

Minimum

Der kleinste numerische Wert, der der Abfrage entspricht.

Maximum

Der größte numerische Wert, der der Abfrage entspricht.

sumOfSquares

Die Summe der Quadrate der numerischen Werte, die der Abfrage entsprechen.

Varianz

Die Varianz der numerischen Werte, die der Abfrage entsprechen. Die Varianz einer Wertemenge ist der Durchschnitt der Quadrate der Differenzen jedes einzelnen Werts vom Durchschnittswert der Menge.

stdDeviation

Die Standardabweichung der numerischen Werte, die der Abfrage entsprechen. Die Standardabweichung einer Wertemenge ist ein Maß für die Verteilung der Werte.

Das folgende Beispiel zeigt, wie get-statistics mit einem numerischen benutzerdefinierten Feld aufgerufen wird.

```
aws iot get-statistics --aggregation-field 'attributes.numericAttribute2'
            --query-string '*'
```

```
{
  "statistics": {
    "count": 3,
    "average": 33.333333333333336,
    "sum": 100.0,
    "minimum": -125.0,
    "maximum": 150.0,
```

```
    "sumOfSquares": 43750.0,
    "variance": 13472.22222222222,
    "stdDeviation": 116.06990230986766
  }
}
```

Wenn die Feldwerte den maximalen doppelten Wert überschreiten, sind bei numerischen Aggregationsfeldern die Statistikwerte leer.

## GetCardinality

Der Befehl GetCardinalityAPIund der get-cardinality CLI Befehl geben die ungefähre Anzahl der eindeutigen Werte zurück, die der Abfrage entsprechen. Beispiel: Sie möchten die Anzahl der Geräte mit einem Akkustand von weniger als 50 Prozent ermitteln:

```
aws iot get-cardinality --index-name AWS_Things --query-string "batterylevel
         > 50" --aggregation-field "shadow.reported.batterylevel"
```

Dieser Befehl gibt die Anzahl der Elemente mit einem Akkustand von mehr als 50 Prozent zurück:

```
{
    "cardinality": 100
}
```

`cardinality` wird immer von get-cardinality zurückgegeben, auch wenn keine übereinstimmenden Felder vorhanden sind. Beispielsweise:

```
aws iot get-cardinality --query-string "thingName:Non-existent*"
         --aggregation-field "attributes.customField_STR"
```

```
{
    "cardinality": 0
}
```

Der get-cardinality-Befehl CLI verwendet die folgenden Parameter:

`index-name`

Der Name des zu durchsuchenden Indexes. Der Standardwert ist `AWS_Things`.

`query-string`

Die zur Abfrage des Indexes verwendete Abfrage. Sie können angeben`"*"`, dass die Anzahl aller indizierten Dinge in Ihrem AWS-Konto abgerufen werden soll.

`aggregationField`

Das zu aggregierende Feld.

`query-version`

Die Version der Abfrage, die verwendet werden soll. Der Standardwert ist `2017-09-30`.

## GetPercentiles

Der Befehl GetPercentilesAPIund der get-percentiles CLI Befehl gruppiert die aggregierten Werte, die der Abfrage entsprechen, in Perzentilgruppierungen. Die standardmäßigen Perzentilgruppierungen sind 1,5,25,50,75,95,99, auch wenn Sie beim Aufrufen von `GetPercentiles` Ihre eigenen angeben können. Diese Funktion gibt einen Wert für jede angegebene Perzentilgruppe (oder die standardmäßigen Perzentilgruppierungen) zurück. Die Perzentilgruppe „1“ enthält den aggregierten Feldwert, der in etwa in einem Prozent der Werte auftritt, die der Abfrage entsprechen. Die Perzentilgruppe „5“ enthält den aggregierten Feldwert, der in etwa in fünf Prozent der Werte auftritt, die der Abfrage entsprechen, usw. Das Ergebnis ist eine Annäherung, je mehr Werte der Abfrage entsprechen, desto genauer sind die Perzentilwerte.

Das folgende Beispiel zeigt, wie der Befehl aufgerufen wird. get-percentiles CLI

```
aws iot get-percentiles --query-string "thingName:*" --aggregation-field
          "attributes.customField_NUM" --percents 10 20 30 40 50 60 70 80 90 99
```

```
{
    "percentiles": [
        {
            "value": 3.0,
            "percent": 80.0
        },
        {
            "value": 2.5999999999999996,
            "percent": 70.0
        },
```

```
        {
            "value": 3.0,
            "percent": 90.0
        },
        {
            "value": 2.0,
            "percent": 50.0
        },
        {
            "value": 2.0,
            "percent": 60.0
        },
        {
            "value": 1.0,
            "percent": 10.0
        },
        {
            "value": 2.0,
            "percent": 40.0
        },
        {
            "value": 1.0,
            "percent": 20.0
        },
        {
            "value": 1.4,
            "percent": 30.0
        },
        {
            "value": 3.0,
            "percent": 99.0
        }
    ]
}
```

Der folgende Befehl zeigt die Ausgabe von get-percentiles, wenn keine entsprechenden Dokumente vorhanden sind.

```
aws iot get-percentiles --query-string "thingName:Non-existent*"
          --aggregation-field "attributes.customField_NUM"
```

```
{
    "percentiles": []
```

```
}
```

Der get-percentile-Befehl CLI verwendet die folgenden Parameter:

`index-name`

Der Name des zu durchsuchenden Indexes. Der Standardwert ist `AWS_Things`.

`query-string`

Die zur Abfrage des Indexes verwendete Abfrage. Sie können angeben`"*"`, dass die Anzahl aller indizierten Dinge in Ihrem AWS-Konto abgerufen werden soll.

`aggregationField`

Das zu aggregierende Feld, das den Typ `Number` aufweisen muss.

`query-version`

Die Version der Abfrage, die verwendet werden soll. Der Standardwert ist `2017-09-30`.

`percents`

Mit diesem Parameter können Sie benutzerdefinierte Perzentilgruppierungen angeben.

## GetBucketsAggregation

Der Befehl GetBucketsAggregationAPIund der get-buckets-aggregation CLI Befehl geben eine Liste von Buckets und die Gesamtzahl der Dinge zurück, die den Kriterien der Abfragezeichenfolge entsprechen.

Das folgende Beispiel zeigt, wie der get-buckets-aggregation CLI Befehl aufgerufen wird.

```
aws iot get-buckets-aggregation --query-string '*' --index-name AWS_Things --
aggregation-field 'shadow.reported.batterylevelpercent' --buckets-aggregation-type
 'termsAggregation={maxBuckets=5}'
```

Dieser Befehl gibt die folgende Ausgabe zurück: .

```
{
    "totalCount": 20,
    "buckets": [
```

```
        {
            "keyValue": "100",
            "count": 12
        },
        {
            "keyValue": "90",
            "count": 5
        },
        {
            "keyValue": "75",
            "count": 3
        }
    ]
}
```

Der get-buckets-aggregation CLI Befehl verwendet die folgenden Parameter:

`index-name`

Der Name des zu durchsuchenden Indexes. Der Standardwert ist `AWS_Things`.

`query-string`

Die zur Abfrage des Indexes verwendete Abfrage. Sie können angeben`"*"`, dass die Anzahl aller indizierten Dinge in Ihrem AWS-Konto abgerufen werden soll.

`aggregation-field`

Das zu aggregierende Feld.

`buckets-aggregation-type`

Die grundlegende Steuerung der Antwortform und des auszuführenden Bucket-Aggregationstyps.

## Autorisierung

Sie können den Index der Dinggruppen wie folgt als Ressource ARN in einer AWS IoT Richtlinienaktion angeben.

| Aktion | Ressource |
| --- | --- |
| `iot:GetStatistics` | Ein Index ARN (zum Beispiel `arn:aws:iot:` *`your-aws-region`* `:index/AW` |

| Aktion | Ressource |
| --- | --- |
| | S_Things oderarn:aws:iot: *your-aws-region* :index/AWS_ThingGroups ). |

# Abfragesyntax

Bei der Flottenindizierung verwenden Sie eine Abfragesyntax, um Abfragen zu spezifizieren.

## Unterstützte Features

Die Abfragesyntax unterstützt die folgenden Funktionen.

- Begriffe und Ausdrücke
- Suchen nach Feldern
- Präfixsuche
- Bereichssuche
- Boolesche Operatoren `AND`, `OR`, `NOT` und `-`. Der Bindestrich wird verwendet, um Suchergebnisse auszuschließen (z. B. `thingName:(tv* AND -plasma)`).
- Gruppierung
- Feldgruppierung
- Escape-Sonderzeichen (wie bei )

## Nicht unterstützte Funktionen

Die Abfragesyntax unterstützt nicht die folgenden Funktionen:

- Suche mit vorangestellten Platzhaltern (z. B. „*xyz“), bei der Suche nach „*“ werden jedoch alle Objekte erfasst
- Reguläre Ausdrücke
- Boosting
- Ranking
- Fuzzysuchen
- Umgebungssuche

- Sortieren
- Aggregation
- Sonderzeichen: `,@,#,%,\,/, ';, und ,. Beachten Sie, dass , dies nur in Geoqueries unterstützt wird.

## Hinweise

Hier einige Hinweise zur Abfragesprache:

- Der Standardoperator istAND. Eine Abfrage für "thingName:abc thingType:xyz" ist äquivalent mit "thingName:abc AND thingType:xyz".
- Wenn kein Feld angegeben ist, wird in allen Registry-, Device Shadow- und Device Defender-Feldern nach dem Begriff AWS IoT gesucht.
- Bei allen Feldnamen muss die Groß- und Kleinschreibung beachtet werden.
- Bei der Suche muss die Groß- und Kleinschreibung nicht beachtet werden. Wörter werden gemäß Definition von Character.isWhitespace(int) von Java durch Leerzeichen getrennt.
- Die Indizierung von Device Schatten enthält die folgenden Abschnitte: gemeldet, gewünscht, Delta und Metadaten.
- Device Schatten- und Registry-Versionen können nicht durchsucht werden, sind jedoch in der Antwort vorhanden.
- Die maximale Anzahl an Begriffen in einer Abfrage ist 5.
- Das Sonderzeichen , wird nur in Geoqueries unterstützt.

# Beispiel für Objektabfragen

Geben Sie Abfragen mithilfe einer Abfragesyntax in einer Abfragezeichenfolge an. Die Abfragen werden an die übergeben SearchIndexAPI. Die folgende Tabelle enthält einige Beispiele für Abfragezeichenfolgen.

| Abfragezeichenfolge | Ergebnis |
| --- | --- |
| abc | Abfragen nach „abc“ in beliebigen Registry-, Schatten- (klassischer unbenannter Shadow und benannter Shadow) oder Device Defender-Verstößen. |

| Abfragezeichenfolge | Ergebnis |
| --- | --- |
| `thingName:myThingName` | Abfragen für ein Ding mit dem Namen "myThingName“. |
| `thingName:my*` | Abfragen von Objekten mit Namen, die mit „my” beginnen. |
| `thingName:ab?` | Abfragen von Objekten mit Namen, die "ab" sowie ein zusätzliches Zeichen enthalten, zum Beispiel: "aba", "abb", "abc" usw. |
| `thingTypeName:aa` | Abfragen für Objekte, die dem Typ aa zugeordnet sind. |
| `thingGroupNames:a` | Abfragen für Dinge mit dem Namen „a“ als übergeordneter Sachgruppe oder Abrechnungsgruppe. |
| `thingGroupNames:a*` | Abfragen für Dinge, bei denen der Name einer übergeord neten Sachgruppe oder einer Abrechnungsgruppe dem Muster „a*“ entspricht. |
| `attributes.myAttribute:75` | Abfragen nach Dingen mit einem Attribut namens "myAttrib ute", das den Wert 75 hat. |
| `attributes.myAttribute: [75 TO 80]` | Abfragen nach Dingen mit einem Attribut namens "myAttrib ute", dessen Wert in einen numerischen Bereich (75—80, einschließlich) fällt. |
| `attributes.myAttribute: {75 TO 80]` | Abfragen nach Dingen mit einem Attribut namens "myAttrib ute", dessen Wert in den numerischen Bereich (>75 und <=80) fällt. |
| `attributes.serialNumber: ["abcd" TO "abcf"]` | Abfragen nach Dingen mit einem Attribut namens "serialNu mber", dessen Wert innerhalb eines alphanumerischen Zeichenkettenbereichs liegt. Diese Abfrage gibt Dinge mit einem "serialNumber" -Attribut mit den Werten „abcd“, „abce“ oder „abcf“ zurück. |
| `attributes.myAttri bute:i*t` | Fragt nach Dingen mit einem Attribut namens "myAttrib ute" ab, wobei der Wert 'i' ist, gefolgt von einer beliebigen Anzahl von Zeichen, gefolgt von 't' |

| Abfragezeichenfolge | Ergebnis |
| --- | --- |
| `attributes.attr1:abc AND attributes.attr2<5 NOT attributes.attr3>10` | Abfragen mit booleschen Ausdrücken von Objekten, die Begriffe kombinieren. Diese Abfrage gibt Objekte zurück, die ein Attribut mit dem Namen "attr1" mit dem Wert "abc", ein Attribut mit dem Namen "attr2", das kleiner als 5 ist, und ein Attribut mit dem Namen "attr3", das nicht größer als 10 ist, aufweisen. |
| `shadow.hasDelta:true` | Abfragen nach Objekten mit einem unbenannten Schatten, der ein Deltaelement enthält. |
| `NOT attributes.model:legacy` | Abfragen von Objekten, bei denen das Attribut namens "model" nicht "legacy" ist. |
| `shadow.reported.stats.battery:{70 TO 100} (v2 OR v3) NOT attributes.model:legacy` | Abfragen von Objekten, für die Folgendes gilt:<br>• Das Schattenattribut `stats.battery` des Objekts enthält einen Wert zwischen 70 und 100.<br>• Der Text „v2” oder „v3” ist im Namen, im Typnamen oder in den Attributwerten eines Objekts enthalten.<br>• Das Attribut `model` des Objekts ist nicht auf „legacy” festgelegt. |
| `shadow.reported.myvalues:2` | Abfragen von Objekten, bei denen das Array `myvalues` im Abschnitt Gemeldete des Schattens den Wert 2 enthält. |
| `shadow.reported.location:* NOT shadow.desired.stats.battery:*` | Abfragen von Objekten, für die Folgendes gilt:<br>• Das Attribut `location` ist im Abschnitt `reported` des Schattens vorhanden.<br>• Das Attribut `stats.battery` ist nicht im Abschnitt `desired` des Schattens vorhanden. |
| `shadow.name.<shadowName>.hasDelta:true` | Abfragen nach Objekten, die einen Schatten mit dem angegebenen Namen und auch ein Delta-Element haben. |

| Abfragezeichenfolge | Ergebnis |
| --- | --- |
| `shadow.name.<shadowName>.desired.filament:*` | Fragt nach Objekten ab, die einen Schatten mit dem angegebenen Namen und auch einer gewünschten Filamenteigenschaft haben. |
| `shadow.name.<shadowName>.reported.location:*` | Fragt nach Objekten, die einen Schatten mit dem angegebenen Namen haben und bei denen das `location` Attribut im Berichtsbereich des benannten Schattens vorhanden ist. |
| `connectivity.connected:true` | Abfragen für alle angeschlossenen Geräte. |
| `connectivity.connected:false` | Abfrage für alle nicht verbundenen Geräte. |
| `connectivity.connected:true AND connectivity.timestamp : [1557651600000 TO 1557867600000]` | Abfragen für alle verbundenen Geräte mit einem Verbindungszeitstempel >= 1557651600000 und <= 1557867600000. Zeitstempel werden in Millisekunden seit der Epoche angegeben. |
| `connectivity.connected:false AND connectivity.timestamp : [1557651600000 TO 1557867600000]` | Abfragen für alle getrennten Geräte mit einem Trennungszeitstempel >= 1557651600000 und <= 1557867600000. Zeitstempel werden in Millisekunden seit der Epoche angegeben. |
| `connectivity.connected:true AND connectivity.timestamp > 1557651600000` | Abfragen für alle verbundenen Geräte mit einem Verbindungszeitstempel > 1557651600000. Zeitstempel werden in Millisekunden seit der Epoche angegeben. |
| `connectivity.connected:*` | Abfragen für alle Geräte mit vorhandenen Verbindungsinformationen. |
| `connectivity.disconnectReason:*` | Abfragen für alle Geräte mit disconnectReason vorhandener Konnektivität. |

| Abfragezeichenfolge | Ergebnis |
| --- | --- |
| `connectivity.disconnectReason:CLIENT_INITIATED_DISCONNECT` | Abfragen für alle Geräte, die aufgrund von CLIENT _ INITIATED _ DISCONNECT getrennt wurden. |
| `deviceDefender.violationCount:[0 TO 100]` | Abfragen nach Objekten, bei denen Device Defender einen Zählwert verletzt, der innerhalb des numerischen Bereichs (0-100, einschließlich) liegt. |
| `deviceDefender.<device-SecurityProfile>.disconnectBehavior.inViolation:true` | Abfragen nach Objekten, die gegen das im Sicherheitsprofil `device-SecurityProfile` definierte Verhalten `disconnectBehavior` verstoßen. Beachten Sie, dass:false keine inViolationgültige Abfrage ist. |
| `deviceDefender.<device-SecurityProfile>.disconnectBehavior.lastViolationValue.number>2` | Abfragen nach Dingen, die gegen das im Sicherheitsprofil des Geräts definierte Verhalten `disconnectBehavior` verstoßen, SecurityProfile wobei der Wert für das letzte Verletzungsereignis größer als 2 ist. |
| `deviceDefender.<device-SecurityProfile>.disconnectBehavior.lastViolationTime>1634227200000` | Abfragen nach Dingen, die gegen das im Sicherheitsprofilgerät definierte Verhalten `disconnectBehavior` verstoßen, SecurityProfile wobei der letzte Verstoß erst nach einer bestimmten Epoche aufgetreten ist. |
| `shadow.name.gps-tracker.reported.coordinates:geo_distance,47.6204,-122.3491,15.5km` | Abfragen nach Objekten, die sich innerhalb einer radialen Entfernung von 15,5 km von den Koordinaten 47.6204, -122.3491 befinden. Diese Abfragezeichenfolge gilt für den Fall, dass Ihre Standortdaten in einem benannten Schatten gespeichert werden. |
| `shadow.reported.coordinates:geo_distance,47.6204,-122.3491,15.5km` | Abfragen für Objekte, die sich innerhalb einer radialen Entfernung von 15,5 km von den Koordinaten 47,6204, -122,3491 befinden. Diese Abfragezeichenfolge gilt für den Fall, dass Ihre Standortdaten in einem klassischen Schatten gespeichert werden. |

# Beispiel für Objektgruppenabfragen

Abfragen werden mithilfe einer Abfragesyntax in einer Abfragezeichenfolge angegeben und an die `SearchIndex`APIübergeben. Die folgende Tabelle enthält einige Beispiele für Abfragezeichenfolgen.

| Abfragezeichenfolge | Ergebnis |
| --- | --- |
| `abc` | Abfragen von "abc" in einem beliebigen Feld. |
| `thingGroupName:myGroupThingName` | Abfragen für eine Dinggruppe mit dem Namen "myGroupThingName“. |
| `thingGroupName:my*` | Abfragen von Objektgruppen mit Namen, die mit "my" beginnen. |
| `thingGroupName:ab?` | Abfragen von Objektgruppen mit Namen, die "ab" sowie ein zusätzliches Zeichen enthalten, zum Beispiel: "aba", "abb", "abc" usw. |
| `attributes.myAttribute:75` | Abfragen nach Dinggruppen mit einem Attribut namens "myAttribute", das den Wert 75 hat. |
| `attributes.myAttribute:[75 TO 80]` | Abfragen nach Dinggruppen mit einem Attribut namens "myAttribute", dessen Wert in einen numerischen Bereich (75—80, einschließlich) fällt. |
| `attributes.myAttribute:[75 TO 80]` | Abfragen nach Dinggruppen mit einem Attribut namens "myAttribute", dessen Wert in den numerischen Bereich (>75 und <=80) fällt. |
| `attributes.myAttribute:["abcd" TO "abcf"]` | Abfragen nach Dinggruppen mit einem Attribut namens "myAttribute", dessen Wert innerhalb eines alphanumerischen Zeichenkettenbereichs liegt. Diese Abfrage gibt Dinggruppen mit einem Attribut "serialNumber" mit den Werten „abcd“, „abce“ oder „abcf“ zurück. |
| `attributes.myAttribute:i*t` | Abfragen nach Dinggruppen mit einem Attribut namens "myAttribute", dessen Wert 'i' ist, gefolgt von einer beliebigen Anzahl von Zeichen, gefolgt von 't' |

| Abfragezeichenfolge | Ergebnis |
| --- | --- |
| `attributes.attr1:abc AND attributes.attr2<5 NOT attributes.attr3>10` | Abfragen für Objektgruppen, mit booleschen Ausdrücken Begriffe kombinieren. Diese Abfrage gibt Objektgruppen zurück, die ein Attribut mit dem Namen "attr1" mit dem Wert "abc", ein Attribut mit dem Namen "attr2", das kleiner als 5 ist, und ein Attribut mit dem Namen "attr3", das nicht größer als 10 ist, aufweisen. |
| `NOT attributes.myAttribute:cde` | Abfragen für Dinggruppen, bei denen das Attribut mit dem Namen "myAttribute" nicht „cde“ ist. |
| `parentGroupNames:(myParentThingGroupName)` | Abfragen für Dinggruppen, deren übergeordneter Gruppenname mit "myParentThingGroupName" übereinstimmt. |
| `parentGroupNames:(myParentThingGroupName OR myRootThingGroupName)` | Abfragen für Dinggruppen, deren übergeordneter Gruppenname mit "myParentThingGroupName" oder "myRootThingGroupName" übereinstimmt. |
| `parentGroupNames:(myParentThingGroupNa*)` | Abfragen für Dinggruppen, deren übergeordneter Gruppenname mit "myParentThingGroupNa" beginnt. |

# Indexierung von Standortdaten

Sie können die AWS IoT Flottenindizierung verwenden, um die zuletzt gesendeten Standortdaten Ihrer Geräte zu indizieren und mithilfe von Geoabfragen nach Geräten zu suchen. Diese Funktion löst Anwendungsfälle für die Geräteüberwachung und -verwaltung wie Standortverfolgung und Näherungssuche. Die Standortindizierung funktioniert ähnlich wie andere Funktionen zur Flottenindizierung, allerObjekts mit zusätzlichen Konfigurationen, die Sie bei der Indexierung Ihres Objekts angeben müssen.

Zu den häufigsten Anwendungsfällen gehören: Suchen und Aggregieren von Geräten, die sich innerhalb der gewünschten geografischen Grenzen befinden, Abrufen von standortspezifischen Erkenntnissen mithilfe von Abfragebegriffen in Bezug auf Gerätemetadaten und Status aus indizierten Datenquellen, Bereitstellung einer detaillierten Ansicht, z. B. das Filtern von Ergebnissen nach einem bestimmten geografischen Gebiet, um Rendering-Verzögerungen innerhalb Ihrer

Flottenüberwachungskarten zu reduzieren und den zuletzt gemeldeten Gerätestandort zu verfolgen und Geräte zu identifizieren, die sich außerhalb der gewünschten Grenzwerte befinden, und anhand von Flottenmetriken Alarme zu generieren. Erste Schritte mit der Standortindizierung und Geoabfragen finden Sie unter ???.

## Unterstützte Datumsformate

AWS IoT Die Flottenindizierung unterstützt die folgenden Standortdatenformate:

1. Bekannte Textdarstellung von Koordinatenreferenzsystemen

   Eine Zeichenfolge, die dem Format Geographische Information — Bekannte Textdarstellung von Koordinatenreferenzsystemen folgt. Ein Beispiel kann sein`"POINT(long lat)"`.
2. Eine Zeichenfolge, die die Koordinaten darstellt

   Eine Zeichenfolge im Format `"latitude, longitude"` oder `"longitude, latitude"`. Wenn Sie `"longitude, latitude"` angeben, müssen Sie auch `order` in `geoLocations` angeben. Ein Beispiel kann sein `"41.12,-71.34"`.
3. Ein Objekt mit den Tasten Lat (Breitengrad) und Lon (Längengrad)

   Dieses Format gilt für klassischen Schatten und benannten Schatten. Unterstützte Schlüssel: `lat`, `latitude`, `lon`, `long`, `longitude`. Ein Beispiel kann `{"lat": 41.12, "lon": -71.34}` sein.
4. Ein Array, das die Koordinaten darstellt

   Ein Array mit dem Format `[lat,lon]` oder `[lon,lat]`. Wenn Sie das Format verwenden`[lon,lat]`, das den Koordinaten in Geo entspricht JSON (gilt für klassischen Schatten und benannten Schatten), müssen Sie auch `order` in `geoLocations` angeben.

   Ein Beispiel kann sein:

```
{
  "location": {
    "coordinates": [
      **Longitude**,
      **Latitude**
    ],
    "type": "Point",
    "properties": {
      "country": "United States",
```

```
      "city": "New York",
      "postalCode": "*****",
      "horizontalAccuracy": 20,
      "horizontalConfidenceLevel": 0.67,
      "state": "New York",
      "timestamp": "2023-01-04T20:59:13.024Z"
    }
  }
}
```

## Wie indexiert man Standortdaten

Die folgenden Schritte zeigen, wie Sie die Indexierungskonfiguration für Ihre Standortdaten aktualisieren und Geoabfragen verwenden, um nach Geräten zu suchen.

1. Erfahren Sie, wo Ihre Standortdaten gespeichert sind

   Die Flottenindizierung unterstützt derzeit die Indizierung von Standortdaten, die in klassischen Schatten oder benannten Schatten gespeichert sind.

2. Verwenden Sie unterstützte Standortdatenformate

   Stellen Sie sicher, dass Ihr Standortdatenformat einem der unterstützten Datenformate entspricht.

3. Aktualisieren Sie die Indexkonfiguration

   Aktivieren Sie mindestens die Konfiguration für die Indizierung von Objekten (Registrierung). Sie müssen auch die Indizierung für klassische Schatten oder Named Schatten aktivieren, die Ihre Standortdaten enthalten. Wenn Sie Ihre Objekt-Indizierung aktualisieren, sollten Sie Ihre Standortdaten in die Indexierungskonfiguration einbeziehen.

4. Erstellen und Ausführen von -Abfragen

   Erstellen Sie je nach Ihren Anwendungsfällen Geoabfragen und führen Sie sie aus, um nach Geräten zu suchen. Die Geoabfrage, die Sie erstellen, muss der Abfragesyntax entsprechen. Sie finden einige Beispiele in ???.

# Konfiguration der Objektindizierung.

Um Standortdaten zu indizieren, müssen Sie die Indexkonfiguration aktualisieren und Ihre Standortdaten einbeziehen. Gehen Sie je nachdem, wo Ihre Standortdaten gespeichert sind, wie folgt vor, um Ihre Indexierungskonfiguration zu aktualisieren:

Standortdaten, die in klassischen Schatten gespeichert werden

Wenn Ihre Standortdaten in einem klassischen Shadow gespeichert sind, müssen Sie `thingIndexingMode` auf `REGISTRY_AND_SHADOW` einstellen und Ihre Standortdaten in den `geoLocations`-Feldern (`name`und`order`) unter `filter` angeben.

Im folgenden Konfigurationsbeispiel für die Indizierung geben Sie den Standortdatenpfad `shadow.reported.coordinates` als `name` und `LonLat` als `order` an.

```
{
 "thingIndexingMode": "REGISTRY_AND_SHADOW",
 "filter": {
  "geoLocations": [
   {
    "name": "shadow.reported.coordinates",
    "order": "LonLat"
   }
  ]
 }
}
```

- `thingIndexingMode`

  Der Indizierungsmodus steuert, ob Registry oder Shadow indexiert wird. Wenn `thingIndexingMode` auf `OFF` eingestellt ist, ist die Indizierung von Objekten deaktiviert.

  Um Standortdaten zu indizieren, die in einem klassischen Schatten gespeichert sind, müssen Sie `thingIndexingMode` den Wert auf `REGISTRY_AND_SHADOW` einstellen. Weitere Informationen finden Sie unter ???.
- `filter`

  Der Indexfilter bietet zusätzliche Auswahlmöglichkeiten für benannte Schatten und Geolokalisierungsdaten. Weitere Informationen finden Sie unter ???.
- `geoLocations`

Die Liste der Geolocation-Ziele, die Sie für die Indizierung auswählen. Die Standardanzahl von Geolocation-Zielen für die Indizierung ist 1. Informationen zum Erhöhen von Limits finden Sie unter AWS IoT Device Management Kotingente.

- `name`

  Der Name des Geolocation-Zielfelds. Ein Beispielwert von `name` kann der Standortdatenpfad Ihres Schattens sein:`shadow.reported.coordinates`.

- `order`

  Die Reihenfolge des Geolocation-Zielfeldes. Gültige Werte: `LatLon` und `LonLat`. `LatLon` bedeutet Breitengrad und Längengrad. `LonLat` bedeutet Längengrad und Breitengrad. Dies ist ein optionales Feld. Der Standardwert ist `LatLon`.

Standortdaten, die in benannten Schatten gespeichert sind

Wenn Ihre Standortdaten in einem benannten Schatten gespeichert sind, setzen Sie `namedShadowIndexingMode` auf den Wert `ON`, fügen Sie Ihre (n) benannten Schattennamen zum `namedShadowNames`-Feld in `filter`hinzu und geben Sie Ihren Standortdatenpfad im `geoLocations` Feld in `filter` an.

Im folgenden Konfigurationsbeispiel für die Indizierung geben Sie den Standortdatenpfad `shadow.name.namedShadow1.reported.coordinates` als `name` und `LonLat` als `order` an.

```
{
 "thingIndexingMode": "REGISTRY",
 "namedShadowIndexingMode": "ON",
 "filter": {
  "namedShadowNames": [
   "namedShadow1"
  ],
  "geoLocations": [
   {
    "name": "shadow.name.namedShadow1.reported.coordinates",
    "order": "LonLat"
   }
  ]
 }
}
```

- `thingIndexingMode`

  Der Indizierungsmodus steuert, ob Registry oder Shadow indexiert wird. Wenn `thingIndexingMode` auf `OFF` eingestellt ist, ist die Indizierung von Objekten deaktiviert.

  Um Standortdaten, die in einem benannten Schatten gespeichert sind, zu indizieren, müssen Sie `thingIndexingMode` den Wert auf `REGISTRY` (oder `REGISTRY_AND_SHADOW`) setzen. Weitere Informationen finden Sie unter ???.

- `filter`

  Der Indexfilter bietet zusätzliche Auswahlmöglichkeiten für benannte Schatten und Geolokalisierungsdaten. Weitere Informationen finden Sie unter ???.

- `geoLocations`

  Die Liste der Geolocation-Ziele, die Sie für die Indizierung auswählen. Die Standardanzahl von Geolocation-Zielen für die Indizierung ist 1. Informationen zum Erhöhen von Limits finden Sie unter AWS IoT Device Management Kotingente.

- `name`

  Der Name des Geolocation-Zielfelds. Ein Beispielwert von `name` kann der Standortdatenpfad Ihres Schattens sein:`shadow.name.namedShadow1.reported.coordinates`.

- `order`

  Die Reihenfolge des Geolocation-Zielfeldes. Gültige Werte: `LatLon` und `LonLat`. `LatLon` bedeutet Breitengrad und Längengrad. `LonLat` bedeutet Längengrad und Breitengrad. Dies ist ein optionales Feld. Der Standardwert ist `LatLon`.

## Beispiele für Geoqueries

Nachdem Sie die Indizierungskonfiguration für Ihre Standortdaten abgeschlossen haben, führen Sie Geoqueries aus, um nach Geräten zu suchen. Sie können Ihre Geoqueries auch mit anderen Abfragezeichenfolgen kombinieren. Weitere Informationen erhalten Sie unter ??? und ???.

Beispiel: Abfrage

In diesem Beispiel wird davon ausgegangen, dass die Standortdaten in einem benannten Schatten `gps-tracker` gespeichert sind. Die Ausgabe dieses Befehls ist die Liste der Geräte, die sich

innerhalb einer radialen Entfernung von 15,5 km vom Mittelpunkt befinden, mit Koordinaten (47.6204, -122.3491).

```
aws iot search-index --query-string \
"shadow.name.gps-tracker.reported.coordinates:geo_distance,47.6204,-122.3491,15.5km"
```

Beispiel: Abfrage

In diesem Beispiel wird davon ausgegangen, dass die Standortdaten in einem klassischen Schatten gespeichert sind. Die Ausgabe dieses Befehls ist die Liste der Geräte, die sich innerhalb einer radialen Entfernung von 15,5 km vom Mittelpunkt befinden, mit Koordinaten (47.6204, -122.3491).

```
aws iot search-index --query-string \
"shadow.reported.coordinates:geo_distance,47.6204,-122.3491,15.5km"
```

Beispiel: Abfrage

In diesem Beispiel wird davon ausgegangen, dass die Standortdaten in einem klassischen Schatten gespeichert sind. Die Ausgabe dieses Befehls ist die Liste der Geräte, die nicht angeschlossen sind und sich außerhalb der radialen Entfernung von 15,5 km vom Mittelpunkt befinden, mit Koordinaten (47.6204, -122.3491).

```
aws iot search-index --query-string \
"connectivity.connected:false AND (NOT
 shadow.reported.coordinates:geo_distance,47.6204,-122.3491,15.5km)"
```

## Erste Schritte-Tutorial

In diesem Tutorial wird gezeigt, wie Sie mithilfe der Flottenindizierung Ihre Standortdaten indexieren können. Der Einfachheit halber erstellen Sie ein Objekt, das Ihr Gerät darstellt, und speichern die Standortdaten in einem benannten Schatten, aktualisieren die Konfiguration der Objektindizierung für die Standortindizierung und führen Beispiel-Geoabfragen aus, um nach Geräten innerhalb einer radialen Grenze zu suchen.

Für dieses Tutorial brauchen Sie ungefähr 20 Minuten.

In diesem Thema:

- Voraussetzungen

- Objekte und Schatten erstellen
- Konfiguration der Objektindizierung.
- Ausführen von Geoquery

## Voraussetzungen

- Installieren der neuesten Version von AWS CLI
- Machen Sie sich mit der Standortindizierung und Geoabfragen, der Verwaltung der Objektindizierung und der Abfragesyntax vertraut.

## Objekte und Schatten erstellen

Sie erstellen ein Objekt, das Ihr Gerät repräsentiert, und einen benannten Schatten, um dessen Standortdaten zu speichern (Koordinaten 47.61564, -122.33584).

1. Führen Sie den folgenden Befehl aus, um Ihr Ding zu erstellen, das Ihr Fahrrad mit dem Namen Bike-1 repräsentiert. Weitere Informationen zum Erstellen eines Dings mit AWS CLI finden Sie unter Create-thing from AWS CLIReference.

   ```
   aws iot create-thing --thing-name "Bike-1" \
   --attribute-payload '{"attributes": {"model":"OEM-2302-12", "battery":"35",
    "acqDate":"06/09/23"}}'
   ```

   Die Ausgabe dieses Befehls kann folgendermaßen aussehen:

   ```
   {
       "thingName": "Bike-1",
       "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/Bike-1",
       "thingId": "df9cf01d-b0c8-48fe-a2e2-e16cff6b23df"
   }
   ```

2. Führen Sie den folgenden Befehl aus, um einen benannten Schatten zum Speichern der Standortdaten von Bike-1 (Koordinaten 47.61564, -122.33584) zu erstellen. Weitere Informationen zum Erstellen eines benannten Schattens mithilfe update-thing-shadowvon AWS CLIfinden Sie in AWS CLI Reference.

   ```
   aws iot-data update-thing-shadow \
   --thing-name Bike-1 \
   ```

```
--shadow-name Bike1-shadow \
--cli-binary-format raw-in-base64-out \
--payload '{"state":{"reported":{"coordinates":{"lat": 47.6153, "lon": -122.3333}}}}'
 \
"output.txt" \
```

Dieser Befehl liefert keine Ausgabe. Um den von Ihnen erstellten benannten Schatten anzuzeigen, können Sie den CLI Befehl list-named-shadows-for-thing ausführen.

```
aws iot-data list-named-shadows-for-thing --thing-name Bike-1
```

Die Ausgabe dieses Befehls sieht wie folgt aus:

```
{
    "results": [
        "Bike1-shadow"
    ],
    "timestamp": 1699574309
}
```

## Konfiguration der Objektindizierung.

Um Ihre Standortdaten zu indizieren, müssen Sie Ihre Objekt-Indizierungskonfiguration so aktualisieren, dass sie die Standortdaten einbezieht. Da Ihre Standortdaten in diesem Tutorial in einem benannten Schatten gespeichert werden, setzen Sie `thingIndexingMode` auf `REGISTRY` (bei einer Mindestanforderung), setzen Sie `namedShadowIndexingMode` auf `ON` und fügen Sie Ihre Standortdaten zur Konfiguration hinzu. In diesem Beispiel müssen Sie den Namen Ihres benannten Schattens und den Pfad für die Standortdaten des Schattens zu `filter` hinzufügen.

1. Führen Sie den Befehl aus, um Ihre Indizierungskonfiguration für die Standortindizierung zu aktualisieren.

```
aws iot update-indexing-configuration --cli-input-json '{
"thingIndexingConfiguration": { "thingIndexingMode": "REGISTRY",
"thingConnectivityIndexingMode": "OFF",
"deviceDefenderIndexingMode": "OFF",
"namedShadowIndexingMode": "ON",
"filter": {
    "namedShadowNames": ["Bike1-shadow"],
```

```
    "geoLocations":[{
        "name":"shadow.name.Bike1-shadow.reported.coordinates"
    }]
},
"customFields": [
{ "name":"attributes.battery",
"type":"Number"}] } }'
```

Der Befehl erzeugt keine Ausgabe. Möglicherweise müssen Sie einen Moment warten, bis das Update abgeschlossen ist. Um den Status zu überprüfen, führen Sie den Befehl describe-index CLI aus. Wenn `indexStatus` Folgendes anzeigt:`ACTIVE`, ist das Indizierungsupdate Ihres Objekts abgeschlossen.

2. Führen Sie den Befehl aus, um Ihre Konfiguration zu überprüfen. Dieser Schritt ist optional.

```
aws iot get-indexing-configuration
```

Die Ausgabe sieht wie folgt aus:

```
{
    "thingIndexingConfiguration": {
        "thingIndexingMode": "REGISTRY",
        "thingConnectivityIndexingMode": "OFF",
        "deviceDefenderIndexingMode": "OFF",
        "namedShadowIndexingMode": "ON",
        "managedFields": [
            {
                "name": "shadow.name.*.hasDelta",
                "type": "Boolean"
            },
            {
                "name": "registry.version",
                "type": "Number"
            },
            {
                "name": "registry.thingTypeName",
                "type": "String"
            },
            {
                "name": "registry.thingGroupNames",
                "type": "String"
            },
```

```
            {
                "name": "shadow.name.*.version",
                "type": "Number"
            },
            {
                "name": "thingName",
                "type": "String"
            },
            {
                "name": "thingId",
                "type": "String"
            }
        ],
        "customFields": [
            {
                "name": "attributes.battery",
                "type": "Number"
            }
        ],
        "filter": {
            "namedShadowNames": [
                "Bike1-shadow"
            ],
            "geoLocations": [
                {
                    "name": "shadow.name.Bike1-shadow.reported.coordinates",
                    "order": "LatLon"
                }
            ]
        }
    },
    "thingGroupIndexingConfiguration": {
        "thingGroupIndexingMode": "OFF"
    }
}
```

## Ausführen von Geoquery

Jetzt haben Sie Ihre Objekt-Indizierungskonfiguration aktualisiert, sodass sie die Standortdaten enthält. Versuchen Sie, einige Geoqueries zu erstellen und sie auszuführen, um zu sehen, ob Sie die gewünschten Suchergebnisse erhalten können. Eine Geoabfrage muss der Abfragesyntax folgen. Einige nützliche Beispiel-Geoabfragen finden Sie unter ???.

Im folgenden Beispielbefehl verwenden Sie die Geoabfrage, `shadow.name.Bike1-shadow.reported.coordinates:geo_distance,47.6204,-122.3491,15.5km` um mit Koordinaten (47.6204, -122.3491) nach Geräten zu suchen, die sich innerhalb einer radialen Entfernung von 15,5 km vom Mittelpunkt befinden.

```
aws iot search-index --query-string "shadow.name.Bike1-
shadow.reported.coordinates:geo_distance,47.6204,-122.3491,15.5km"
```

Da Sie ein Gerät an den Koordinaten „lat“: 47.6153, „lon“: -122.3333 haben, das innerhalb einer Entfernung von 15,5 km vom Mittelpunkt liegt, sollten Sie dieses Gerät (Bike-1) in der Ausgabe sehen können. Die Ausgabe sieht wie folgt aus:

```
{
    "things": [
        {
            "thingName": "Bike-1",
            "thingId": "df9cf01d-b0c8-48fe-a2e2-e16cff6b23df",
            "attributes": {
                "acqDate": "06/09/23",
                "battery": "35",
                "model": "OEM-2302-12"
            },
            "shadow": "{\"reported\":{\"coordinates\":{\"lat\":47.6153,\"lon
\":-122.3333}},\"metadata\":{\"reported\":{\"coordinates\":{\"lat\":{\"timestamp
\":1699572906},\"lon\":{\"timestamp\":1699572906}}}},\"hasDelta\":false,\"version\":1}"
        }
    ]
}
```

Weitere Informationen finden Sie unter ???.

# Flottenmetriken

Flottenmetriken sind ein Feature der Flottenindizierung, einem verwalteten Service, mit dem Sie die Daten Ihrer Geräte in indizieren, durchsuchen und aggregieren können AWS IoT. Sie können Flottenmetriken verwenden, um den Aggregatstatus Ihrer Flottengeräte im CloudWatch Laufe der Zeit zu überwachen, einschließlich der Überprüfung der Verbindungstrennungsrate Ihrer Flottengeräte oder der durchschnittlichen Änderungen des Batteriestands eines bestimmten Zeitraums.

Mithilfe von Flottenmetriken können Sie Aggregationsabfragen erstellen, deren Ergebnisse kontinuierlich CloudWatch als Metriken für die Analyse von Trends und die Erstellung von Alarmen an ausgegeben werden. Für Ihre Überwachungsaufgaben können Sie die Aggregationsabfragen verschiedener Aggregationstypen (Statistik, Kardinalität und Perzentil) angeben. Sie können all Ihre Aggregationsabfragen speichern, um Flottenmetriken für die zukünftige Wiederverwendung zu erstellen.

## Erste Schritte-Tutorial

In diesem Tutorial erstellen Sie eine Flottenmetrik, um die Temperaturen Ihrer Sensoren zu überwachen und potenzielle Anomalien zu erkennen. Bei der Erstellung der Flottenmetrik definieren Sie eine Aggregationsabfrage, die die Anzahl der Sensoren mit Temperaturen über ca. 80 Grad Fahrenheit erkennt. Sie geben an, dass die Abfrage alle 60 Sekunden ausgeführt werden soll, und die Abfrageergebnisse werden an ausgegeben CloudWatch, wo Sie die Anzahl der Sensoren mit potenziellen Hochalarmrisiken anzeigen und Alarme festlegen können. Zum Abschließen dieses Tutorials wird die AWS CLI verwendet.

In diesem Tutorial lernen Sie Folgendes:

- Einrichten
- Erstellen einer Flottenmetrik
- Anzeigen von Metriken in CloudWatch
- Bereinigen von Ressourcen

Für dieses Tutorial brauchen Sie ungefähr 15 Minuten.

### Voraussetzungen

- Installieren der neuesten Version von AWS CLI
- Vertrautmachen mit Abfragen von Aggregatdaten
- Machen Sie sich mit der Verwendung von Amazon CloudWatch-Metriken vertraut

### Einrichten

Um Flottenmetriken zu verwenden, aktivieren Sie die Flottenindizierung. Um die Flottenindizierung für Ihre Objekte oder Objektgruppen mit bestimmten Datenquellen und zugehörigen Konfigurationen zu

aktivieren, folgen Sie den Anweisungen unter Verwaltung der Objektindizierung und Verwalten der Objektgruppenindizierung.

So führen Sie die Einrichtung durch:

1. Führen Sie den folgenden Befehl aus, um die Flottenindizierung zu aktivieren, und geben Sie die Datenquellen an, in denen gesucht werden soll.

```
aws iot update-indexing-configuration \
--thing-indexing-configuration
 "thingIndexingMode=REGISTRY_AND_SHADOW,customFields=[{name=attributes.temperature,type=Num
{name=attributes.rackId,type=String},
{name=attributes.stateNormal,type=Boolean}],thingConnectivityIndexingMode=STATUS" \
```

   Der obenstehende CLI-Beispielbefehl ermöglicht die Flottenindizierung, um die Suche nach Registrierungsdaten, Schattendaten und dem Status der Objektkonnektivität mithilfe des `AWS_Things`-Index zu unterstützen.

   Die Änderung der Konfiguration kann einige Minuten in Anspruch nehmen. Stellen Sie sicher, dass Ihre Flottenindizierung aktiviert ist, bevor Sie Flottenmetriken erstellen.

   Führen Sie zum Überprüfen, ob Ihre Flottenindizierung aktiviert wurde, den folgenden CLI-Befehl aus:

```
aws --region us-east-1 iot describe-index --index-name "AWS_Things"
```

   Weitere Informationen finden Sie unter Aktivieren der Objektindizierung.

2. Führen Sie das folgende Bash-Skript aus, um zehn Objekte zu erstellen und zu beschreiben.

```
# Bash script. Type `bash` before running in other shells.

Temperatures=(70 71 72 73 74 75 47 97 98 99)
Racks=(Rack1 Rack1 Rack2 Rack2 Rack3 Rack4 Rack5 Rack6 Rack6 Rack6)
IsNormal=(true true true true true true false false false false)

for ((i=0; i < 10; i++))
do
  thing=$(aws iot create-thing --thing-name "TempSensor$i" --attribute-
payload attributes="{temperature=${Temperatures[@]:$i:1},rackId=${Racks[@]:
$i:1},stateNormal=${IsNormal[@]:$i:1}}")
```

```
  aws iot describe-thing --thing-name "TempSensor$i"
done
```

Dieses Skript erstellt zehn Objekte, die zehn Sensoren repräsentieren. Jedes Objekt hat die Attribute `temperature`, `rackId` und `stateNormal`, wie in der folgenden Tabelle beschrieben:

| Attribut | Datentyp | Beschreibung |
| --- | --- | --- |
| `temperature` | Zahl | Temperaturwert in Fahrenheit |
| `rackId` | String | ID des Server-Racks, das Sensoren enthält |
| `stateNormal` | Boolesch | Ob der Temperaturwert des Sensors normal ist oder nicht |

Die Ausgabe dieses Skripts enthält zehn JSON-Dateien. Eine der JSON-Dateien sieht wie folgt aus:

```
{
    "version": 1,
    "thingName": "TempSensor0",
    "defaultClientId": "TempSensor0",
    "attributes": {
        "rackId": "Rack1",
        "stateNormal": "true",
        "temperature": "70"
    },
    "thingArn": "arn:aws:iot:region:account:thing/TempSensor0",
    "thingId": "example-thing-id"
}
```

Weitere Informationen finden Sie unter Ein Objekt erstellen.

## Erstellen einer Flottenmetrik

So erstellen Sie eine Flottenmetrik:

1. Führen Sie den folgenden Befehl aus, um eine Flottenmetrik mit dem Namen *high_temp_FM* zu erstellen. Sie erstellen die Flottenmetrik, um die Anzahl der Sensoren zu überwachen, deren Temperatur 80 Grad Fahrenheit in überschreitet CloudWatch.

   ```
   aws iot create-fleet-metric --metric-name "high_temp_FM" --query-string
    "thingName:TempSensor* AND attributes.temperature >80" --period 60 --aggregation-
   field "attributes.temperature" --aggregation-type name=Statistics,values=count
   ```

   --metric-name

   Datentyp: Zeichenfolge. Der Parameter `--metric-name` gibt den Namen einer Flottenmetrik an. In diesem Beispiel erstellen Sie eine Flottenmetrik mit dem Namen high_temp_FM.

   --query-string

   Datentyp: Zeichenfolge. Der Parameter `--query-string` gibt die Abfragezeichenfolge an. In diesem Beispiel bedeutet die Abfragezeichenfolge, dass alle Objekte mit Namen abgefragt werden sollen, die mit TempSensor und mit Temperatur über 80 Grad Fahrenheit beginnen. Weitere Informationen finden Sie unter Abfragesyntax.

   --period

   Datentyp: Ganzzahl. Der Parameter `--period` gibt die Zeit in Sekunden für die Abfrage der aggregierten Daten an. In diesem Beispiel geben Sie an, dass die Flottenmetrik, die Sie erstellen, die aggregierten Daten alle 60 Sekunden abruft.

   --aggregation-field

   Datentyp: Zeichenfolge. Der Parameter `--aggregation-field` gibt das auszuwertende Attribut an. In diesem Beispiel soll das Temperaturattribut ausgewertet werden.

   --aggregation-type

   Der Parameter`--aggregation-type` gibt die statistische Zusammenfassung an, die in der Flottenmetrik angezeigt werden soll. Für Ihre Überwachungsaufgaben können Sie die Eigenschaften von Aggregationsabfragen für die verschiedenen Aggregationstypen

(Statistik, Kardinalität und Perzentil) anpassen. In diesem Beispiel geben Sie Anzahl für den Aggregationstyp und Statistik an, um die Anzahl der Geräte zurückzugeben, deren Attribute mit der Abfrage übereinstimmen, d. h. um die Anzahl der Geräte zurückzugeben, deren Namen mit beginnen TempSensor und deren Temperatur über 80 Grad Fahrenheit liegt. Weitere Informationen finden Sie unter Abfragen von Aggregatdaten.

Die Ausgabe dieses Befehls sieht wie folgt aus:

```
{
    "metricArn": "arn:aws:iot:region:111122223333:fleetmetric/high_temp_FM",
    "metricName": "high_temp_FM"
}
```

> **Note**
>
> Es kann einen Moment dauern, bis die Datenpunkte in angezeigt werden CloudWatch.

Weitere Informationen zum Erstellen einer Flottenmetrik finden Sie unter Verwalten von Flottenmetriken.

Wenn Sie keine Flottenmetrik erstellen können, lesen Sie den Artikel Problembehebung bei Flottenmetriken.

2. (Optional) Führen Sie den folgenden Befehl aus, um Ihre Flottenmetrik mit dem Namen high_temp_FM zu beschreiben.

```
aws iot describe-fleet-metric --metric-name "high_temp_FM"
```

Die Ausgabe dieses Befehls sieht wie folgt aus:

```
{
    "queryVersion": "2017-09-30",
    "lastModifiedDate": 1625249775.834,
    "queryString": "*",
    "period": 60,
    "metricArn": "arn:aws:iot:region:111122223333:fleetmetric/high_temp_FM",
    "aggregationField": "registry.version",
    "version": 1,
    "aggregationType": {
```

```
        "values": [
            "count"
        ],
        "name": "Statistics"
    },
    "indexName": "AWS_Things",
    "creationDate": 1625249775.834,
    "metricName": "high_temp_FM"
}
```

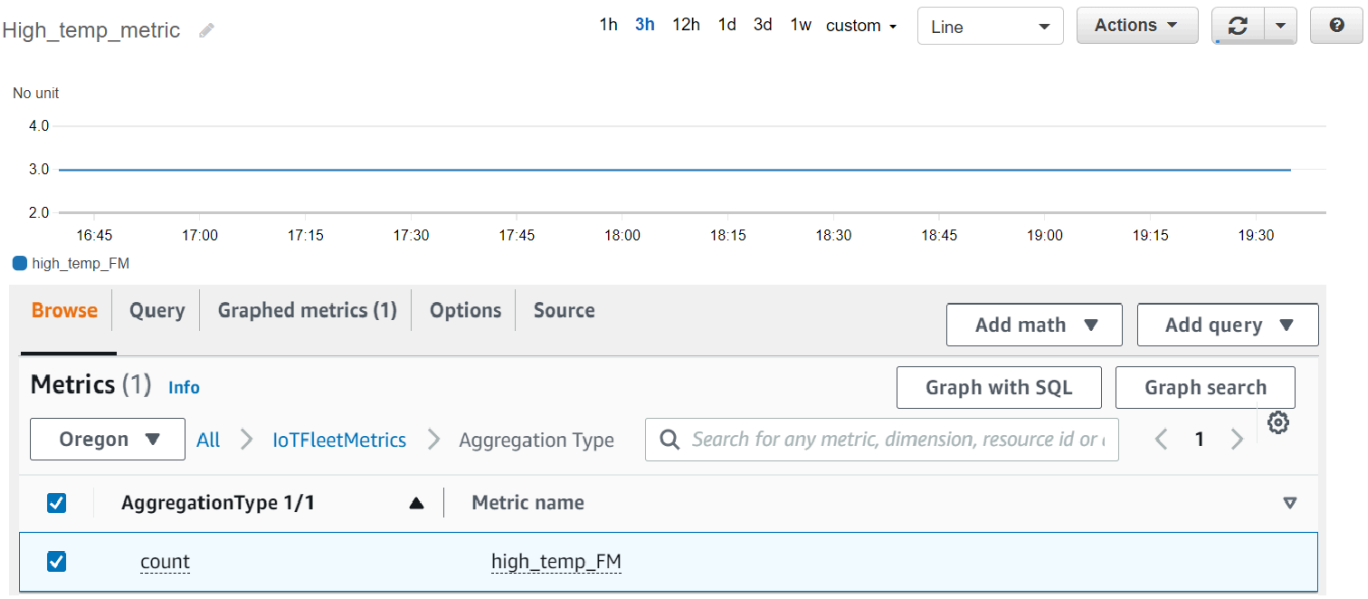
## Anzeigen von Flottenmetriken in CloudWatch

Nachdem Sie die Flottenmetrik erstellt haben, können Sie die Metrikdaten in anzeigen CloudWatch. In diesem Tutorial sehen Sie die -Metrik, die die Anzahl der Sensoren anzeigt, deren Namen mit beginnen TempSensor und deren Temperatur über 80 Grad Fahrenheit liegt.

So zeigen Sie Datenpunkte in an CloudWatch

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im CloudWatch Menü im linken Bereich Metriken aus, um das Untermenü zu erweitern, und wählen Sie dann Alle Metriken aus. Dadurch wird eine Seite geöffnet, bei der die obere Hälfte das Diagramm und die untere Hälfte vier Abschnitte mit Registerkarten enthält.
3. Der erste Abschnitt mit Registerkarten Alle Metriken listet alle Metriken auf, die Sie in Gruppen anzeigen können. Wählen Sie IoTFleetMetrics aus. Diese enthält all Ihre Flottenmetriken.
4. Wählen Sie auf der Registerkarte Alle Metriken im Abschnitt Aggregationstyp die Option Aggregationstyp aus, um alle von Ihnen erstellten Flottenmetriken anzuzeigen.
5. Wählen Sie links im Abschnitt Aggregationstyp die Flottenmetrik aus, für die das Diagramm angezeigt werden soll. Links neben Ihrem Metriknamen wird der Wert *Anzahl* angezeigt. Dies ist der Wert des Aggregationstyps, den Sie in diesem Tutorial im Abschnitt Erstellen einer Flottenmetrik angegeben haben.
6. Wählen Sie die zweite Registerkarte mit dem Namen Grafische Metriken rechts neben der Registerkarte Alle Metriken, um die Flottenmetrik anzuzeigen, die Sie im vorherigen Schritt ausgewählt haben.

   Sie sollten ein Diagramm sehen, das die Anzahl der Sensoren mit Temperaturen über 80 Grad Fahrenheit anzeigt, wie in diesem Beispiel:




> **Note**
>
> Das Period-Attribut in ist CloudWatch standardmäßig 5 Minuten. Dies ist das Zeitintervall zwischen Datenpunkten, die in angezeigt werden CloudWatch. Sie können die Einstellung für den Zeitraum je nach Bedarf ändern.

7. (Optional) Sie können einen metrischen Alarm einrichten.

   1. Wählen Sie im CloudWatch Menü im linken Bereich Alarme aus, um das Untermenü zu erweitern, und wählen Sie dann Alle Alarme aus.
   2. Wählen Sie auf der Seite Alarme in der oberen rechten Ecke die Option Alarm erstellen aus. Folgen Sie den Anweisungen zum Erstellen eines Alarms in der Konsole, um bei Bedarf einen Alarm zu erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon-CloudWatch Alarmen.

Weitere Informationen finden Sie unter Verwenden von Amazon- CloudWatch Metriken.

Wenn Sie keine Datenpunkte in sehen können CloudWatch, lesen Sie Fehlerbehebung bei Flottenmetriken.

## Bereinigen

So löschen Sie Flottenkennzahlen:

Verwenden Sie den delete-fleet-metric-CLI-Befehl, um Flottenmetriken zu löschen.

Führen Sie den folgenden Befehl aus, um die Flottenmetrik mit dem Namen high_temp_FM zu löschen.

```
aws iot delete-fleet-metric --metric-name "high_temp_FM"
```

So löschen Sie Objekte:

Mit dem CLI-Befehl delete-thing können Sie ein Objekt löschen.

Um die zehn Objekte zu löschen, die Sie erstellt haben, führen Sie das folgende Skript aus:

```
# Bash script. Type `bash` before running in other shells.

for ((i=0; i < 10; i++))
do
  thing=$(aws iot delete-thing --thing-name "TempSensor$i")
done
```

So bereinigen Sie Metriken in CloudWatch

CloudWatch unterstützt das Löschen von Metriken nicht. Metriken laufen je nach ihren Aufbewahrungplänen ab. Weitere Informationen finden Sie unter Verwenden von Amazon-CloudWatch Metriken.

## Verwalten von Flottenmetriken

In diesem Thema wird gezeigt, wie Sie die AWS IoT Konsole und verwenden AWS CLI , um Ihre Flottenmetriken zu verwalten.

Themen

- Verwalten von Flottenmetriken (Konsole)
- Verwalten von Flottenmetriken (CLI)
- Autorisieren des Taggings von IoT-Ressourcen

### Verwalten von Flottenmetriken (Konsole)

In den folgenden Abschnitten wird gezeigt, wie Sie die AWS IoT Konsole verwenden, um Ihre Flottenmetriken zu verwalten. Stellen Sie sicher, dass Sie die Flottenindizierung mit den zugehörigen Datenquellen und Konfigurationen aktiviert haben, bevor Sie Flottenmetriken erstellen.

### Aktivieren der Flottenindizierung

Wenn Sie die Flottenindizierung bereits aktiviert haben, überspringen Sie diesen Abschnitt.

Wenn Sie die Flottenindizierung nicht aktiviert haben, folgen Sie diesen Anweisungen.

1. Öffnen Sie Ihre - AWS IoT Konsole unter https://console.aws.amazon.com/iot/.
2. Wählen Sie im AWS IoT Menü Einstellungen aus.
3. Um die detaillierten Einstellungen einzusehen, scrollen Sie auf der Seite Einstellungen nach unten zum Abschnitt Flottenindizierung.
4. Um Ihre Einstellungen für die Flottenindizierung zu aktualisieren, wählen Sie rechts neben dem Abschnitt Flottenindizierung die Option Indizierung verwalten aus.
5. Aktualisieren Sie auf der Seite Einstellungen für die Flottenindizierung verwalten Ihre Einstellungen für die Flottenindizierung nach Ihren Anforderungen.
   - Konfiguration

     Um die Objektindizierung zu aktivieren, aktivieren Sie die Objektindizierung und wählen Sie dann die Datenquellen aus, für die Sie die Indizierung durchführen möchten.

     Um die Indizierung von Objektgruppen zu aktivieren, aktivieren Sie die Indexierung von Thing-Gruppen.
   - Benutzerdefinierte Felder für die Aggregation – optional

     Benutzerdefinierte Felder sind eine Liste von Paaren aus Feldnamen und Feldtypen.

     Um ein benutzerdefiniertes Feldpaar hinzuzufügen, wählen Sie Neues Feld hinzufügen. Geben Sie einen benutzerdefinierten Feldnamen ein, wie z. B. `attributes.temperature`, und wählen Sie dann einen Feldtyp aus dem Menü Feldtyp aus. Beachten Sie, dass ein benutzerdefinierter Feldname mit `attributes.` beginnt und als Attribut gespeichert wird, um Abfragen zur Aggregation von Objekten auszuführen.

     Um die Einstellung zu aktualisieren und zu speichern, wählen Sie Aktualisieren.

### Erstellen einer Flottenmetrik

1. Öffnen Sie Ihre - AWS IoT Konsole unter https://console.aws.amazon.com/iot/.
2. Wählen Sie im AWS IoT Menü Verwalten und dann Flottenmetriken aus.

3. Wählen Sie auf der Seite Flottenmetriken die Option Flottenmetrik erstellen aus und schließen Sie die Schritte zur Erstellung ab.
4. Konfigurieren Sie in Schritt 1 Flottenmetriken.
   - Geben Sie im Abschnitt Abfrage eine Abfragezeichenfolge ein, um die Objekte oder Objektgruppen anzugeben, für die Sie die Aggregatsuche durchführen möchten. Die Abfragezeichenfolge besteht aus einem Attribut und einem Wert. Wählen Sie unter Eigenschaften das gewünschte Attribut aus, oder geben Sie das Attribut in das Feld ein, falls es nicht in der Liste angezeigt wird. Geben Sie den Wert nach `:` ein. Ein Beispiel für eine Abfragezeichenfolge kann `thingName:TempSensor*` sein. Drücken Sie für jede eingegebene Abfragezeichenfolge die Eingabetaste auf Ihrer Tastatur. Wenn Sie mehrere Abfragezeichenfolgen eingeben, geben Sie deren Beziehung an, indem Sie und, oder und nicht oder oder nicht auswählen.
   - Wählen Sie in den Berichtseigenschaften Indexname, Aggregationstyp und Aggregationsfeld aus den jeweiligen Listen aus. Wählen Sie als Nächstes unter Daten auswählen die Daten aus, die Sie aggregieren möchten. Sie können dabei mehrere Datenwerte auswählen.
   - Wählen Sie Weiter aus.
5. Geben Sie in Schritt 2 die Eigenschaften der Flottenmetrik an.
   - Geben Sie im Feld Name der Flottenmetrik einen Namen für die Flottenmetrik ein, die Sie erstellen.
   - Geben Sie im Feld Beschreibung – optional eine Beschreibung für die Flottenmetrik ein, die Sie erstellen. Dies ist ein optionales Feld.
   - Geben Sie in die Felder Stunden und Minuten die Zeit ein (wie oft), zu der die Flottenmetrik Daten an ausgeben soll CloudWatch.
   - Wählen Sie Weiter aus.
6. Überprüfen und Erstellen Sie Ihre Metrik in Schritt 5.
   - Überprüfen Sie die Einstellungen aus Schritt 1 und Schritt 2. Zum Bearbeiten der Einstellungen wählen Sie Bearbeiten.
   - Wählen Sie Flottenmetrik erstellen aus.

Nach erfolgreicher Erstellung wird die Flottenmetrik auf der Seite Flottenmetrik aufgeführt.

Aktualisieren einer Flottenmetrik

1. Wählen Sie auf der Seite Flottenmetrik die Flottenmetrik aus, die Sie aktualisieren möchten.

2. Klicken Sie auf der Seite Details auf Bearbeiten. Dadurch werden die Schritte zur Erstellung geöffnet, in denen Sie Ihre Flottenmetrik in einem der drei Schritte aktualisieren können.
3. Nachdem Sie die Aktualisierung der Flottenmetrik abgeschlossen haben, wählen Sie Flottenmetrik aktualisieren aus.

Löschen einer Flottenmetrik

1. Wählen Sie auf der Seite Flottenmetrik die Flottenmetrik aus, die Sie löschen möchten.
2. Wählen Sie auf der nächsten Seite, auf der Details zu Ihrer Flottenmetrik angezeigt werden, Löschen aus.
3. Geben Sie im Dialogfeld den Namen Ihrer Flottenmetrik ein, um das Löschen zu bestätigen.
4. Wählen Sie Löschen aus. In diesem Schritt wird Ihre Flottenmetrik dauerhaft gelöscht.

## Verwalten von Flottenmetriken (CLI)

In den folgenden Abschnitten wird gezeigt, wie Sie AWS CLI Ihre Flottenmetriken mithilfe der verwalten. Stellen Sie sicher, dass Sie die Flottenindizierung mit den zugehörigen Datenquellen und Konfigurationen aktiviert haben, bevor Sie Flottenmetriken erstellen. Um die Flottenindizierung für Ihre Objekte oder Objektgruppen zu aktivieren, folgen Sie den Anweisungen unter Verwalten der Objektindizierung oder Verwalten der Objektgruppenindizierung.

Erstellen einer Flottenmetrik

Sie können den create-fleet-metric CLI-Befehl verwenden, um eine Flottenmetrik zu erstellen.

```
aws iot create-fleet-metric --metric-name "YourFleetMetricName" --query-string
 "*" --period 60 --aggregation-field "registry.version" --aggregation-type
 name=Statistics,values=sum
```

Die Ausgabe dieses Befehls enthält den Namen und den Amazon-Ressourcennamen (ARN) Ihrer Flottenmetrik. Die Ausgabe sollte wie folgt aussehen:

```
{
    "metricArn": "arn:aws:iot:us-east-1:111122223333:fleetmetric/YourFleetMetricName",
    "metricName": "YourFleetMetricName"
}
```

### Auflisten von Flottenmetriken

Sie können den list-fleet-metric CLI-Befehl verwenden, um alle Flottenmetriken in Ihrem Konto aufzulisten.

```
aws iot list-fleet-metrics
```

Die Ausgabe dieses Befehls enthält alle Flottenmetriken. Die Ausgabe sollte wie folgt aussehen:

```
{
    "fleetMetrics": [
        {
            "metricArn": "arn:aws:iot:us-east-1:111122223333:fleetmetric/
YourFleetMetric1",
            "metricName": "YourFleetMetric1"
        },
        {
            "metricArn": "arn:aws:iot:us-east-1:111122223333:fleetmetric/
YourFleetMetric2",
            "metricName": "YourFleetMetric2"
        }
    ]
}
```

### Beschreiben einer Flottenmetrik

Sie können den describe-fleet-metric CLI-Befehl verwenden, um detailliertere Informationen zu einer Flottenmetrik anzuzeigen.

```
aws iot describe-fleet-metric --metric-name "YourFleetMetricName"
```

Die Ausgabe des Befehls enthält detaillierte Informationen über die angegebene Flottenmetrik. Die Ausgabe sollte wie folgt aussehen:

```
{
    "queryVersion": "2017-09-30",
    "lastModifiedDate": 1625790642.355,
    "queryString": "*",
    "period": 60,
    "metricArn": "arn:aws:iot:us-east-1:111122223333:fleetmetric/YourFleetMetricName",
    "aggregationField": "registry.version",
```

```
    "version": 1,
    "aggregationType": {
        "values": [
            "sum"
        ],
        "name": "Statistics"
    },
    "indexName": "AWS_Things",
    "creationDate": 1625790642.355,
    "metricName": "YourFleetMetricName"
}
```

Aktualisieren einer Flottenmetrik

Sie können den update-fleet-metric CLI-Befehl verwenden, um eine Flottenmetrik zu aktualisieren.

```
aws iot update-fleet-metric --metric-name "YourFleetMetricName" --query-string
 "*" --period 120 --aggregation-field "registry.version" --aggregation-type
 name=Statistics,values=sum,count --index-name AWS_Things
```

Der update-fleet-metric Befehl erzeugt keine Ausgabe. Sie können den describe-fleet-metric CLI-Befehl verwenden, um das Ergebnis anzuzeigen.

```
{
    "queryVersion": "2017-09-30",
    "lastModifiedDate": 1625792300.881,
    "queryString": "*",
    "period": 120,
    "metricArn": "arn:aws:iot:us-east-1:111122223333:fleetmetric/YourFleetMetricName",
    "aggregationField": "registry.version",
    "version": 2,
    "aggregationType": {
        "values": [
            "sum",
            "count"
        ],
        "name": "Statistics"
    },
    "indexName": "AWS_Things",
    "creationDate": 1625792300.881,
    "metricName": "YourFleetMetricName"
}
```

Löschen einer Flottenmetrik

Verwenden Sie den delete-fleet-metric CLI-Befehl , um eine Flottenmetrik zu löschen.

```
aws iot delete-fleet-metric --metric-name "YourFleetMetricName"
```

Dieser Befehl erzeugt keine Ausgabe, wenn das Löschen erfolgreich ist oder wenn Sie eine Flottenmetrik angeben, die nicht existiert.

Weitere Informationen finden Sie unter Problembehebung bei Flottenmetriken.

## Autorisieren des Taggings von IoT-Ressourcen

Für eine bessere Kontrolle über Flottenmetriken, die Sie erstellen, ändern oder verwenden, können Sie den Flottenmetriken Tags hinzufügen.

Um Flottenmetriken zu markieren, die Sie mit AWS Management Console oder erstellen AWS CLI, müssen Sie die -`iot:TagResource`Aktion in Ihre IAM-Richtlinie aufnehmen, um dem Benutzer Berechtigungen zu erteilen. Wenn Ihre IAM-Richtlinie `iot:TagResource` nicht beinhaltet, wird bei allen Aktionen zur Erstellung einer Flottenmetrik mit einem Tag ein Fehler `AccessDeniedException` zurückgegeben.

Weitere allgemeine Informationen zum Taggen von Ressourcen finden Sie unter Markieren Ihrer AWS IoT -Ressourcen.

Beispiele für IAM-Richtlinien

Sehen Sie sich das folgende Beispiel für eine IAM-Richtlinie an, in dem Tagging-Berechtigungen gewährt werden, wenn Sie eine Flottenmetrik erstellen:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": [
    "iot:TagResource"
   ],
   "Effect": "Allow",
   "Resource": [
    "arn:aws:iot:*:*:fleetmetric/*"
   ]
```

```
  },
  {
   "Action": [
    "iot:CreateFleetMetric"
   ],
   "Effect": "Allow",
   "Resource": [
    "arn:aws:iot:*:*:index/*",
    "arn:aws:iot:*:*:fleetmetric/*"
   ]
  }
 ]
}
```

Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT.

# MQTTbasierte Dateibereitstellung

Eine Option, mit der Sie Dateien verwalten und auf AWS IoT Geräte in Ihrer Flotte übertragen können, ist die MQTT basierte Dateizustellung. Mit dieser Funktion in der AWS Cloud können Sie einen Stream erstellen, der mehrere Dateien enthält, Sie können Stream-Daten (die Dateiliste und Beschreibungen) aktualisieren, die Stream-Daten abrufen und vieles mehr. AWS IoT MQTTDie basierte Dateizustellung kann Daten in kleinen Blöcken auf Ihre IoT-Geräte übertragen. Dabei wird das MQTT Protokoll mit Unterstützung für Anfrage- und Antwortnachrichten in JSON oder verwendetCBOR.

Weitere Informationen zur Übertragung von Daten zu und von IoT-Geräten mithilfe AWS IoT vonGeräte Connect mit AWS IoT.

Themen

- Was ist ein Stream?
- Einen Stream in der AWS Cloud verwalten
- Verwendung der AWS IoT MQTT basierten Dateibereitstellung auf Geräten
- Ein Beispiel für einen Anwendungsfall in Free RTOS OTA

## Was ist ein Stream?

In AWS IoT ist ein Stream eine öffentlich adressierbare Ressource, die eine Abstraktion für eine Liste von Dateien darstellt, die auf ein IoT-Gerät übertragen werden können. Ein typischer Stream enthält folgende Informationen:

- Ein Amazon-Ressourcenname (ARN), der einen Stream zu einem bestimmten Zeitpunkt eindeutig identifiziert. Das ARN hat das Musterarn:*partition*:iot:*region*:*account-ID*:stream/*stream ID*.
- Eine Stream-ID, die Ihren Stream identifiziert und in () oder SDK -Befehlen verwendet AWS Command Line Interface (und normalerweise erforderlich AWS CLI) wird.
- Eine Stream-Beschreibung, die eine Beschreibung der Stream-Ressource enthält.
- Eine Stream-Version, die eine bestimmte Version des Streams identifiziert. Da Stream-Daten unmittelbar geändert werden können, bevor Geräte mit der Datenübertragung beginnen, kann die Stream-Version von den Geräten verwendet werden, um eine Konsistenzprüfung zu erzwingen.

- Eine Liste von Dateien, die auf Geräte übertragen werden können. Für jede Datei in der Liste zeichnet der Stream eine Datei-ID, die Dateigröße und die Adressinformationen der Datei auf, die z. B. aus dem Namen des Amazon S3-Bucket, dem Objektschlüssel und der Objektversion bestehen.
- Eine Rolle AWS Identity and Access Management (IAM), die der AWS IoT MQTT basierten Dateizustellung die Berechtigung zum Lesen von im Datenspeicher gespeicherten Stream-Dateien erteilt.

AWS IoT MQTTDie basierte Dateizustellung bietet die folgenden Funktionen, sodass Geräte Daten aus der AWS Cloud übertragen können:

- Datenübertragung mithilfe des MQTT Protokolls.
- Support für JSON unsere CBOR Formate.
- Die Fähigkeit, einen Stream (`DescribeStream`API) zu beschreiben, um eine Stream-Dateiliste, eine Stream-Version und verwandte Informationen abzurufen.
- Die Fähigkeit, Daten in kleinen Blöcken (`GetStream`API) zu senden, sodass Geräte mit Hardwareeinschränkungen die Blöcke empfangen können.
- Support für eine dynamische Blockgröße pro Anforderung, um Geräte mit unterschiedlichen Speicherkapazitäten zu unterstützen.
- Optimierung für gleichzeitige Streaming-Anforderungen, wenn mehrere Geräte Datenblöcke aus derselben Stream-Datei anfordern.
- Amazon S3 als Datenspeicher für Stream-Dateien.
- Support für die Veröffentlichung von Datenübertragungsprotokollen von der AWS IoT MQTT basierten Dateizustellung an CloudWatch.

Informationen zu MQTT basierten Dateibereitstellungskontingenten finden Sie unter AWS IoT Core Servicekontingente in der Allgemeine AWS-Referenz.

## Einen Stream in der AWS Cloud verwalten

AWS IoT bietet AWS SDK und AWS CLI Befehle, mit denen Sie einen Stream in der AWS Cloud verwalten können. Diese Befehle bieten Ihnen folgende Möglichkeiten:

- Erstellen Sie einen Stream. CLI/SDK
- Beschreiben Sie einen Stream, um seine Informationen abzurufen. CLI/SDK

- Listen Sie Streams in Ihrem auf AWS-Konto. CLI/SDK
- Aktualisieren Sie die Dateiliste oder die Stream-Beschreibung in einem Stream. CLI/SDK
- Löschen Sie einen Stream. CLI/SDK

> **Note**
>
> Derzeit sind Streams in der AWS Management Console nicht sichtbar. Sie müssen das AWS CLI oder verwenden AWS SDK, um einen Stream in zu verwalten AWS IoT. Außerdem SDK ist Embedded C das einzigeSDK, das MQTT basierte Dateiübertragungen unterstützt.

Bevor Sie die AWS IoT MQTT basierte Dateizustellung von Ihren Geräten aus verwenden, müssen Sie sicherstellen, dass die folgenden Bedingungen für Ihre Geräte erfüllt sind, wie in den nächsten Abschnitten beschrieben:

- Eine Richtlinie, die die korrekten Berechtigungen widerspiegelt, die für die Übertragung von Daten über erforderlich sindMQTT.
- Ihr Gerät kann eine Verbindung zum AWS IoT Device Gateway herstellen.
- Eine Richtlinienanweisung, die besagt, dass Sie Ressourcen markieren können. Wenn `CreateStream` mit Markierungen aufgerufen wird, dann ist `iot:TagResource` erforderlich.

Bevor Sie die AWS IoT MQTT basierte Dateizustellung von Ihren Geräten aus verwenden, müssen Sie die Schritte in den nächsten Abschnitten befolgen, um sicherzustellen, dass Ihre Geräte ordnungsgemäß autorisiert sind und eine Verbindung zum AWS IoT Device Gateway herstellen können.

## Erteilen von Berechtigungen für Ihre Geräte

Sie können den Schritten unter Eine AWS IoT -Richtlinie erstellen folgen, um eine Geräterichtlinie zu erstellen oder eine bestehende Geräterichtlinie zu verwenden. Hängen Sie die Richtlinie an die Zertifikate an, die Ihren Geräten zugeordnet sind, und fügen Sie der Geräterichtlinie folgenden Berechtigungen hinzu.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {   "Effect": "Allow",
            "Action": [ "iot:Connect" ],
            "Resource": [
                "arn:partition:iot:region:accountID:client/
${iot:Connection.Thing.ThingName}"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [ "iot:Receive", "iot:Publish" ],
            "Resource": [
                "arn:partition:iot:region:accountID:topic/$aws/things/
${iot:Connection.Thing.ThingName}/streams/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iot:Subscribe",
            "Resource": [
                "arn:partition:iot:region:accountID:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/streams/*"
            ]
        }
    ]
}
```

## Connect deine Geräte mit AWS IoT

Geräte, die die AWS IoT MQTT basierte Dateizustellung verwenden, müssen eine Verbindung herstellen AWS IoT. AWS IoT MQTTDie basierte Dateibereitstellung lässt sich AWS IoT in die AWS Cloud integrieren, sodass Ihre Geräte eine direkte Verbindung zum Endpunkt der AWS IoT Datenebene herstellen sollten.

> **Note**
>
> Der Endpunkt der AWS IoT Datenebene ist spezifisch für die Region AWS-Konto und. Sie müssen den Endpunkt für die AWS-Konto und die Region verwenden, in der Ihre Geräte registriert sind AWS IoT.

Weitere Informationen finden Sie unter Verbinden mit AWS IoT Core.

## TagResource Verwendung

Die `CreateStream` API Aktion erstellt einen Stream für die Bereitstellung einer oder mehrerer großer Dateien in Blöcken. MQTT

Für einen erfolgreichen `CreateStream` API Anruf sind die folgenden Berechtigungen erforderlich:

- `iot:CreateStream`
- `iot:TagResource` (wenn `CreateStream` mit Markierungen vorliegt)

Die Richtlinie, die diese beiden Berechtigungen unterstützt, ist unten dargestellt:

```
{
 "Version": "2012-10-17",
 "Statement": {
     "Action": [ "iot:CreateStream", "iot:TagResource" ],
     "Effect": "Allow",
     "Resource": "arn:partition:iot:region:accountID:stream/streamId",
 }
}
```

Die Richtlinienanweisungsaktion `iot:TagResource` ist erforderlich, um sicherzustellen, dass ein Benutzer ohne die entsprechenden Berechtigungen keine Markierung für eine Ressource erstellen oder aktualisieren kann. Ohne die spezifische Richtlinienanweisung, Aktion von`iot:TagResource`, wird der `CreateStream` API Anruf zurückgegeben, und `AccessDeniedException` wenn die Anfrage Tags enthält.

Weitere Informationen erhalten Sie in folgenden Themen:

- CreateStream
- TagResource
- Markierung

# Verwendung der AWS IoT MQTT basierten Dateibereitstellung auf Geräten

Um den Datenübertragungsprozess einzuleiten, muss ein Gerät einen ersten Datensatz erhalten, der mindestens eine Stream-ID enthält. Sie können einen AWS IoT Jobs verwenden, um

Datenübertragungsaufgaben für Ihre Geräte zu planen, indem Sie den ursprünglichen Datensatz in das Auftragsdokument aufnehmen. Wenn ein Gerät den ersten Datensatz empfängt, sollte es dann die Interaktion mit der AWS IoT MQTT basierten Dateizustellung starten. Um Daten mit AWS IoT MQTT basierter Dateizustellung auszutauschen, sollte ein Gerät:

- Verwenden Sie das MQTT Protokoll, um das zu abonnierenThemen der MQTT-basierten Dateiübertragung.
- Senden Sie Anfragen und warten Sie dann, bis Sie die Antworten mithilfe von MQTT Nachrichten erhalten.

Sie können optional eine Stream-Datei-ID und eine Stream-Version in den ursprünglichen Datensatz aufnehmen. Das Senden einer Stream-Datei-ID an ein Gerät kann die Programmierung der Firmware/Software des Geräts vereinfachen, da dadurch keine `DescribeStream`-Anforderung vom Gerät gestellt werden muss, um diese ID zu erhalten. Das Gerät kann die Stream-Version in einer `GetStream`-Anforderung angeben, um eine Konsistenzprüfung zu erzwingen, falls der Stream unerwartet aktualisiert wurde.

## Wird verwendet DescribeStream , um Stream-Daten abzurufen

AWS IoT MQTTDie basierte Dateizustellung ermöglicht `DescribeStream` API das Senden von Stream-Daten an ein Gerät. Die dadurch zurückgegebenen Stream-Daten API umfassen die Stream-ID, die Stream-Version, die Stream-Beschreibung und eine Liste von Stream-Dateien, von denen jede eine Datei-ID und die Dateigröße in Byte hat. Mit diesen Informationen kann ein Gerät beliebige Dateien auswählen, um den Datenübertragungsprozess einzuleiten.

> **Note**
>
> Sie müssen die nicht verwenden, `DescribeStream` API wenn Ihr Gerät alle erforderlichen Stream-Dateien IDs im ursprünglichen Datensatz empfängt.

Führen Sie diese Schritte aus, um eine `DescribeStream`-Anforderung zu stellen.

1. Abonnieren Sie den „Akzeptiert“-Themenfilter `$aws/things/`*`ThingName`*`/streams/`*`StreamId`*`/description/json`.
2. Abonnieren Sie den „Abgelehnt“-Themenfilter `$aws/things/`*`ThingName`*`/streams/`*`StreamId`*`/rejected/json`.

3. Veröffentlichen Sie eine `DescribeStream`-Anforderung, indem Sie eine Nachricht an `$aws/things/ThingName/streams/StreamId/describe/json` senden.
4. Wenn die Anforderung akzeptiert wurde, erhält Ihr Gerät eine `DescribeStream`-Antwort auf den Themenfilter „Akzeptiert“.
5. Wenn die Anforderung abgelehnt wurde, erhält Ihr Gerät die Fehlerantwort im Themenfilter „Abgelehnt“.

> **Note**
>
> Wenn Sie `cbor` in den angezeigten Themen und Themenfiltern durch `json` ersetzen, empfängt Ihr Gerät Nachrichten in dem CBOR Format, das kompakter ist alsJSON.

## DescribeStream Anfrage

Eine typische `DescribeStream` Anfrage in JSON sieht wie das folgende Beispiel aus.

```
{
    "c": "ec944cfb-1e3c-49ac-97de-9dc4aaad0039"
}
```

- (Optional) „c“ ist das Feld für das Client-Token.

  Das Client-Token darf nicht länger als 64 Bytes sein. Ein Client-Token, das länger als 64 Byte ist, verursacht eine Fehlerantwort und eine `InvalidRequest`-Fehlermeldung.

## DescribeStream Antwort

Eine `DescribeStream` Antwort in JSON sieht wie das folgende Beispiel aus.

```
{
    "c": "ec944cfb-1e3c-49ac-97de-9dc4aaad0039",
    "s": 1,
    "d": "This is the description of stream ABC.",
    "r": [
        {
            "f": 0,
            "z": 131072
```

```
        },
        {
            "f": 1,
            "z": 51200
        }
    ]
}
```

- „c“ ist das Feld für das Client-Token. Es wird zurückgegeben, wenn es in der `DescribeStream`-Anforderung angegeben wurde. Verwenden Sie das Client-Token, um die Antwort der Anforderung zuzuordnen.
- "s" ist die Stream-Version als Ganzzahl. Sie können diese Version verwenden, um eine Konsistenzprüfung mit Ihren `GetStream` Anfragen durchzuführen.
- „r“ enthält eine Liste der Dateien im Stream.
  - „f“ ist die Stream-Datei-ID als Ganzzahl.
  - „z“ ist die Größe der Stream-Datei in Byte.
- „d“ enthält die Beschreibung des Streams.

## Abrufen von Datenblöcken aus einer Stream-Datei

Sie können das verwenden, `GetStream` API damit ein Gerät Stream-Dateien in kleinen Datenblöcken empfangen kann, sodass es von Geräten verwendet werden kann, die Einschränkungen bei der Verarbeitung großer Blockgrößen haben. Um eine komplette Datendatei zu empfangen, muss ein Gerät möglicherweise mehrere Anforderungen und Antworten senden oder empfangen, bis alle Datenblöcke empfangen und verarbeitet sind.

### GetStream Anfrage

Führen Sie diese Schritte aus, um eine `GetStream`-Anforderung zu stellen.

1. Abonnieren Sie den „Akzeptiert“-Themenfilter `$aws/things/`*`ThingName`*`/streams/`*`StreamId`*`/data/json`.
2. Abonnieren Sie den „Abgelehnt“-Themenfilter `$aws/things/`*`ThingName`*`/streams/`*`StreamId`*`/rejected/json`.
3. Veröffentlichen Sie eine `GetStream`-Anforderung zum Thema `$aws/things/`*`ThingName`*`/streams/`*`StreamId`*`/get/json`.

4. Wenn die Anforderung akzeptiert wurde, erhält Ihr Gerät eine oder mehrere `GetStream` Antworten auf den Themenfilter „Akzeptiert“. Jede Antwortnachricht enthält grundlegende Informationen und Nutzlastdaten für einen einzelnen Block.
5. Wiederholen Sie die Schritte 3 und 4, um alle Datenblöcke zu empfangen. Sie müssen diese Schritte wiederholen, wenn die angeforderte Datenmenge mehr als 128 KB beträgt. Sie müssen Ihr Gerät so programmieren, dass es mehrere `GetStream`-Anforderungen verwendet, damit alle angeforderten Daten empfangen werden.
6. Wenn die Anforderung abgelehnt wurde, erhält Ihr Gerät die Fehlerantwort im Themenfilter „Abgelehnt“.

> **Note**
>
> - Wenn Sie in den angezeigten Themen- und Themenfiltern „json“ durch „cbor“ ersetzen, empfängt Ihr Gerät Nachrichten in dem CBOR Format, das kompakter ist alsJSON.
> - AWS IoT MQTTDie basierte Dateizustellung begrenzt die Größe eines Blocks auf 128 KB. Wenn Sie eine Anforderung für einen Block stellen, der mehr als 128 KB groß ist, schlägt die Anforderung fehl.
> - Sie können eine Anforderung für mehrere Blöcke stellen, deren Gesamtgröße größer als 128 KB ist (wenn Sie beispielsweise eine Anforderung für 5 Blöcke mit jeweils 32 KB für insgesamt 160 KB an Daten stellen). In diesem Fall schlägt die Anfrage nicht fehl, aber Ihr Gerät muss mehrere Anfragen stellen, um alle angeforderten Daten zu empfangen. Der Service sendet zusätzliche Blöcke, wenn Ihr Gerät zusätzliche Anforderungen stellt. Wir empfehlen Ihnen, erst dann mit einer neuen Anforderungen fortzufahren, wenn die vorherige Antwort korrekt empfangen und verarbeitet wurde.
> - Unabhängig von der Gesamtgröße der angeforderten Daten sollten Sie Ihr Gerät so programmieren, dass es Wiederholungsversuche einleitet, wenn Blöcke nicht oder nicht korrekt empfangen werden.

Eine typische `GetStream` Anfrage in JSON sieht wie das folgende Beispiel aus.

```
{
    "c": "1bb8aaa1-5c18-4d21-80c2-0b44fee10380",
    "s": 1,
    "f": 0,
    "l": 4096,
```

```
    "o": 2,
    "n": 100,
    "b": "..."
}
```

- [optional] „c“ ist das Feld für das Client-Token.

  Das Client-Token darf nicht länger als 64 Bytes sein. Ein Client-Token, das länger als 64 Byte ist, verursacht eine Fehlerantwort und eine `InvalidRequest`-Fehlermeldung.
- [optional] „s“ ist das Feld für die Stream-Version (eine Ganzzahl).

  MQTTBei der basierten Dateibereitstellung wird eine Konsistenzprüfung durchgeführt, die auf dieser angeforderten Version und der neuesten Stream-Version in der Cloud basiert. Wenn die von einem Gerät in einer `GetStream`-Anforderung gesendete Stream-Version nicht mit der neuesten Stream-Version in der Cloud übereinstimmt, sendet der Service eine Fehlerantwort und eine `VersionMismatch`-Fehlermeldung. In der Regel empfängt ein Gerät die erwartete (neueste) Stream-Version im ursprünglichen Datensatz oder in der Antwort auf `DescribeStream`.
- „f“ ist die Stream-Datei-ID (eine Ganzzahl im Bereich von 0 bis 255).

  Die Stream-Datei-ID ist erforderlich, wenn Sie einen Stream mit dem oder erstellen AWS CLI oder aktualisierenSDK. Wenn ein Gerät eine Stream-Datei mit einer ID anfordert, die nicht existiert, sendet der Service eine Fehlerantwort und eine `ResourceNotFound`-Fehlermeldung.
- „l“ ist die Datenblockgröße in Byte (eine Ganzzahl im Bereich von 256 bis 131.072).

  Informationen zu Erstellen Sie eine Bitmap für eine Anfrage GetStream für Anweisungen, wie die Bitmap-Felder verwendet werden, um festzulegen, welcher Teil der Stream-Datei in der `GetStream`-Antwort zurückgegeben werden soll. Wenn ein Gerät eine Blockgröße angibt, die außerhalb des zulässigen Bereichs liegt, sendet der Service eine Fehlerantwort und eine `BlockSizeOutOfBounds`-Fehlermeldung.
- [optional] „o“ ist der Offset des Blocks in der Stream-Datei (eine Ganzzahl im Bereich von 0 bis 98.304).

  Informationen zu Erstellen Sie eine Bitmap für eine Anfrage GetStream für Anweisungen, wie die Bitmap-Felder verwendet werden, um festzulegen, welcher Teil der Stream-Datei in der `GetStream`-Antwort zurückgegeben werden soll. Der Höchstwert von 98.304 basiert auf einer Größenbeschränkung von 24 MB für Stream-Dateien und 256 Byte für die minimale Blockgröße. Wenn nichts angegeben ist, beträgt der Standardwert 0.
- [optional] „n“ ist die Anzahl der angeforderten Blöcke (eine Ganzzahl im Bereich von 0 bis 98.304).

Das Feld „n“ gibt entweder (1) die Anzahl der angeforderten Blöcke oder (2), wenn das Bitmap-Feld („b“) verwendet wird, eine Obergrenze für die Anzahl der Blöcke an, die von der Bitmap-Anforderung zurückgegeben werden. Diese zweite Verwendung ist optional. Wenn nicht definiert, ist sie standardmäßig 131072/*DataBlockSize*.

- [optional] „b“ ist eine Bitmap, welche die angeforderten Blöcke darstellt.

  Mithilfe einer Bitmap kann Ihr Gerät nicht aufeinanderfolgende Blöcke anfordern, was die Handhabung von Wiederholungsversuchen nach einem Fehler komfortabler macht. Informationen zu Erstellen Sie eine Bitmap für eine Anfrage GetStream für Anweisungen, wie die Bitmap-Felder verwendet werden, um festzulegen, welcher Teil der Stream-Datei in der `GetStream`-Antwort zurückgegeben werden soll. Konvertieren Sie für dieses Feld die Bitmap in eine Zeichenfolge, die den Bitmap-Wert in hexadezimaler Schreibweise darstellt. Die Bitmap muss kleiner als 12.288 Byte sein.

> **Important**
>
> Entweder „n“ oder „b“ sollte angegeben werden. Wenn keines von beiden festgelegt wurde, ist die `GetStream` Anforderung möglicherweise nicht gültig, wenn die Dateigröße weniger als 131.072 Byte (128 KB) beträgt.

## GetStream Antwort

Eine `GetStream` Antwort in JSON sieht für jeden angeforderten Datenblock wie in diesem Beispiel aus.

```
{
    "c": "1bb8aaa1-5c18-4d21-80c2-0b44fee10380",
    "f": 0,
    "l": 4096,
    "i": 2,
    "p": "..."
}
```

- „c“ ist das Feld für das Client-Token. Es wird zurückgegeben, wenn es in der `GetStream`-Anforderung angegeben wurde. Verwenden Sie das Client-Token, um die Antwort der Anforderung zuzuordnen.

- „f“ ist die ID der Stream-Datei, zu der die aktuelle Datenblock-Nutzlast gehört.
- „l“ ist die Größe der Datenblock-Nutzlast in Byte.
- „i“ ist die ID des Datenblocks, der in der Nutzlast enthalten ist. Datenblöcke werden beginnend mit 0 durchnummeriert.
- „p“ enthält die Nutzlast des Datenblocks. Dieses Feld ist eine Zeichenfolge, die den Wert des Datenblocks in Base64-Kodierung darstellt.

## Erstellen Sie eine Bitmap für eine Anfrage GetStream

Sie können das Bitmap-Feld (b) in einer `GetStream`-Anforderung verwenden, um nicht aufeinanderfolgende Blöcke aus einer Stream-Datei abzurufen. Dies hilft Geräten mit begrenzter RAM Kapazität, Probleme mit der Netzwerkzustellung zu lösen. Ein Gerät kann nur die Blöcke anfordern, die nicht oder nicht korrekt empfangen wurden. Die Bitmap bestimmt, welche Blöcke der Stream-Datei zurückgegeben werden. Für jedes Bit, das in der Bitmap auf 1 festgelegt ist, wird ein entsprechender Block der Stream-Datei zurückgegeben.

Hier sehen Sie ein Beispiel für die Angabe einer Bitmap und ihrer unterstützenden Felder in einer `GetStream`-Anforderung. Sie möchten beispielsweise eine Stream-Datei in Blöcken von 256 Byte (der Blockgröße) empfangen. Stellen Sie sich vor, dass jeder Block mit 256 Byte eine Zahl hat, die seine Position in der Datei angibt, beginnend bei 0. Block 0 ist also der erste Block mit 256 Byte in der Datei, Block 1 der zweite usw. Sie möchten die Blöcke 20, 21, 24 und 43 aus der Datei anfordern.

Block-Offset

Da der erste Block die Nummer 20 hat, geben Sie als Offset (Feld o) 20 an, um Platz in der Bitmap zu sparen.

Anzahl der Blöcke

Um sicherzustellen, dass Ihr Gerät nicht mehr Blöcke empfängt, als es mit begrenzten Speicherressourcen verarbeiten kann, können Sie die maximale Anzahl von Blöcken angeben, die in jeder per MQTT basierter Dateizustellung gesendeten Nachricht zurückgegeben werden sollen. Beachten Sie, dass dieser Wert nicht berücksichtigt wird, wenn die Bitmap selbst weniger als diese Anzahl von Blöcken angibt oder wenn dadurch die Gesamtgröße der per MQTT basierter Dateizustellung gesendeten Antwortnachrichten das Servicelimit von 128 KB pro `GetStream` Anfrage überschreiten würde.

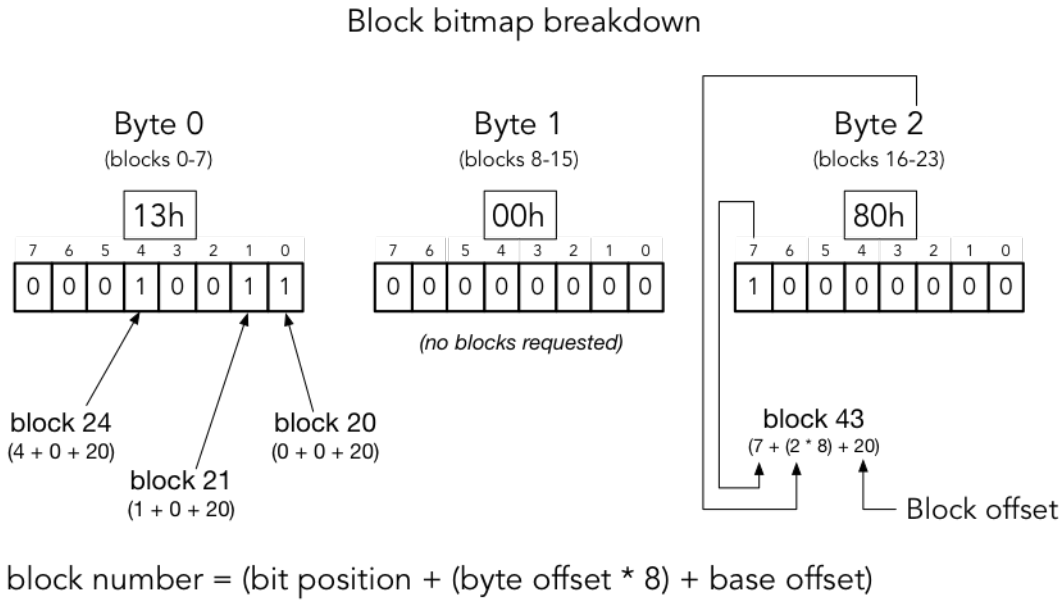
### Block-Bitmap

Die Bitmap selbst ist ein Array von Bytes ohne Vorzeichen, die in hexadezimaler Schreibweise ausgedrückt und in der `GetStream`-Anforderung als Zeichenkettendarstellung der Zahl enthalten sind. Aber um diese Zeichenfolge zu konstruieren, stellen wir uns die Bitmap zunächst als eine lange Folge von Bits (eine Binärzahl) vor. Wenn ein Bit in dieser Sequenz auf 1 festgelegt ist, wird der entsprechende Block aus der Stream-Datei an das Gerät zurückgesendet. In unserem Beispiel wollen wir die Blöcke 20, 21, 24 und 43 empfangen, also müssen wir die Bits 20, 21, 24 und 43 in unserer Bitmap setzen. Wir können den Block-Offset verwenden, um Platz zu sparen. Nachdem wir also den Offset von jeder Blocknummer subtrahiert haben, möchten wir die Bits 0, 1, 4 und 23 wie im folgenden Beispiel setzen.

```
1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
```

Wenn wir jeweils ein Byte (8 Bit) nehmen, wird dies üblicherweise wie folgt geschrieben: „0b00010011“, „0b00000000“ und „0b10000000“. Bit 0 erscheint in unserer binären Darstellung am Ende des ersten Bytes und Bit 23 am Anfang des letzten Bytes. Das kann verwirrend sein, es sei denn, Sie kennen die Konventionen. Das erste Byte enthält die Bits 7-0 (in dieser Reihenfolge), das zweite Byte enthält die Bits 15-8, das dritte Byte enthält die Bits 23-16 und so weiter. In hexadezimaler Schreibweise wird dies in „0x130080“ umgewandelt.

> **Tip**
>
> Sie können die standardmäßige Binärschreibweise in die hexadezimale Schreibweise konvertieren. Nehmen Sie jeweils vier Binärziffern und konvertieren Sie diese in ihre hexadezimale Entsprechung. Zum Beispiel wird aus „0001“ „1“, aus „0011“ wird „3“ und so weiter.




Wenn wir das alles zusammenfassen, sieht das JSON für unsere `GetStream` Anfrage wie folgt aus.

```
{
    "c" : "1",
    "s" : 1,
    "l" : 256,
    "f" : 1,
    "o" : 20,
    "n" : 32,
    "b" : "130080"
}
```

- „c“ ist das Feld für das Client-Token.
- „s“ ist die erwartete Stream-Version.
- „l“ ist die Größe der Datenblock-Nutzlast in Byte.
- „f“ ist die ID des Quelldatei-Indexes.
- „o“ ist der Block-Offset.
- „n“ ist die Anzahl der Blöcke.
- "b" ist die fehlende blockId Bitmap, beginnend mit dem Offset. Dieser Wert muss based64-codiert sein.

# Behandlung von Fehlern bei der AWS IoT MQTT basierten Dateizustellung

Eine Fehlerantwort, die für beide an ein Gerät gesendet wird `DescribeStream` und ein Client-Token, einen Fehlercode und eine Fehlermeldung `GetStream` APIs enthält. Eine typische Fehlerantwort sieht wie im folgenden Beispiel aus.

```
{
    "o": "BlockSizeOutOfBounds",
    "m": "The block size is out of bounds",
    "c": "1bb8aaa1-5c18-4d21-80c2-0b44fee10380"
}
```

- „o“ ist der Fehlercode, der den Grund anzeigt, warum ein Fehler aufgetreten ist. Weitere Informationen finden Sie in den Fehlercodes weiter unten in diesem Abschnitt.
- „m“ ist die Fehlermeldung, die Einzelheiten des Fehlers anzeigt.
- „c“ ist das Feld für das Client-Token. Dies kann zurückgegeben werden, wenn es in der `DescribeStream`-Anforderung angegeben wurde. Sie können das Client-Token verwenden, um die Antwort der Anforderung zuzuordnen.

  Das Client-Token-Feld ist nicht immer in einer Fehlerantwort enthalten. Wenn das in der Anforderung angegebene Client-Token nicht gültig oder falsch formatiert ist, wird es in der Fehlerantwort nicht zurückgegeben.

> **Note**
>
> Aus Gründen der Abwärtskompatibilität können Felder in der Fehlerantwort nicht abgekürzt sein. Beispielsweise kann der Fehlercode entweder durch die Felder „Code“ oder „o“ und das Client-Token-Feld entweder durch die Felder "clientToken" oder „c“ gekennzeichnet werden. Wir empfehlen Ihnen, die oben abgebildete Abkürzungsform zu verwenden.

InvalidTopic

Das MQTT Thema der Streamnachricht ist ungültig.

InvalidJson

Die Stream-Anfrage ist kein gültiges JSON Dokument.

InvalidCbor

Die Stream-Anfrage ist kein gültiges CBOR Dokument.

InvalidRequest

Die Anforderung wird im Allgemeinen als falsch formatiert identifiziert. Weitere Informationen finden Sie in der Fehlermeldung.

Nicht autorisiert

Die Anforderung ist nicht berechtigt, auf die Stream-Daten-Dateien auf dem Speichermedium wie Amazon S3 zuzugreifen. Weitere Informationen finden Sie in der Fehlermeldung.

BlockSizeOutOfBounds

Die Blockgröße liegt außerhalb der Grenzen. Weitere Informationen finden Sie im Abschnitt „MQTTbasierte Dateibereitstellung“ unter AWS IoT Core Service Quotas.

OffsetOutOfBounds

Der Offset liegt außerhalb der Grenzen. Weitere Informationen finden Sie im Abschnitt „MQTTbasierte Dateibereitstellung“ unter AWS IoT Core Service Quotas.

BlockCountLimitExceeded

Die Anzahl der Anforderungsblöcke ist außerhalb des zulässigen Bereichs. Weitere Informationen finden Sie im Abschnitt „MQTTbasierte Dateibereitstellung“ unter AWS IoT Core Service Quotas.

BlockBitmapLimitExceeded

Die Größe der Anforderungsbitmap liegt außerhalb des gültigen Bereichs. Weitere Informationen finden Sie im Abschnitt „MQTTbasierte Dateibereitstellung“ unter AWS IoT Core Service Quotas.

ResourceNotFound

Der angeforderte Stream, die Dateien, Dateiversionen oder Blöcke wurden nicht gefunden. Weitere Details und Informationen finden Sie in der Fehlermeldung.

VersionMismatch

Die Stream-Version in der Anfrage stimmt nicht mit der Stream-Version in der Funktion zur MQTT basierten Dateizustellung überein. Dies weist darauf hin, dass die Stream-Daten seit dem ersten Empfang der Stream-Version durch das Gerät geändert wurden.

ETagMismatch

Die S3 ETag im Stream stimmt nicht mit ETag der aktuellen S3-Objektversion überein.

InternalError

Bei der MQTT basierten Dateizustellung ist ein interner Fehler aufgetreten.

# Ein Beispiel für einen Anwendungsfall in Free RTOS OTA

Der Free RTOS OTA (over-the-air) -Agent verwendet die AWS IoT MQTT basierte Dateibereitstellung, um kostenlose RTOS Firmware-Images auf RTOS Free-Geräte zu übertragen. Um den ersten Datensatz an ein Gerät zu senden, verwendet es den AWS IoT Job Service, um einen OTA Aktualisierungsauftrag für kostenlose RTOS Geräte zu planen.

Eine Referenzimplementierung eines MQTT basierten Clients für die Dateizustellung finden Sie in der kostenlosen RTOS Dokumentation unter Kostenlose RTOS OTA Agent-Codes.

# Device Advisor

Device Advisor ist eine cloudbasierte, vollständig verwaltete Testfunktion zur Validierung von IoT-Geräten während der Entwicklung von Gerätesoftware. Device Advisor bietet vorgefertigte Tests, mit denen Sie IoT-Geräte auf zuverlässige und sichere Konnektivität überprüfen können AWS IoT Core, bevor Sie Geräte in der Produktion einsetzen. Die vorgefertigten Tests von Device Advisor helfen Ihnen dabei, Ihre Gerätesoftware anhand von Best Practices für die Verwendung von TLSMQTT, Device Shadow und IoT-Jobs zu validieren. Sie können auch signierte Qualifikationsberichte herunterladen, um sie an das AWS -Partnernetzwerk zu senden, damit Ihr Gerät für den AWS -Partnergerätekatalog qualifiziert wird, ohne dass Sie Ihr Gerät einschicken und warten müssen, bis es getestet wird.

> **Note**
>
> Device Advisor wird in den Regionen us-east-1, us-west-2, ap-northeast-1 und eu-west-1 unterstützt.
> Device Advisor unterstützt Geräte und Clients, die die Protokolle MQTT und MQTT over WebSocket Secure (WSS) verwenden, um Nachrichten zu veröffentlichen und zu abonnieren.
> Alle Protokolle unterstützen IPv4 undIPv6.
> Device Advisor unterstützt RSA Serverzertifikate.

Jedes Gerät, mit dem eine Verbindung hergestellt werden AWS IoT Core kann, kann Device Advisor nutzen. Sie können auf Device Advisor von der AWS IoT Konsole aus zugreifen, oder verwenden Sie die Taste AWS CLI oderSDK. Wenn Sie bereit sind, Ihr Gerät zu testen, registrieren Sie es AWS IoT Core und konfigurieren Sie die Gerätesoftware mit dem Device Advisor-Endpunkt. Wählen Sie dann die vorgefertigten Tests aus, konfigurieren Sie sie und führen Sie die Tests auf Ihrem Gerät aus. Sie erhalten dann die Testergebnisse zusammen mit detaillierten Protokollen oder einem Qualifizierungsbericht.

Device Advisor ist ein Testendpunkt in der AWS Cloud. Sie können Ihre Geräte testen, indem Sie sie so konfigurieren, dass sie eine Verbindung zu dem vom Device Advisor bereitgestellten Testendpunkt herstellen. Nachdem ein Gerät für die Verbindung mit dem Testendpunkt konfiguriert wurde, können Sie die Device Advisor-Konsole aufrufen oder AWS SDK dort die Tests auswählen, die Sie auf Ihren Geräten ausführen möchten. Device Advisor verwaltet dann den gesamten Lebenszyklus eines Tests, einschließlich der Bereitstellung von Ressourcen, der Planung des Testprozesses, der

Verwaltung des Zustandsautomats, der Aufzeichnung des Geräteverhaltens, der Protokollierung der Ergebnisse und der Bereitstellung der Endergebnisse in Form eines Testberichts.

TLSProtokolle

Das Transport Layer Security (TLS) -Protokoll wird verwendet, um vertrauliche Daten in unsicheren Netzwerken wie dem Internet zu verschlüsseln. Das TLS Protokoll ist der Nachfolger des Secure Sockets Layer (SSL) -Protokolls.

Device Advisor unterstützt die folgenden TLS Protokolle:

- TLS1.3 (empfohlen)
- TLS1.2

Protokolle, Port-Zuweisungen und Authentifizierung

Das Gerätekommunikationsprotokoll wird von einem Gerät oder einem Client verwendet, um über einen Geräteendpunkt eine Verbindung zum Message Broker herzustellen. In der folgenden Tabelle sind die Protokolle aufgeführt, die von den Device-Advisor-Endpunkten unterstützt werden, sowie die verwendeten Authentifizierungsmethoden und Ports.

Protokolle, Authentifizierung und Port-Zuweisungen

| Protokoll | Unterstützte Operationen | Authentifizierung | Port | ALPNName des Protokolls |
|---|---|---|---|---|
| MQTTüber WebSocket | Veröffentlichen, Abonnieren | Signaturversion 4 | 443 | N/A |
| MQTT | Veröffentlichen, Abonnieren | X.509-Clientzertifikat | 8883 | `x-amzn-mqtt-ca` |
| MQTT | Veröffentlichen, Abonnieren | X.509-Clientzertifikat | 443 | N/A |

Dieses Kapitel enthält die folgenden Abschnitte:

- Einrichtung
- Erste Schritte mit Device Advisor in der Konsole
- Device-Advisor-Workflow

- Ausführlicher Konsolen-Workflow von Device Advisor
- Konsolen-Workflow für Tests mit langer Dauer
- Device VPC Advisor-Endpunkte ()AWS PrivateLink
- Device-Advisor-Testfälle

# Einrichtung

Führen Sie die folgenden Schritte aus, bevor Sie Device Advisor zum ersten Mal verwenden:

## Erstellen eines IoT-Dings

Erstellen Sie zunächst ein IoT-Ding und fügen Sie diesem Ding ein Zertifikat hinzu. Ein Tutorial zum Erstellen von Dingen finden Sie unter Create a thing object (Erstellen eines Dingobjekts).

## Erstellen Sie eine IAM Rolle, die Sie als Ihre Geräterolle verwenden möchten

> **Note**
>
> Sie können die Geräterolle mit der Device-Advisor-Konsole schnell erstellen. Informationen zum Einrichten Ihrer Geräterolle mit der Device-Advisor-Konsole finden Sie unter Getting started with the Device Advisor in the console.

1. Rufen Sie die AWS Identity and Access Management Konsole auf und melden Sie sich bei dem an, den AWS-Konto Sie für Device Advisor-Tests verwenden.
2. Wählen Sie im linken Navigationsbereich die Option Richtlinien aus.
3. Wählen Sie Create Policy (Richtlinie erstellen) aus.
4. Gehen Sie unter Richtlinie erstellen wie folgt vor:

    a. Wählen Sie unter Service die Option IoT aus.

    b. Führen Sie unter Aktionen eine der folgenden Aktionen aus.

    - (Empfohlen) Wählen Sie Aktionen auf der Grundlage der Richtlinie aus, die dem IoT-Ding oder dem IoT-Zertifikat zugeordnet ist, das Sie im vorherigen Abschnitt erstellt haben.
    - Suchen Sie im Feld Filteraktion nach den folgenden Aktionen und wählen Sie sie aus:

- `Connect`
- `Publish`
- `Subscribe`
- `Receive`
- `RetainPublish`

c. Schränken Sie unter Ressourcen die Ressourcen für Client und Thema ein. Die Einschränkung dieser Ressourcen ist eine bewährte Sicherheitsmethode. Gehen Sie wie folgt vor, um Ressourcen einzuschränken:

i. Wählen Sie ARNfür die Aktion Connect die Option Client-Ressource angeben aus.

ii. Wählen Sie „Hinzufügen ARN“ und führen Sie dann einen der folgenden Schritte aus:

> **Note**
>
> Das clientIdist die MQTT Client-ID, die Ihr Gerät für die Interaktion mit Device Advisor verwendet.

- Geben Sie die Region, die accountID und clientID im Visual Editor an. ARN
- Geben Sie manuell die Amazon-Ressourcennamen (ARNs) der IoT-Themen ein, mit denen Sie Ihre Testfälle ausführen möchten.

iii. Wählen Sie Hinzufügen aus.

iv. Wählen Sie „Themenressource angeben“ ARN für „Empfangen“ und eine weitere Aktion aus.

v. Wählen Sie „Hinzufügen ARN“ und führen Sie dann einen der folgenden Schritte aus:

> **Note**
>
> Der Themenname ist das MQTT Thema, zu dem Ihr Gerät Nachrichten veröffentlicht.

- Geben Sie die Region, die accountID und den Themennamen im Visual ARN Editor an.

- Geben Sie manuell ARNs die IoT-Themen ein, mit denen Sie Ihre Testfälle ausführen möchten.

vi. Wählen Sie Hinzufügen aus.

vii. Wählen Sie ARNfür die Aktion Abonnieren die Option topicFilter Ressource angeben aus.

viii. Wählen Sie „Hinzufügen ARN“ und führen Sie dann einen der folgenden Schritte aus:

> **Note**
>
> Der Themenname ist das MQTT Thema, das Ihr Gerät abonniert hat.

- Geben Sie die Region, die accountID und den Themennamen im Visual ARN Editor an.
- Geben Sie manuell ARNs die IoT-Themen ein, mit denen Sie Ihre Testfälle ausführen möchten.

ix. Wählen Sie Hinzufügen aus.

5. Wählen Sie Next: Tags (Weiter: Tags) aus.
6. Klicken Sie auf Weiter: Prüfen.
7. Geben Sie unter Richtlinie überprüfen einen Namen für Ihre Richtlinie ein.
8. Wählen Sie Create Policy (Richtlinie erstellen) aus.
9. Wählen Sie im linken Navigationsbereich Rollen aus.
10. Wählen Sie Create Role aus.
11. Wählen Sie unter Vertrauenswürdige Entitäten auswählen die Option Benutzerdefinierte Vertrauensrichtlinie aus.
12. Geben Sie die folgende Vertrauensrichtlinie in das Feld Benutzerdefinierte Vertrauensrichtlinie ein. Verwenden Sie die globalen Konditionsschlüssel `aws:SourceArn` und `aws:SourceAccount` für die Richtlinie, um vor dem Confused-Deputy-Problem zu schützen.

> **Important**
>
> Ihr `aws:SourceArn` muss mit dem `format: arn:aws:iotdeviceadvisor:`*`region:account-id`*`:*.` konform sein. Stellen Sie sicher, dass *`region`* Ihrer AWS IoT -Region entspricht und dass *`account-id`* Ihrer

Kundenkonto-ID entspricht. Weitere Informationen finden Sie unter Vermeidung des dienstübergreifenden Confused-Deputy-Problems.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAwsIoTCoreDeviceAdvisor",
            "Effect": "Allow",
            "Principal": {
                "Service": "iotdeviceadvisor.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn":
 "arn:aws:iotdeviceadvisor:*:111122223333:suitedefinition/*"
                }
            }
        }
    ]
}
```

13. Wählen Sie Weiter.
14. Wählen Sie die Richtlinie aus, den Sie in Schritt 4 erstellt haben.
15. (Optional) Wählen Sie unter Berechtigungsgrenze festlegen die Option Use a permissions boundary to control the maximum role permissions (Eine Berechtigungsgrenze verwenden, um die maximalen Rollenberechtigungen zu kontrollieren) aus und dann die Richtlinie, die Sie erstellt haben.
16. Wählen Sie Weiter.
17. Geben Sie einen Rollennamen und eine Rollenbeschreibung an.
18. Wählen Sie Rolle erstellen.

## Erstellen Sie eine individuell verwaltete Richtlinie für einen IAM Benutzer zur Verwendung von Device Advisor

1. Navigieren Sie zur IAM-Konsole unter https://console.aws.amazon.com/iam/. Geben Sie bei Aufforderung Ihre AWS -Anmeldeinformationen ein.
2. Wählen Sie im linken Navigationsbereich Richtlinien aus.
3. Wählen Sie Create Policy und anschließend die JSONRegisterkarte aus.
4. Fügen Sie die erforderlichen Berechtigungen hinzu, um Device Advisor zu verwenden. Das Richtliniendokument finden Sie im Thema Bewährte Methoden für die Sicherheit.
5. Wählen Sie Review policy (Richtlinie überprüfen) aus.
6. Geben Sie Name (Name) und Description (Beschreibung) ein.
7. Wählen Sie Create Policy (Richtlinie erstellen) aus.

## Erstellen Sie einen IAM Benutzer für die Verwendung von Device Advisor

> **Note**
>
> Es wird empfohlen, einen IAM Benutzer für die Ausführung von Device Advisor-Tests zu erstellen. Das Ausführen von Device-Advisor-Tests als Administratorbenutzer kann Sicherheitsrisiken bergen und wird nicht empfohlen.

1. Navigieren Sie zur IAM Konsole unter https://console.aws.amazon.com/iam/Wenn Sie dazu aufgefordert werden, geben Sie Ihre AWS Anmeldeinformationen ein, um sich anzumelden.
2. Wählen Sie im linken Navigationsbereich Benutzer aus.
3. Wählen Sie Benutzer hinzufügen.
4. Geben Sie einen Benutzernamen ein.
5. Benutzer benötigen programmgesteuerten Zugriff, wenn sie mit AWS außerhalb des AWS Management Console interagieren möchten. Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

   Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

| Welcher Benutzer benötigt programmgesteuerten Zugriff? | Bis | Von |
| --- | --- | --- |
| Mitarbeiteridentität<br><br>(In IAM Identity Center verwaltete Benutzer) | Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren. | Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.<br><br>• Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zur Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch.<br>• Informationen zu AWS SDKs Tools und AWS APIs finden Sie unter IAMIdentity Center-Authentifizierung im Referenzhandbuch AWS SDKsund im Tools-Ref erenzhandbuch. |
| IAM | Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren. | Folgen Sie den Anweisungen unter Verwenden temporäre r Anmeldeinformationen mit AWS Ressourcen im IAMBenutzerhandbuch. |

| Welcher Benutzer benötigt programmgesteuerten Zugriff? | Bis | Von |
| --- | --- | --- |
| IAM | (Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren. | Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.<br>• Informationen dazu AWS CLI finden Sie unter Authentifizierung mithilfe von IAM Benutzeranmeldedaten im AWS Command Line Interface Benutzerhandbuch.<br>• Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch AWS SDKsund im Tools-Referenzhandbuch.<br>• Weitere Informationen finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM Benutzer im IAMBenutzerhandbuch. AWS APIs |

6. Wählen Sie Weiter: Berechtigungen aus.
7. Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

   • Benutzer und Gruppen in AWS IAM Identity Center:

   Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, IAM die über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verband) im IAMBenutzerhandbuch.

- IAMBenutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Eine Rolle für einen IAM Benutzer erstellen im IAMBenutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Folgen Sie den Anweisungen unter Hinzufügen von Berechtigungen für einen Benutzer (Konsole) im IAMBenutzerhandbuch.

8. Geben Sie in das Suchfeld den Namen der individuell verwalteten Richtlinie ein, die Sie erstellt haben. Aktivieren Sie dann das Kontrollkästchen für Richtliniennamen.
9. Wählen Sie Next: Tags (Weiter: Tags) aus.
10. Klicken Sie auf Next: Review (Weiter: Prüfen).
11. Wählen Sie Create user aus.
12. Klicken Sie auf Close (Schließen).

Device Advisor benötigt in Ihrem Namen Zugriff auf Ihre AWS Ressourcen (Dinge, Zertifikate und Endpunkte). Ihr IAM Benutzer muss über die erforderlichen Berechtigungen verfügen. Device Advisor veröffentlicht auch Protokolle auf Amazon, CloudWatch wenn Sie Ihrem IAM Benutzer die erforderlichen Berechtigungsrichtlinien beifügen.

## Konfigurieren Ihres Geräts

Device Advisor verwendet die TLS Erweiterung „Servername Indication“ (SNI), um TLS Konfigurationen anzuwenden. Geräte müssen diese Erweiterung verwenden, wenn sie eine Verbindung herstellen und einen Servernamen übergeben, der mit dem Device-Advisor-Testendpunkt identisch ist.

Device Advisor ermöglicht die TLS Verbindung, wenn sich ein Test im `Running` Status befindet. Er verweigert die TLS Verbindung vor und nach jedem Testlauf. Aus diesem Grund empfehlen wir, den Mechanismus zur Wiederholung der Geräteverbindung zu verwenden, um ein vollautomatisches Testerlebnis mit Device Advisor zu gewährleisten. Sie können Testsuiten ausführen, die mehr als einen Testfall enthalten, z. B. TLS Connect, MQTT Connect und MQTT Publish. Wenn Sie mehrere Testfälle ausführen, empfehlen wir, dass Ihr Gerät versucht, alle fünf Sekunden eine

Verbindung zu unserem Testendpunkt herzustellen. Sie können dann die Ausführung mehrerer Testfälle nacheinander automatisieren.

> **Note**
>
> Um Ihre Gerätesoftware für das Testen vorzubereiten, empfehlen wir, eine zu verwendenSDK, mit der eine Verbindung hergestellt werden kann AWS IoT Core. Anschließend sollten Sie den SDK mit dem für Sie bereitgestellten Device Advisor-Testendpunkt aktualisieren AWS-Konto.

Device Advisor unterstützt zwei Arten von Endpunkten: Endpunkte auf Kontoebene und Endpunkte auf Geräteebene. Wählen Sie den Endpunkt aus, der Ihrem Anwendungsfall am besten entspricht. Um mehrere Testsuiten für verschiedene Geräte gleichzeitig auszuführen, verwenden Sie einen Endpunkt auf Geräteebene.

Führen Sie den folgenden Befehl aus, um den Endpunkt auf Geräteebene abzurufen:

Für MQTT Kunden, die X.509-Client-Zertifikate verwenden:

```
aws iotdeviceadvisor get-endpoint --thing-arn your-thing-arn
```

or

```
aws iotdeviceadvisor get-endpoint --certificate-arn your-certificate-arn
```

Für MQTT mehr als WebSocket Kunden, die Signature Version 4 verwenden:

```
aws iotdeviceadvisor get-endpoint --device-role-arn your-device-role-arn --
authentication-method SignatureVersion4
```

Um jeweils eine Testsuite auszuführen, wählen Sie einen Endpunkt auf Kontoebene. Führen Sie den folgenden Befehl aus, um den Endpunkt auf Kontoebene abzurufen:

```
aws iotdeviceadvisor get-endpoint
```

# Erste Schritte mit Device Advisor in der Konsole

Dieses Tutorial hilft Ihnen bei den ersten Schritten AWS IoT Core Device Advisor auf der Konsole. Device Advisor bietet Features wie erforderliche Tests und signierte Qualifikationsberichte. Sie können diese Tests und Berichte verwenden, um Geräte zu qualifizieren und im -Partner-Gerätekatalog aufzulisten, wie im AWS IoT Core -Qualifizierungsprogramm beschrieben.

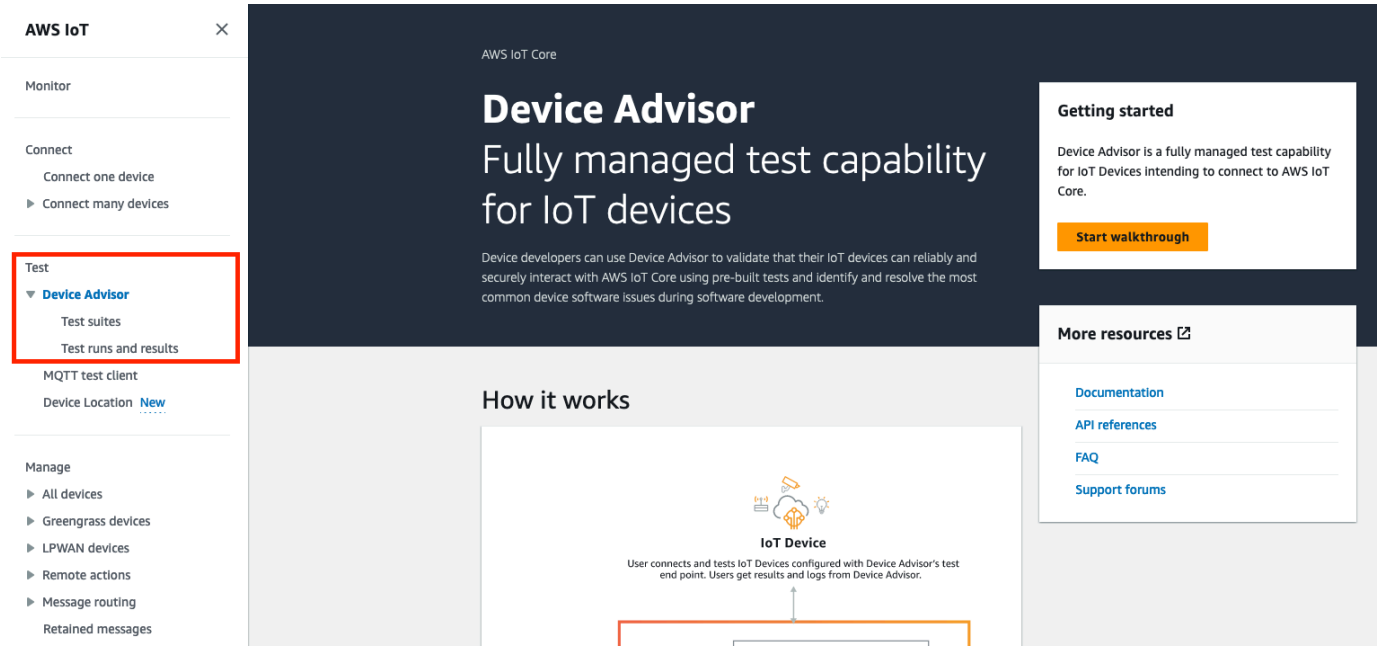
Weitere Informationen zum Verwenden von Device Advisor finden Sie unter Device-Advisor-Workflow und Ausführlicher Konsolen-Workflow von Device Advisor.

Führen Sie die Schritte in Einrichtung aus, um dieses Tutorial abzuschließen.

> **Note**
>
> Device Advisor wird in den folgenden Bereichen unterstützt AWS-Regionen:
>
> - USA Ost (Nord-Virginia)
> - USA West (Oregon)
> - Asien-Pazifik (Tokio)
> - Europa (Irland)

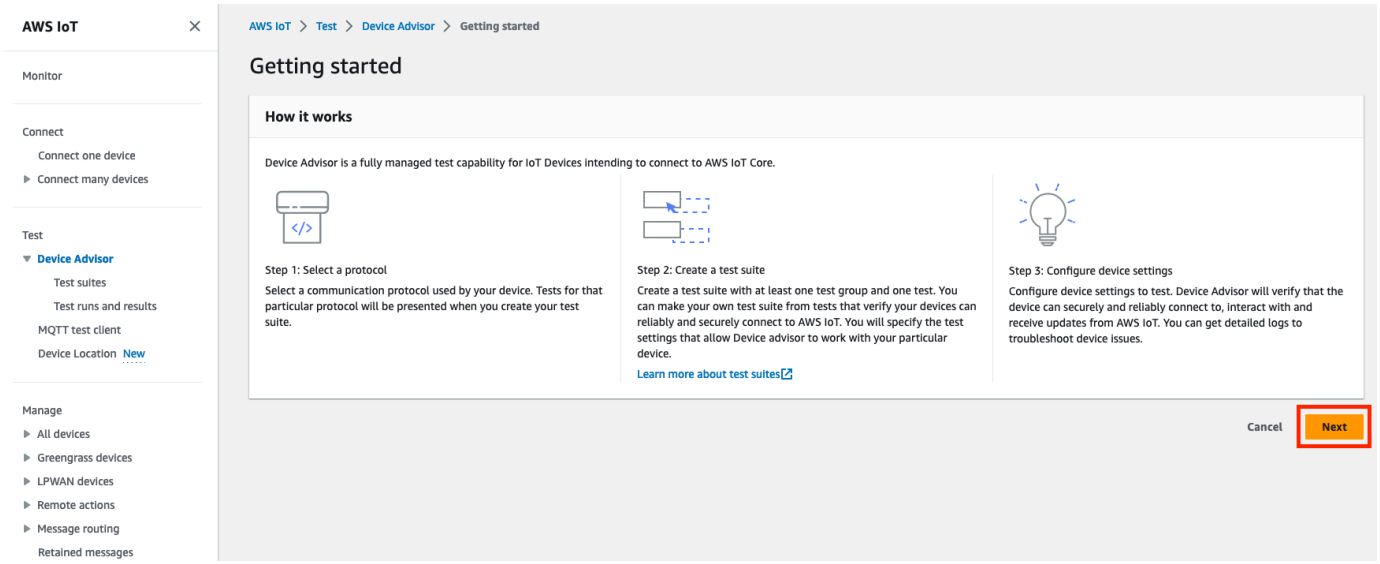
Erste Schritte

1. Wählen Sie im Navigationsbereich der AWS IoT -Konsole unter Test die Option Device Advisor aus. Wählen Sie dann auf der Konsole die Schaltfläche Walkthrough starten aus.

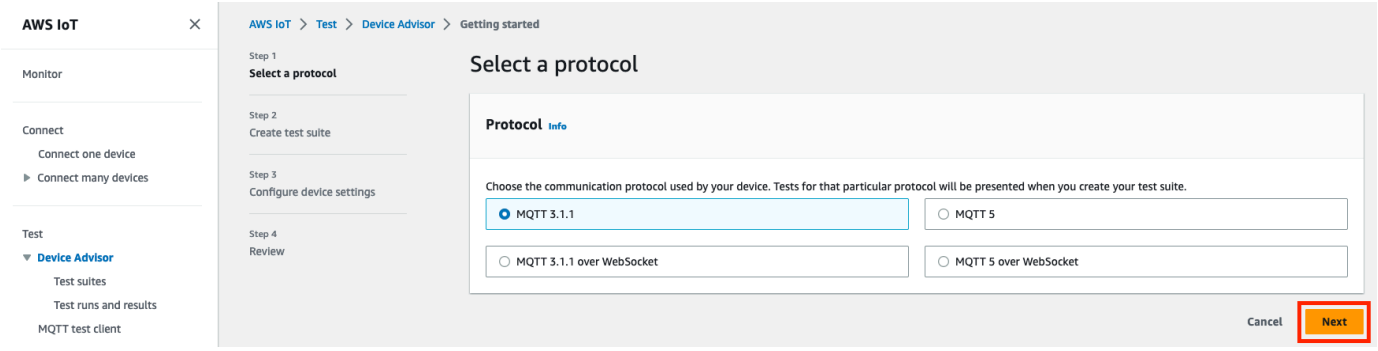



2. Die Seite Erste Schritte mit Device Advisor bietet einen Überblick über die Schritte, die zum Erstellen einer Testsuite und zum Ausführen von Tests auf Ihrem Gerät erforderlich sind. Den Device-Advisor-Testendpunkt für Ihr Konto finden Sie auch hier. Sie müssen die Firmware oder Software auf dem zum Testen verwendeten Gerät konfigurieren, um eine Verbindung zu diesem Testendpunkt herzustellen.

   Um dieses Tutorial abzuschließen, müssen Sie zunächst eine Sache und ein Zertifikat erstellen. Nachdem Sie sich die Informationen unter Funktionsweise gelesen haben, wählen Sie Weiter aus.

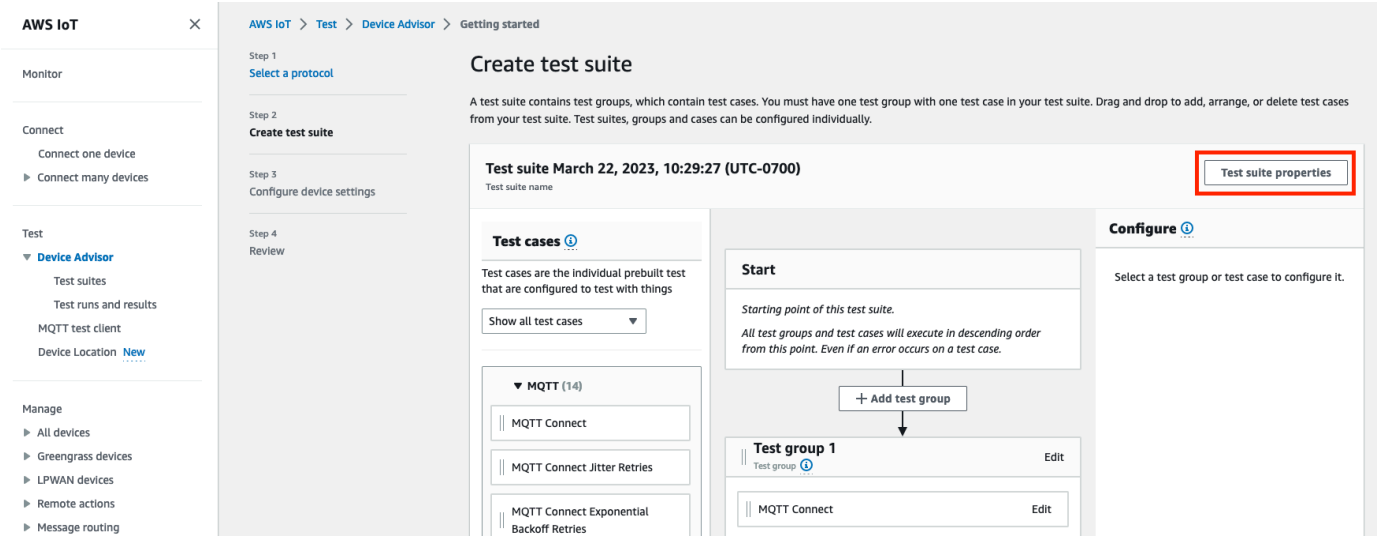


3. Wählen Sie in Schritt 1: Protokoll auswählen ein Protokoll aus den aufgelisteten Optionen aus. Wählen Sie anschließend Weiter.




4. In Schritt 2 erstellen und konfigurieren Sie eine benutzerdefinierte Testsuite. Eine benutzerdefinierte Testsuite muss mindestens eine Testgruppe haben und jede Testgruppe muss mindestens einen Testfall haben. Wir haben den MQTTConnect-Testfall hinzugefügt, damit Sie loslegen können.

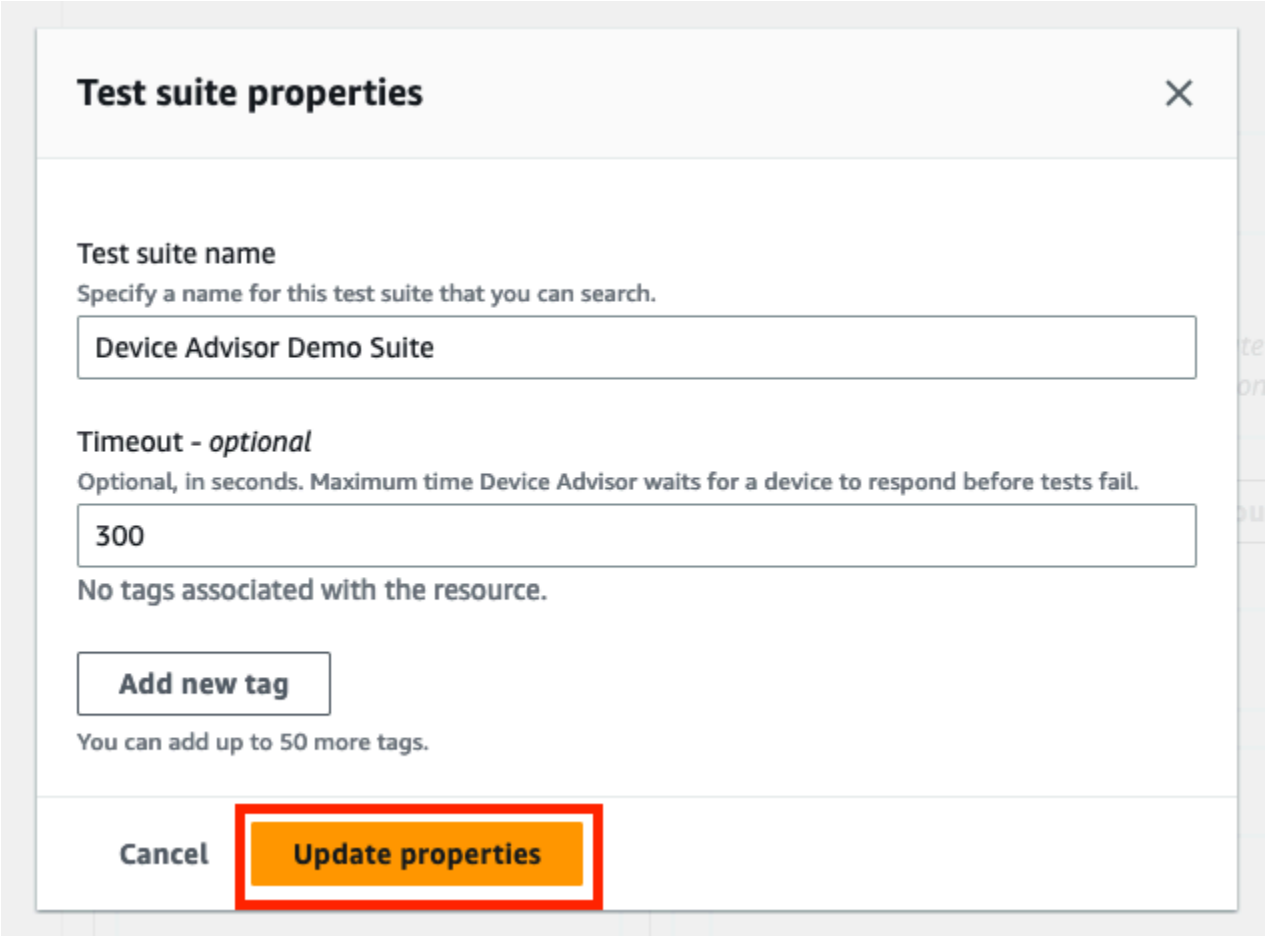
   Wählen Sie Eigenschaften der Testsuite aus.




   Geben Sie die Eigenschaften der Testsuite an, wenn Sie Ihre Testsuite erstellen. Sie können die folgenden Eigenschaften auf Suite-Ebene konfigurieren:

   - Name der Testsuite: Geben Sie einen Namen für Ihre Testsuite ein.
   - Timeout (optional): Das Timeout (in Sekunden) für jeden Testfall in der aktuellen Testsuite. Wenn Sie keinen Timeout-Wert angeben, wird der Standardwert verwendet.
   - Tags (optional): Fügen Sie der Testsuite Tags hinzu.

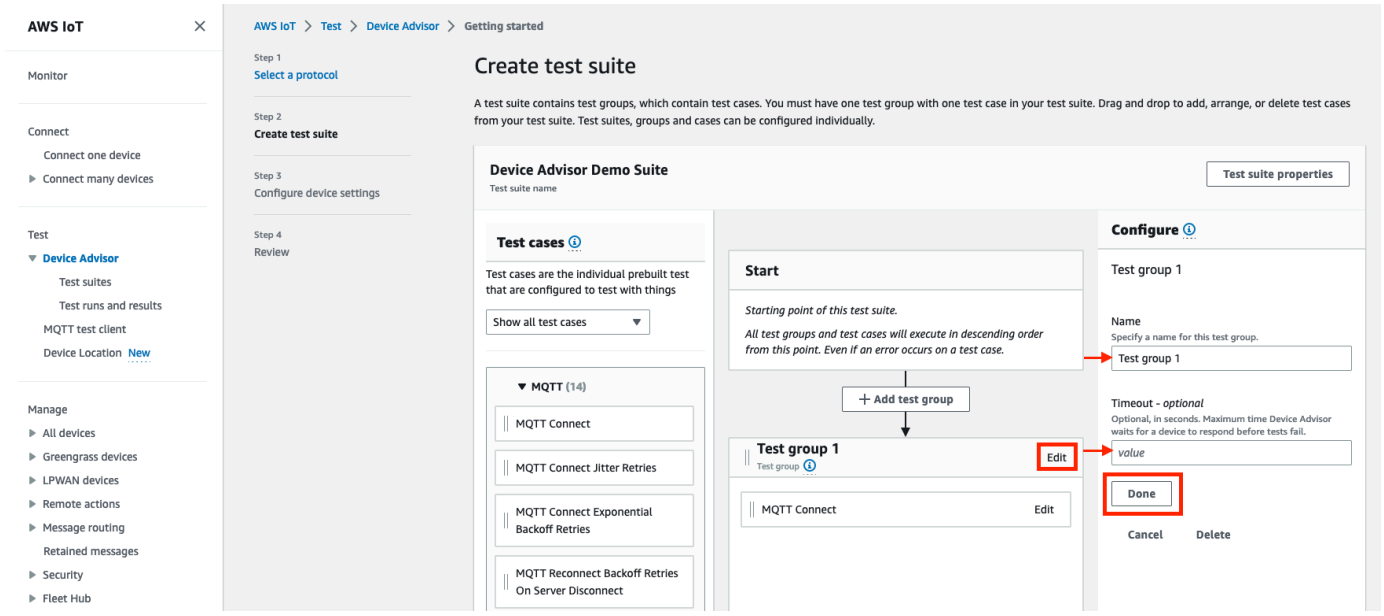
Wenn Sie fertig sind, wählen Sie Eigenschaften aktualisieren aus.




5. (Optional) Um die Konfiguration der Testsuite-Gruppe zu aktualisieren, klicken Sie auf die Schaltfläche Bearbeiten neben dem Namen der Testgruppe.

   - Name: Geben Sie einen Namen für die Testsuite-Gruppe ein.
   - Timeout (optional): Das Timeout (in Sekunden) für jeden Testfall in der aktuellen Testsuite. Wenn Sie keinen Timeout-Wert angeben, wird der Standardwert verwendet.

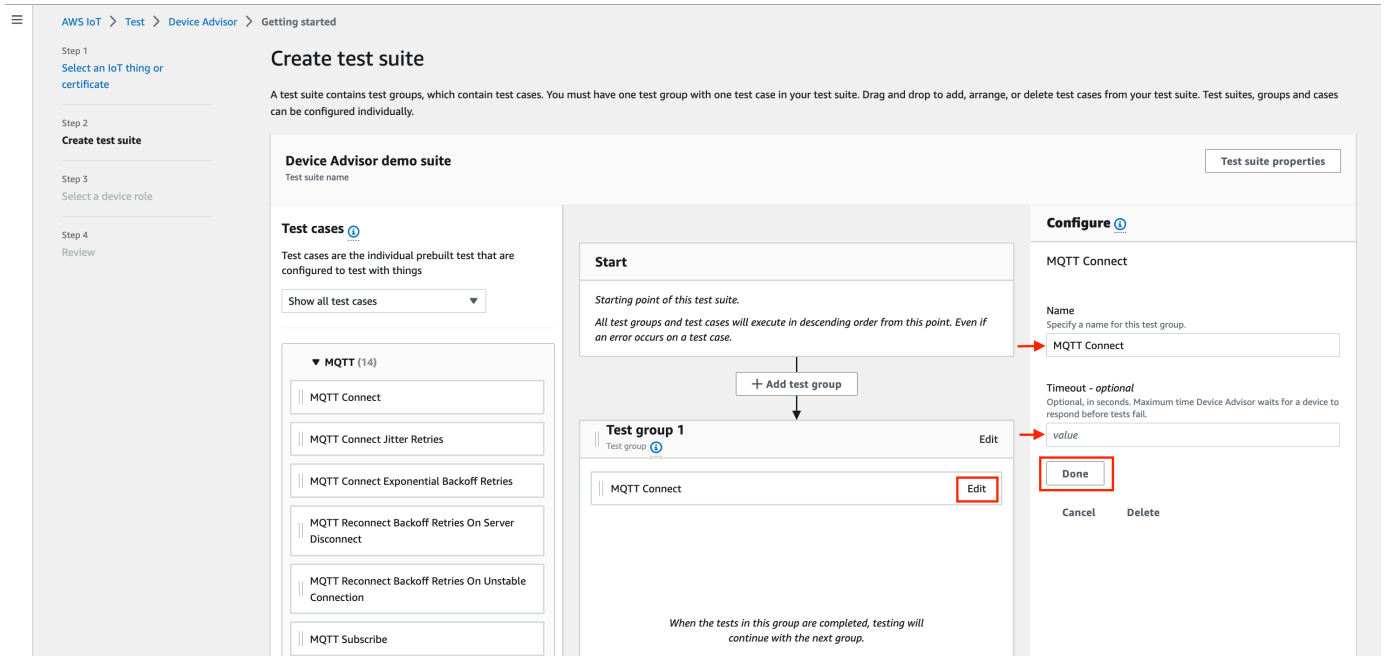
   Wenn Sie fertig sind, wählen Sie Fertig aus, um fortzufahren.



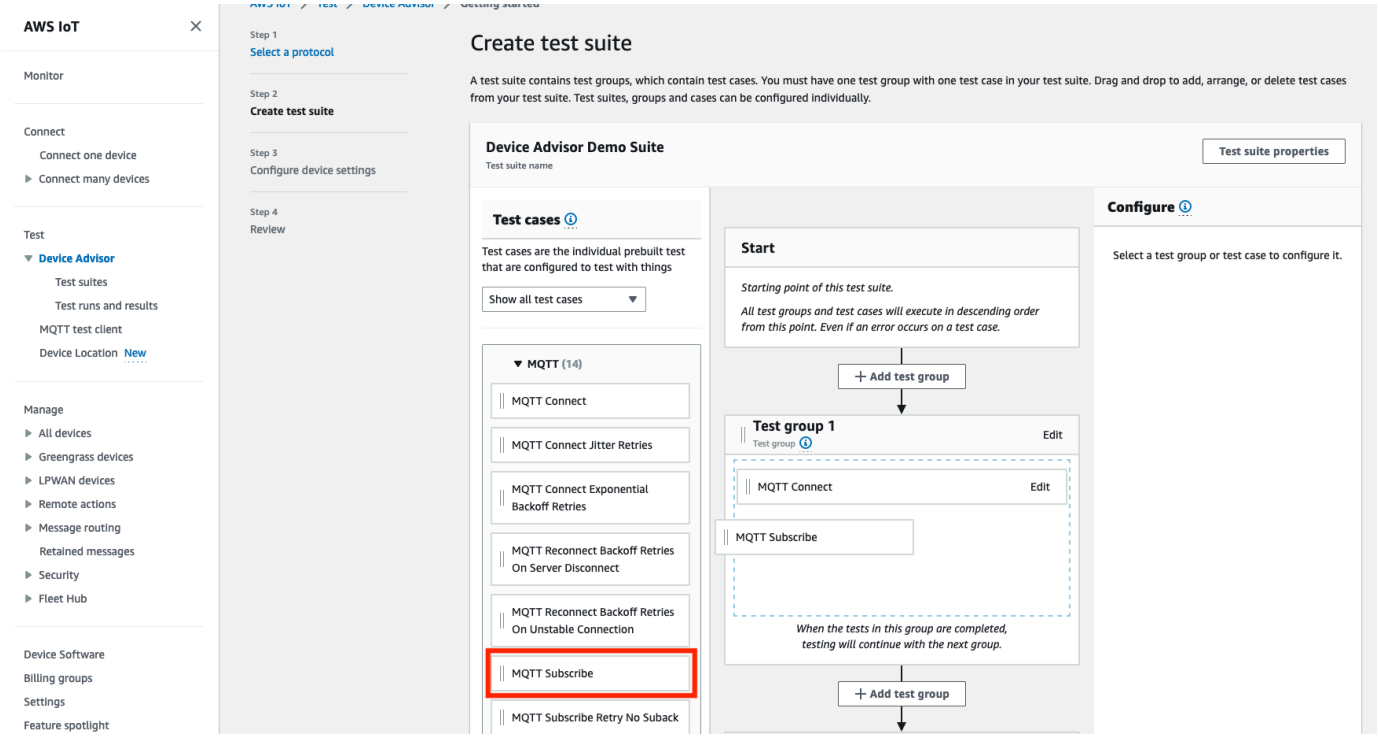

6. (Optional) Um die Testfall-Konfiguration für einen Testfall zu aktualisieren, klicken Sie auf die Schaltfläche Bearbeiten neben dem Namen der Testgruppe.

   - Name: Geben Sie einen Namen für die Testsuite-Gruppe ein.
   - Timeout (optional): Das Timeout (in Sekunden) für den ausgewählten Testfall. Wenn Sie keinen Timeout-Wert angeben, wird der Standardwert verwendet.

   Wenn Sie fertig sind, wählen Sie Fertig aus, um fortzufahren.

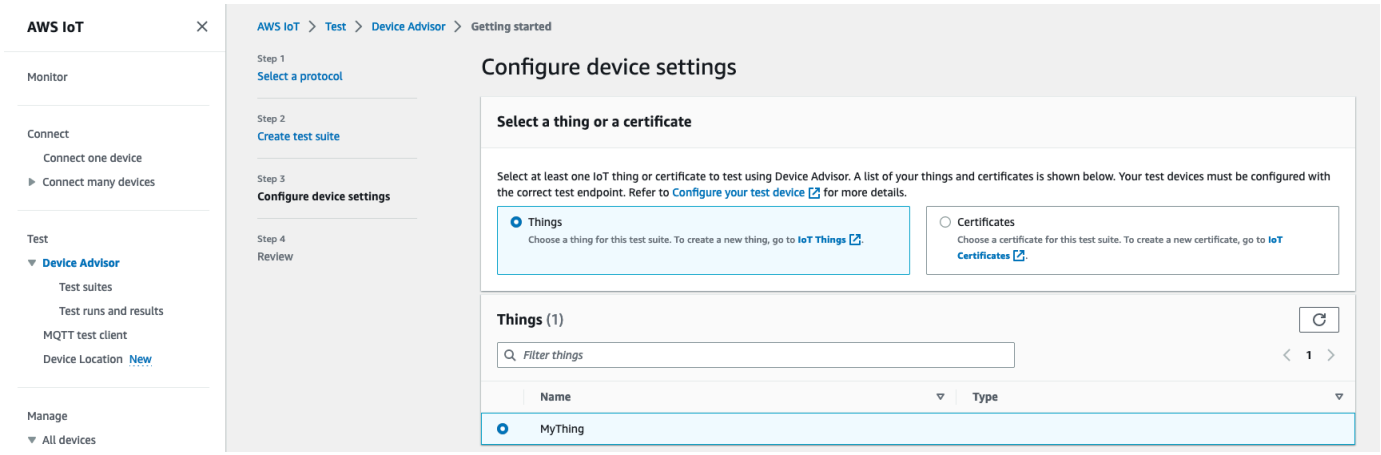


7. (Optional) Um der Testsuite weitere Testgruppen hinzuzufügen, wählen Sie Add test group (Testgruppe hinzufügen) aus und folgen Sie dann den Anweisungen in Schritt 5.
8. (Optional) Um weitere Testfälle hinzuzufügen, ziehen Sie die Testfälle im Abschnitt Testfälle in eine Ihrer Testgruppen.



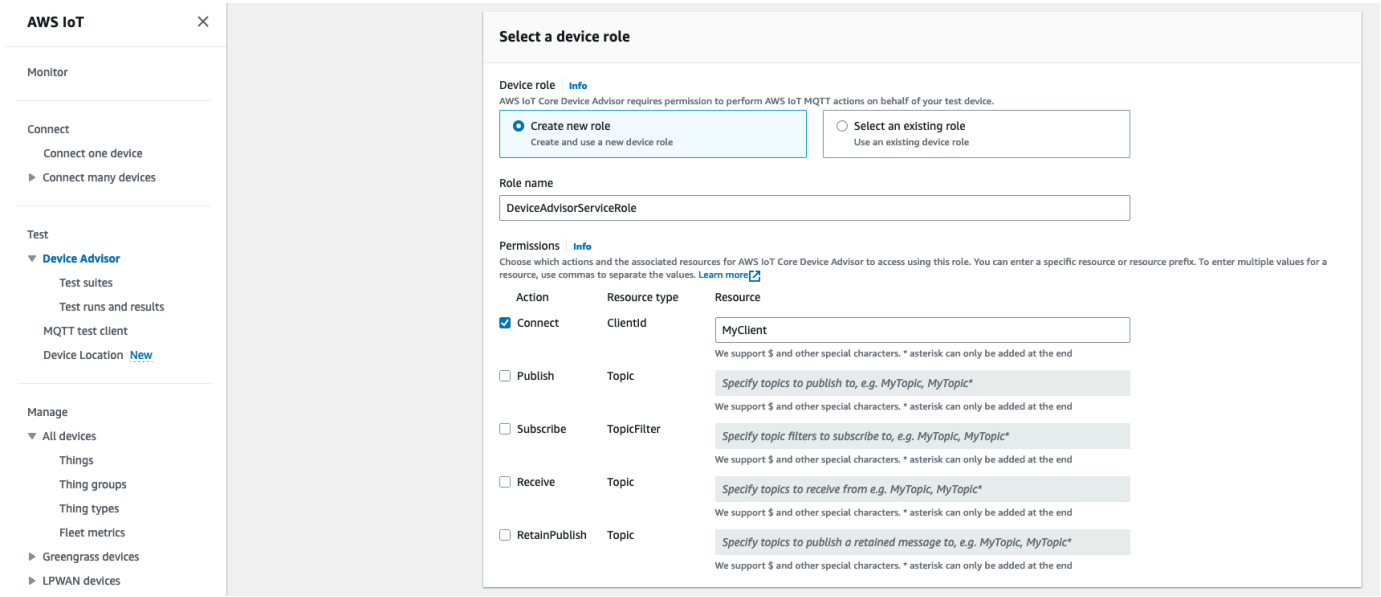

9. Sie können die Reihenfolge Ihrer Testgruppen und Testfälle ändern. Ziehen Sie die aufgelisteten Testfälle in der Liste nach oben oder unten, um Änderungen vorzunehmen. Device Advisor führt Tests in der Reihenfolge aus, in der Sie sie aufgelistet haben.

   Nachdem Sie Ihre Testsuite konfiguriert haben, wählen Sie Weiter aus.
10. Wählen Sie in Schritt 3 eine AWS IoT Sache oder ein Zertifikat aus, das mit Device Advisor getestet werden soll. Wenn Sie noch keine Dinge oder Zertifikate haben, finden Sie weitere Informationen unter Einrichten.

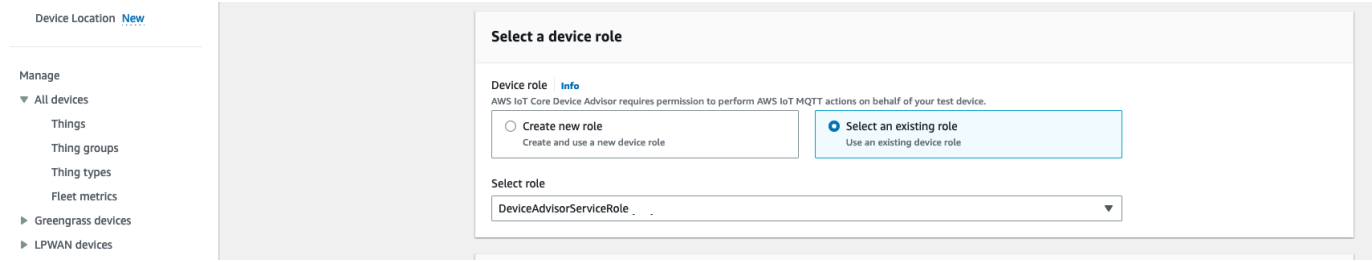



11. Sie können eine Geräterolle konfigurieren, die Device Advisor verwendet, um AWS IoT MQTT Aktionen im Namen Ihres Testgeräts auszuführen. Nur für den MQTTConnect-Testfall wird die Aktion Connect automatisch ausgewählt. Dies liegt daran, dass die Geräterolle diese Berechtigung benötigt, um die Testsuite auszuführen. Für andere Testfälle werden die entsprechenden Aktionen ausgewählt.

    Geben Sie die Ressourcenwerte für jede der ausgewählten Aktionen an. Geben Sie beispielsweise für die Connect-Aktion die Client-ID an, die Ihr Gerät für die Verbindung mit dem Device-Advisor-Endpunkt verwendet. Sie können mehrere Werte mit durch Kommas getrennten Werten und Präfixwerte mit einem Platzhalterzeichen (*) angeben. Um beispielsweise die Erlaubnis zur Veröffentlichung zu einem beliebigen Thema zu erteilen, das mit `MyTopic` beginnt, geben Sie **`MyTopic*`** als Ressourcenwert ein.

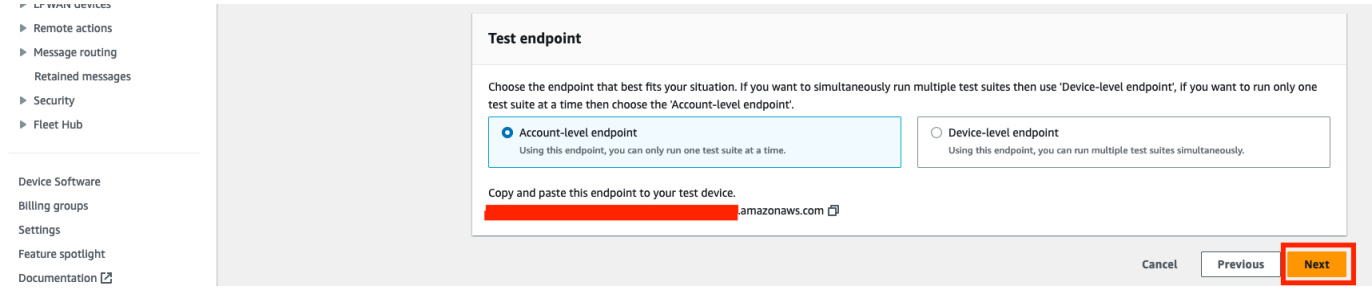


Um eine zuvor erstellte Geräterolle aus Einrichten zu verwenden, wählen Sie Vorhandene Rolle auswählen aus. Wählen Sie dann unter Rolle auswählen Ihre Geräterolle aus.



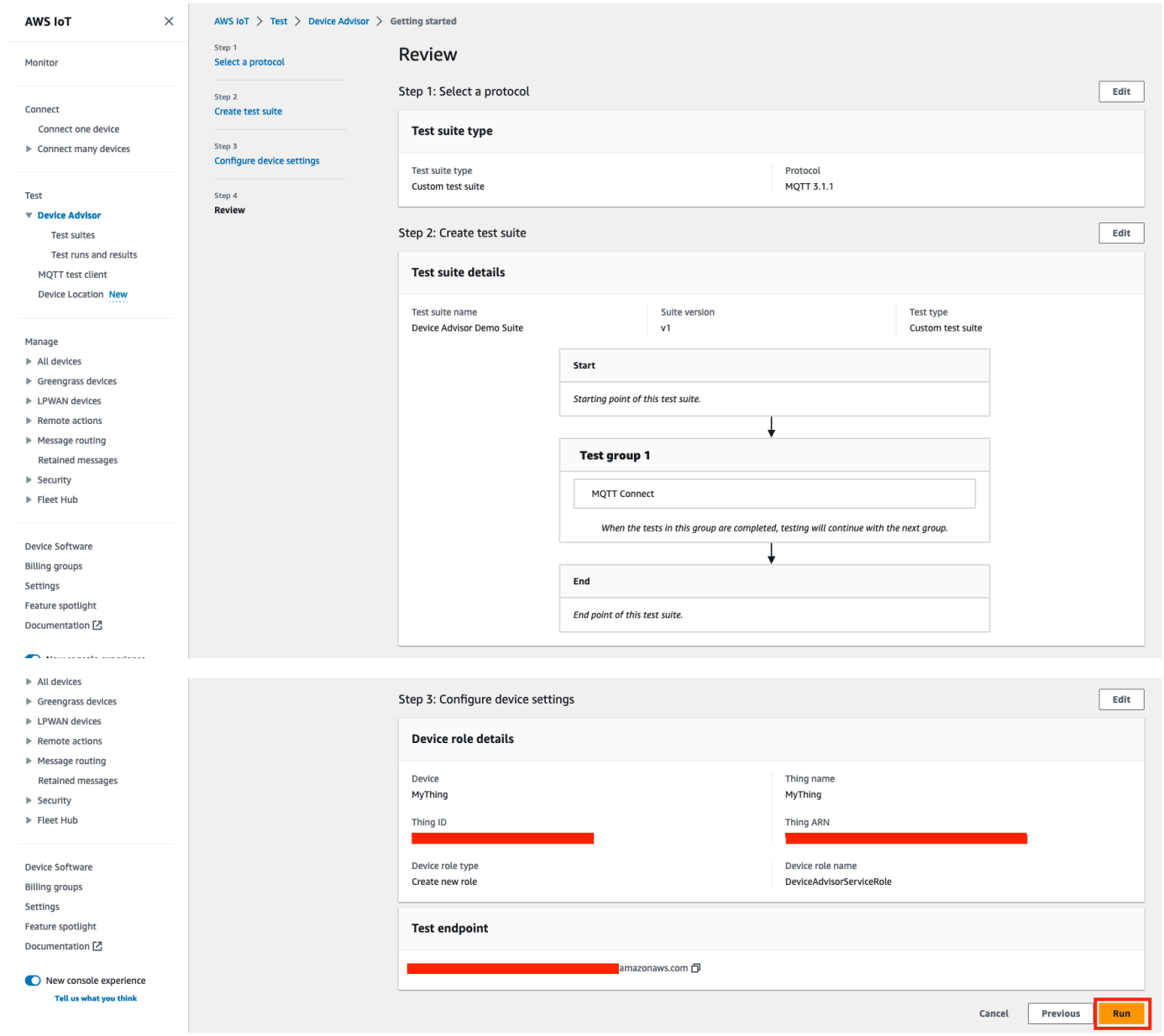

Konfigurieren Sie Ihre Geräterolle mit einer der beiden verfügbaren Optionen und wählen Sie dann Weiter aus.

12. Wählen Sie im Abschnitt Testendpunkt den Endpunkt aus, der am besten zu Ihrem Anwendungsfall passt. Um mehrere Testsuiten gleichzeitig mit derselben auszuführen AWS-Konto, wählen Sie Endpunkt auf Geräteebene. Wählen Sie Endpunkt auf Kontoebene aus, um jeweils eine Testsuite auszuführen.

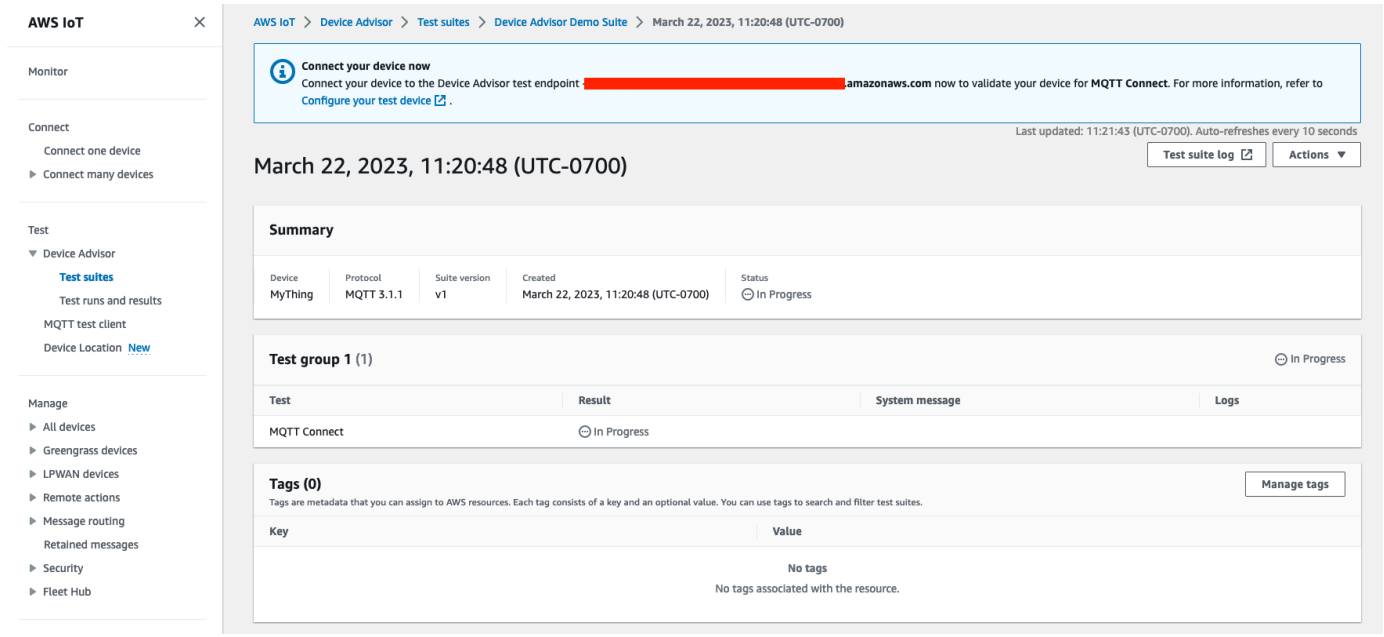



13. Schritt 4 zeigt eine Übersicht über das ausgewählte Testgerät, den Testendpunkt, die Testsuite und die konfigurierte Testgeräterolle. Wählen Sie die Schaltfläche Bearbeiten für jeden Abschnitt aus, den Sie bearbeiten möchten, um Änderungen vorzunehmen. Nachdem Sie Ihre Testkonfiguration bestätigt haben, wählen Sie Ausführen aus, um die Testsuite zu erstellen und Ihre Tests auszuführen.

> **Note**
>
> Zum Erzielen optimaler Ergebnisse können Sie Ihr ausgewähltes Testgerät mit dem Device-Advisor-Testendpunkt verbinden, bevor Sie mit der Ausführung der Testsuite beginnen. Wir empfehlen, dass Sie für Ihr Gerät einen Mechanismus entwickeln, mit dem Sie alle fünf Sekunden bis zu ein bis zwei Minuten lang versuchen können, eine Verbindung zu unserem Testendpunkt herzustellen.




14. Wählen Sie im Navigationsbereich unter Test die Option Device Advisor und dann Testläufe und Ergebnisse aus. Wählen Sie eine Testsuite-Ausführung aus, um deren Ausführungsdetails und Protokolle anzuzeigen.




15. Um auf die CloudWatch Amazon-Logs für die Suite zuzugreifen, führe folgenden Befehl aus:

    - Wählen Sie Test Suite Log, um die CloudWatch Protokolle für den Test Suite-Lauf anzuzeigen.
    - Wählen Sie Testfallprotokoll für einen beliebigen Testfall aus, um testfallspezifische CloudWatch Protokolle anzuzeigen.

16. Führen Sie auf der Grundlage Ihrer Testergebnisse eine Fehlerbehebung auf Ihrem Gerät durch, bis alle Tests bestanden sind.

# Device-Advisor-Workflow

In diesem Tutorial wird erklärt, wie Sie eine benutzerdefinierte Testsuite erstellen und Tests für das Gerät ausführen, das Sie in der Konsole testen möchten. Nach Abschluss der Tests können Sie die Testergebnisse und detaillierte Protokolle anzeigen.

## Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, führen Sie die unter Einrichtung beschriebenen Schritte aus.

## Erstellen einer Testsuite-Definition

Installieren Sie zunächst eine AWS SDK.

## **rootGroup**-Syntax

Eine Stammgruppe ist eine JSON Zeichenfolge, die angibt, welche Testfälle in Ihre Testsuite aufgenommen werden sollen. Sie spezifiziert auch alle erforderlichen Konfigurationen für diese Testfälle. Verwenden Sie die Root-Gruppe, um Ihre Testsuite nach Ihren Bedürfnissen zu strukturieren und zu ordnen. Die Hierarchie einer Testsuite ist folgende:

```
test suite # test group(s) # test case(s)
```

Eine Testsuite muss mindestens eine Testgruppe haben und jede Testgruppe muss mindestens einen Testfall haben. Device Advisor führt Tests in der Reihenfolge aus, in der Sie die Testgruppen und Testfälle definieren.

Jede Root-Gruppe folgt dieser Grundstruktur:

```
{
    "configuration": {  // for all tests in the test suite
        "": ""
    }
    "tests": [{
        "name": ""
        "configuration": {  // for all sub-groups in this test group
            "": ""
        },
        "tests": [{
            "name": ""
            "configuration": {  // for all test cases in this test group
                "": ""
            },
            "test": {
                "id": ""
                "version": ""
            }
        }]
    }]
}
```

In der Root-Gruppe definieren Sie die Testsuite mit einem `name`, der `configuration` und den `tests`, die die Gruppe enthält. Die `tests`-Gruppe enthält die Definitionen der einzelnen Tests. Sie definieren jeden Test mit einem `name`, einer `configuration` und einem `test`-Block, der die

Testfälle für diesen Test definiert. Schließlich wird jeder Testfall mit einer `id` und einer `version` definiert.

Hinweise zur Verwendung der Felder `"id"` und `"version"` und für jeden Testfall (`test`-Block) finden Sie unter Device-Advisor-Testfälle. Dieser Abschnitt enthält auch Informationen zu den verfügbaren `configuration`-Einstellungen.

Der folgende Block ist ein Beispiel für eine Root-Gruppenkonfiguration. Diese Konfiguration spezifiziert die Testfälle MQTTConnect Happy Case und MQTTConnect Exponential Backoff Retries zusammen mit Beschreibungen der Konfigurationsfelder.

```
{
    "configuration": {},  // Suite-level configuration
    "tests": [            // Group definitions should be provided here
      {
        "name": "My_MQTT_Connect_Group",  // Group definition name
        "configuration": {}               // Group definition-level configuration,
        "tests": [                        // Test case definitions should be provided
 here
        {
            "name": "My_MQTT_Connect_Happy_Case",  // Test case definition name
            "configuration": {
                "EXECUTION_TIMEOUT": 300        // Test case definition-level
 configuration, in seconds
            },
            "test": {
                "id": "MQTT_Connect",              // test case id
                "version": "0.0.0"                 // test case version
            }
        },
        {
            "name": "My_MQTT_Connect_Jitter_Backoff_Retries",  // Test case definition
 name
            "configuration": {
                "EXECUTION_TIMEOUT": 600                // Test case definition-level
 configuration,  in seconds
            },
            "test": {
                "id": "MQTT_Connect_Jitter_Backoff_Retries",  // test case id
                "version": "0.0.0"                                  // test case version
            }
        }]
    }]
```

```
}
```

Sie müssen die Root-Gruppenkonfiguration angeben, wenn Sie Ihre Testsuite-Definition erstellen. Speichern Sie die `suiteDefinitionId`, die im Antwortobjekt zurückgegeben wird. Sie können diese ID verwenden, um Ihre Testsuite-Definitionsinformationen abzurufen und Ihre Testsuite auszuführen.

Hier ist ein Java-Beispiel: SDK

```
response = iotDeviceAdvisorClient.createSuiteDefinition(
        CreateSuiteDefinitionRequest.builder()
            .suiteDefinitionConfiguration(SuiteDefinitionConfiguration.builder()
                .suiteDefinitionName("your-suite-definition-name")
                .devices(
                    DeviceUnderTest.builder()
                        .thingArn("your-test-device-thing-arn")
                        .certificateArn("your-test-device-certificate-arn")
                        .deviceRoleArn("your-device-role-arn") //if using SigV4 for
 MQTT over WebSocket
                        .build()
                )
                .rootGroup("your-root-group-configuration")
                .devicePermissionRoleArn("your-device-permission-role-arn")
                .protocol("MqttV3_1_1 || MqttV5 || MqttV3_1_1_OverWebSocket ||
 MqttV5_OverWebSocket")
                .build()
            )
            .build()
)
```

## Abrufen einer Testsuite-Definition

Nachdem Sie Ihre Testsuite-Definition erstellt haben, erhalten Sie `suiteDefinitionId` im Antwortobjekt der `CreateSuiteDefinition` API Operation das Objekt.

Wenn der Vorgang die `suiteDefinitionId` zurückgibt, sehen Sie möglicherweise neue `id`-Felder in jeder Gruppe und eine Testfalldefinition innerhalb der Root-Gruppe. Sie können diese verwendenIDs, um eine Teilmenge Ihrer Testsuite-Definition auszuführen.

SDKJava-Beispiel:

```
response = iotDeviceAdvisorClient.GetSuiteDefinition(
```

```
    GetSuiteDefinitionRequest.builder()
        .suiteDefinitionId("your-suite-definition-id")
        .build()
)
```

## Abrufen eines Testendpunkts

Verwenden Sie den `GetEndpoint` API Vorgang, um den von Ihrem Gerät verwendeten Testendpunkt abzurufen. Wählen Sie den Endpunkt aus, der am besten zu Ihrem Test passt. Um mehrere Testsuiten gleichzeitig auszuführen, verwenden Sie den Endpunkt auf Geräteebene, indem Sie einen `thing ARN`, `certificate ARN` oder `device role ARN` angeben. Um eine einzelne Testsuite auszuführen, geben Sie keine Argumente für den GetEndpoint Vorgang zur Auswahl des Endpunkts auf Kontoebene an.

SDKBeispiel:

```
response = iotDeviceAdvisorClient.getEndpoint(GetEndpointRequest.builder()
.certificateArn("your-test-device-certificate-arn")
.thingArn("your-test-device-thing-arn")
.deviceRoleArn("your-device-role-arn") //if using SigV4 for MQTT over WebSocket

.build())
```

## Ausführen einer Testsuite

Nachdem Sie eine Testsuite-Definition erstellt und Ihr Testgerät so konfiguriert haben, dass es eine Verbindung zu Ihrem Device Advisor-Testendpunkt herstellt, führen Sie Ihre Testsuite mit dem aus. `StartSuiteRun` API

MQTTKunden können entweder `certificateArn` oder verwenden, `thingArn` um die Testsuite auszuführen. Wenn beide konfiguriert sind, wird das Zertifikat verwendet, wenn es zum Ding gehört.

Verwenden Sie für MQTT mehr WebSocket Kunden, `deviceRoleArn` um die Testsuite auszuführen. Wenn sich die angegebene Rolle von der in der Testsuite-Definition angegebenen Rolle unterscheidet, hat die angegebene Rolle Vorrang vor der definierten Rolle.

Verwenden Sie für `.parallelRun()` `true`, wenn Sie einen Endpunkt auf Geräteebene verwenden, um mehrere Testsuiten parallel mit einem AWS-Konto auszuführen.

SDKBeispiel:

```
response = iotDeviceAdvisorClient.startSuiteRun(StartSuiteRunRequest.builder()
.suiteDefinitionId("your-suite-definition-id")
.suiteRunConfiguration(SuiteRunConfiguration.builder()
    .primaryDevice(DeviceUnderTest.builder()
        .certificateArn("your-test-device-certificate-arn")
        .thingArn("your-test-device-thing-arn")
        .deviceRoleArn("your-device-role-arn") //if using SigV4 for MQTT over WebSocket

        .build())
    .parallelRun(true | false)
    .build())
.build())
```

Speichern Sie die `suiteRunId` aus der Antwort. Sie werden diese verwenden, um die Ergebnisse dieser Testsuite-Ausführung abzurufen.

## Abrufen einer Testsuite-Ausführung

Nachdem Sie eine Testsuite gestartet haben, können Sie den Fortschritt und die Ergebnisse mit dem überprüfen `GetSuiteRun`API.

SDKBeispiel:

```
// Using the SDK, call the GetSuiteRun API.

response = iotDeviceAdvisorClient.GetSuiteRun(
GetSuiteRunRequest.builder()
    .suiteDefinitionId("your-suite-definition-id")
    .suiteRunId("your-suite-run-id")
.build())
```

## Beenden einer Testsuite-Ausführung

Um einen Testsuite-Lauf zu beenden, der noch läuft, können Sie den `StopSuiteRun` API Vorgang aufrufen. Nachdem Sie die `StopSuiteRun`-Operation aufgerufen haben, startet der Service den Bereinigungsvorgang. Während der Service den Bereinigungsvorgang ausführt, führt die Testsuite Statusaktualisierungen bis `Stopping` durch. Der Bereinigungsvorgang kann mehrere Minuten in Anspruch nehmen. Sobald der Vorgang abgeschlossen ist, führt die Testsuite Statusaktualisierungen bis `Stopped` durch. Nachdem ein Testlauf vollständig beendet wurde, starten Sie eine weitere

Testsuite-Ausführung. Sie können den Status der Ausführung der Suite mithilfe des `GetSuiteRun` API Vorgangs regelmäßig überprüfen, wie im vorherigen Abschnitt gezeigt.

SDKBeispiel:

```
// Using the SDK, call the StopSuiteRun API.

response = iotDeviceAdvisorClient.StopSuiteRun(
StopSuiteRun.builder()
    .suiteDefinitionId("your-suite-definition-id")
    .suiteRunId("your-suite-run-id")
.build())
```

## Abrufen eines Qualifizierungsberichts für eine erfolgreiche Ausführung der Qualifizierungstestsuite

Wenn Sie eine Qualifizierungstestsuite ausführen, die erfolgreich abgeschlossen wurde, können Sie einen Qualifizierungsbericht mit dem `GetSuiteRunReport` API Vorgang abrufen. Sie verwenden diesen Qualifizierungsbericht, um Ihr Gerät für das AWS IoT Core -Qualifizierungsprogramm zu qualifizieren. Um festzustellen, ob es sich bei Ihrer Testsuite um eine Qualifizierungstestsuite handelt, überprüfen Sie, ob der `intendedForQualification`-Parameter auf `true` eingestellt ist. Nachdem Sie den `GetSuiteRunReport` API Vorgang aufgerufen haben, können Sie den Bericht von der zurückgegebenen Datei URL bis zu 90 Sekunden lang herunterladen. Wenn seit dem letzten Aufruf des Vorgangs mehr als 90 Sekunden vergangen sind, rufen Sie den `GetSuiteRunReport` Vorgang erneut auf, um einen neuen, gültigen URL Vorgang abzurufen.

SDKBeispiel:

```
// Using the SDK, call the getSuiteRunReport API.

response = iotDeviceAdvisorClient.getSuiteRunReport(
    GetSuiteRunReportRequest.builder()
        .suiteDefinitionId("your-suite-definition-id")
        .suiteRunId("your-suite-run-id")
        .build()
)
```

# Ausführlicher Konsolen-Workflow von Device Advisor

In diesem Tutorial erstellen Sie eine benutzerdefinierte Testsuite und führen Tests für das Gerät aus, das Sie in der Konsole testen möchten. Nach Abschluss der Tests können Sie die Testergebnisse und detaillierte Protokolle anzeigen.

Tutorials

- Voraussetzungen
- Erstellen einer Testsuite-Definition
- Ausführen einer Testsuite
- Beenden einer Testsuite-Ausführung (optional)
- Anzeigen von Details und Protokolle der Testsuite-Ausführung
- Herunterladen eines AWS IoT -Qualifikationsberichts

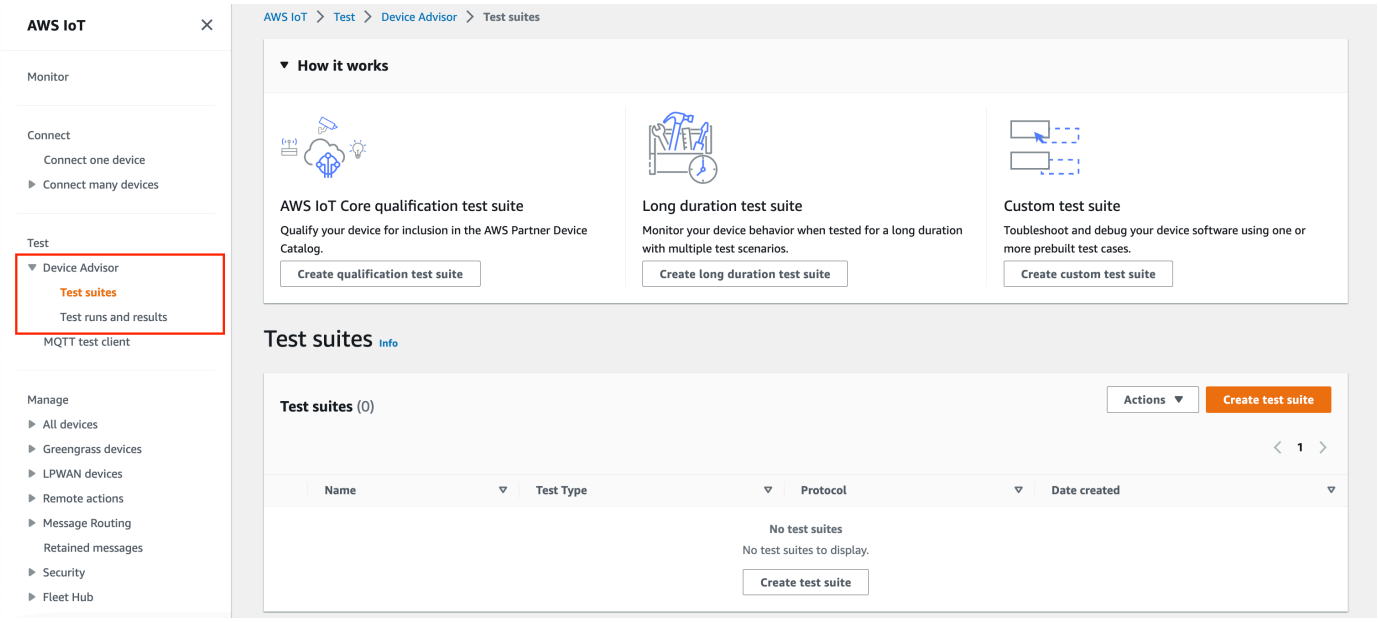
## Voraussetzungen

Sie müssen zuerst ein Ding und ein Zertifikat erstellen, bevor Sie dieses Tutorial abschließen können.

## Erstellen einer Testsuite-Definition

Erstellen Sie eine Testsuite-Suite, damit Sie sie für Ihre Geräte ausführen und die Überprüfung durchführen können.

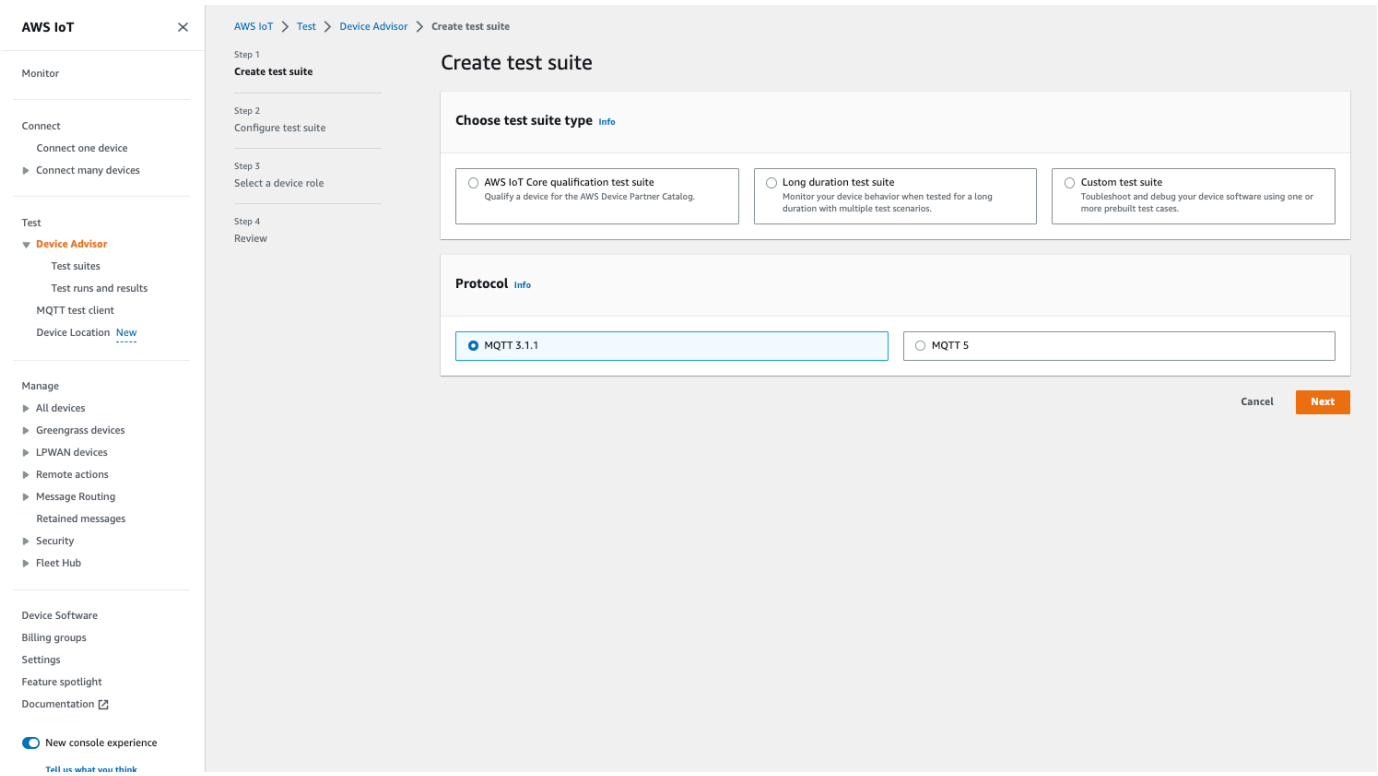
1. Erweitern Sie im Navigationsbereich in der AWS IoT -Konsole die Optionen Test, Device Advisor und wählen Sie dann Testsuites aus.




Wählen Sie Testsuite erstellen aus.

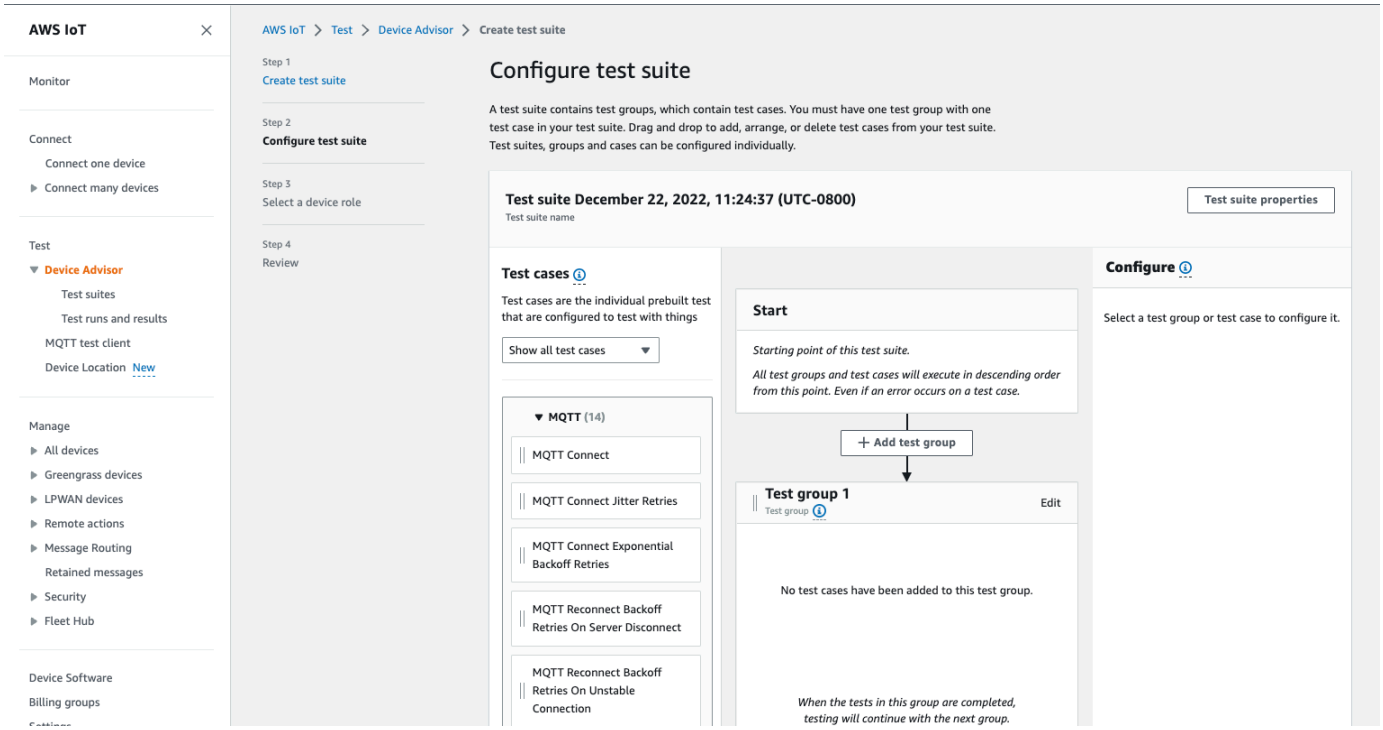
2. Wählen Sie entweder `Use the AWS Qualification test suite` oder `Create a new test suite` aus.

   Wählen Sie als Protokoll entweder MQTT3.1.1 oder MQTT5.

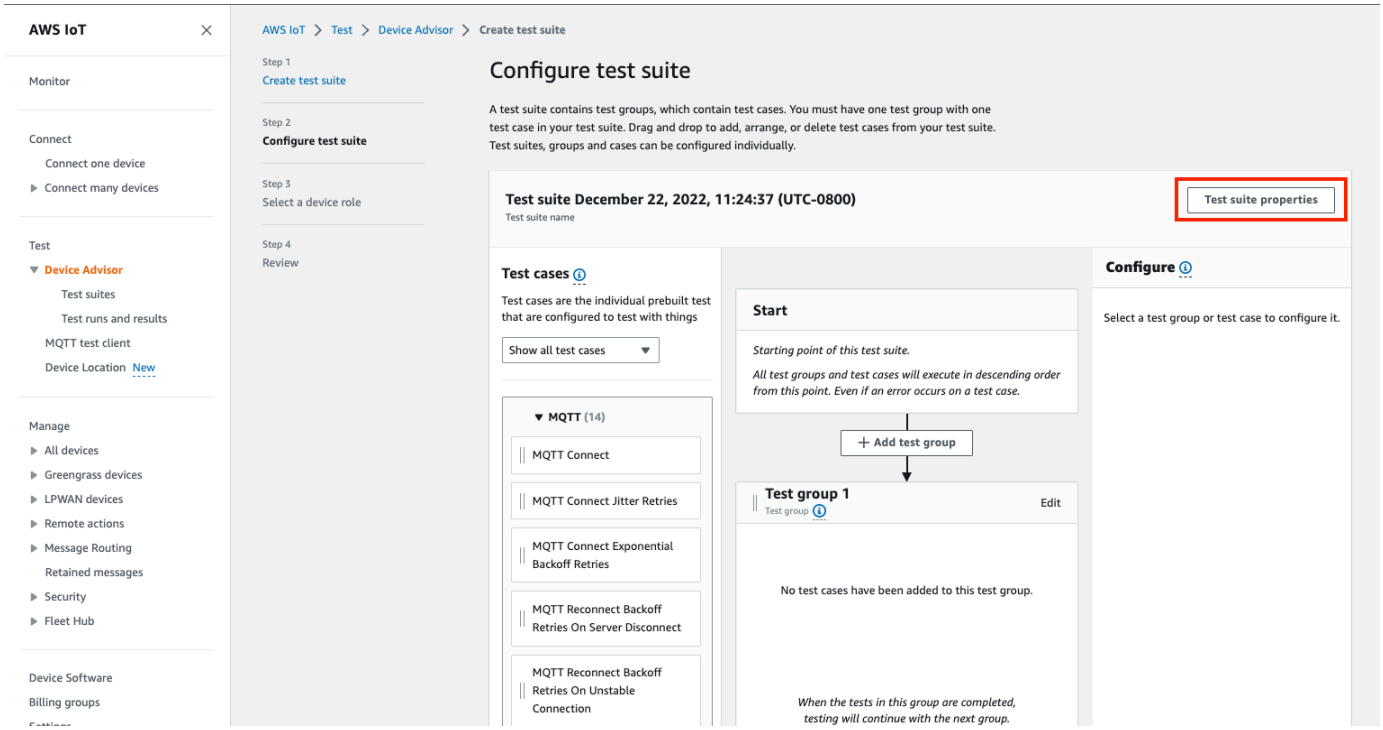


Wählen Sie aus`Use the AWS Qualification test suite`, ob Sie Ihr Gerät qualifizieren und es im Gerätekatalog für AWS Partner auflisten möchten. Wenn Sie diese Option wählen, werden die Testfälle, die für die Qualifizierung Ihres Geräts für das AWS IoT Core - Qualifizierungsprogramm erforderlich sind, vorab ausgewählt. Testgruppen und Testfälle können nicht hinzugefügt oder entfernt werden. Sie müssen trotzdem die Eigenschaften der Testsuite konfigurieren.

Wählen Sie `Create a new test suite` aus, um eine benutzerdefinierte Testsuite zu erstellen und zu konfigurieren. Wir empfehlen, für erste Tests und zur Fehlerbehebung mit dieser Option zu beginnen. Eine benutzerdefinierte Testsuite muss mindestens eine Testgruppe haben und jede Testgruppe muss mindestens einen Testfall haben. Für die Zwecke dieses Tutorials wählen wir diese Option und wählen Weiter aus.

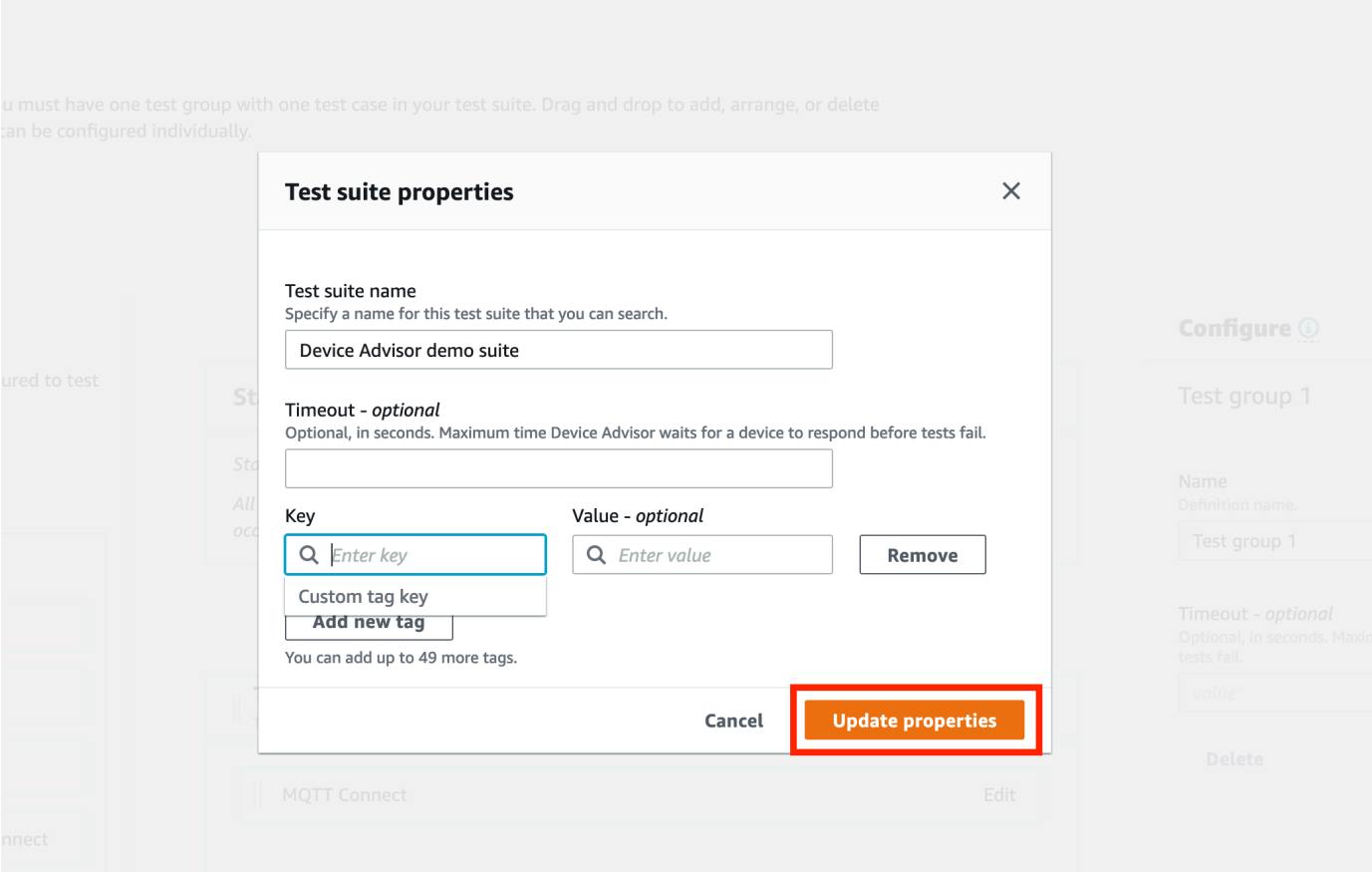



3. Wählen Sie Eigenschaften der Testsuite aus. Sie müssen die Eigenschaften der Testsuite erstellen, wenn Sie Ihre Testsuite erstellen.




Füllen Sie unter Eigenschaften der Testsuite die folgenden Felder aus:

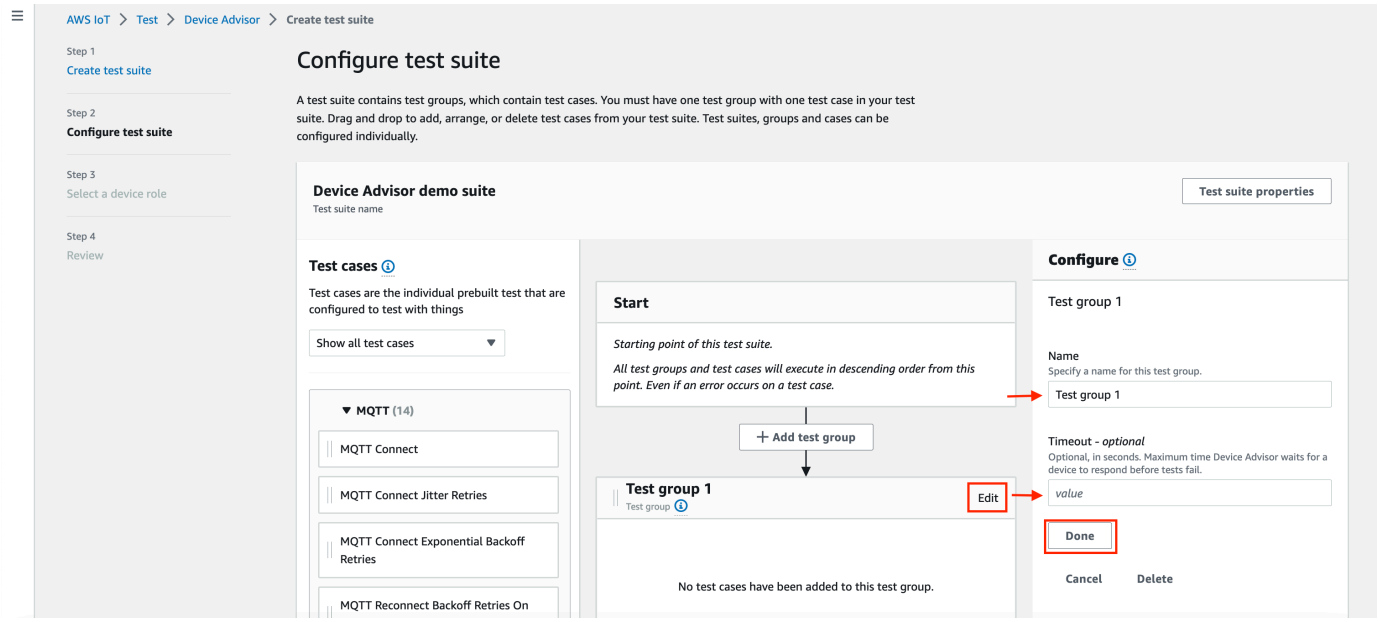
- Name der Testsuite: Sie können die Suite mit einem benutzerdefinierten Namen erstellen.
- Timeout (optional): Das Timeout in Sekunden für jeden Testfall in der aktuellen Testsuite. Wenn Sie keinen Timeout-Wert angeben, wird der Standardwert verwendet.
- Tags (optional): Fügen Sie der Testsuite Tags hinzu.




Wenn Sie fertig sind, wählen Sie Eigenschaften aktualisieren aus.

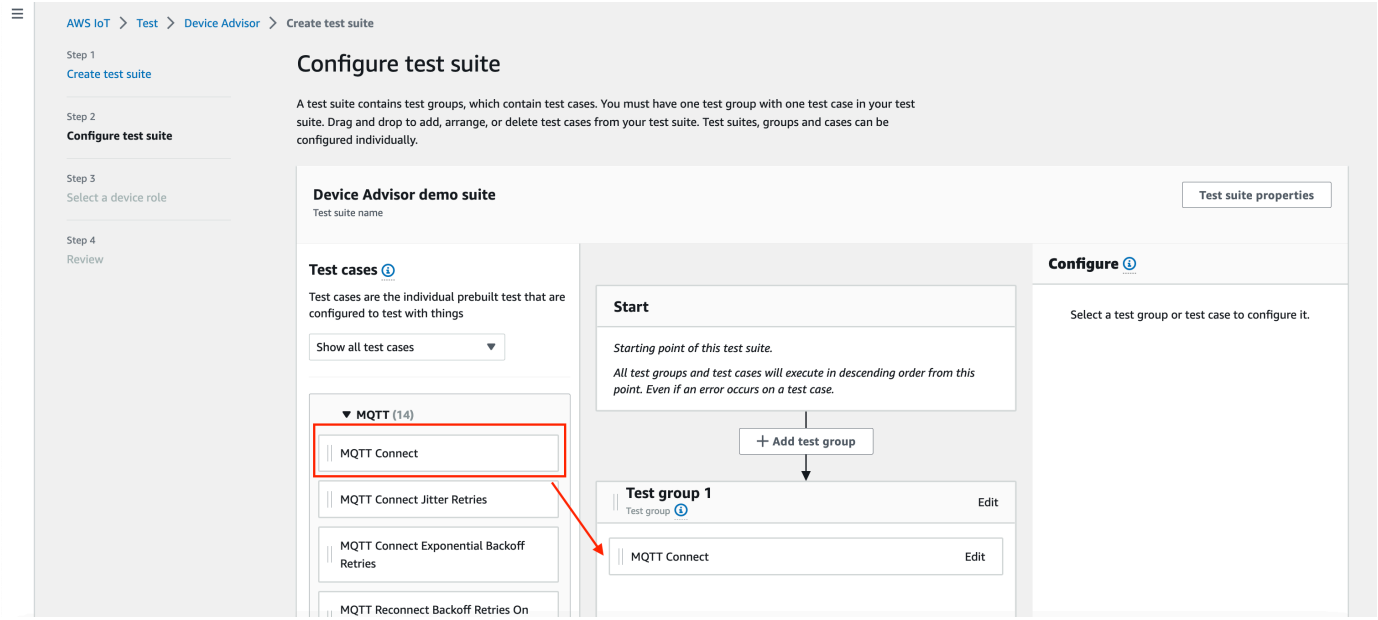
4. Um die Konfiguration auf Gruppenebene zu ändern, wählen Sie unter `Test group 1` Bearbeiten aus. Geben Sie dann einen Namen ein, um der Gruppe einen benutzerdefinierten Namen zu geben.

   Optional können Sie unter der ausgewählten Testgruppe auch einen Timeout-Wert in Sekunden eingeben. Wenn Sie keinen Timeout-Wert angeben, wird der Standardwert verwendet.



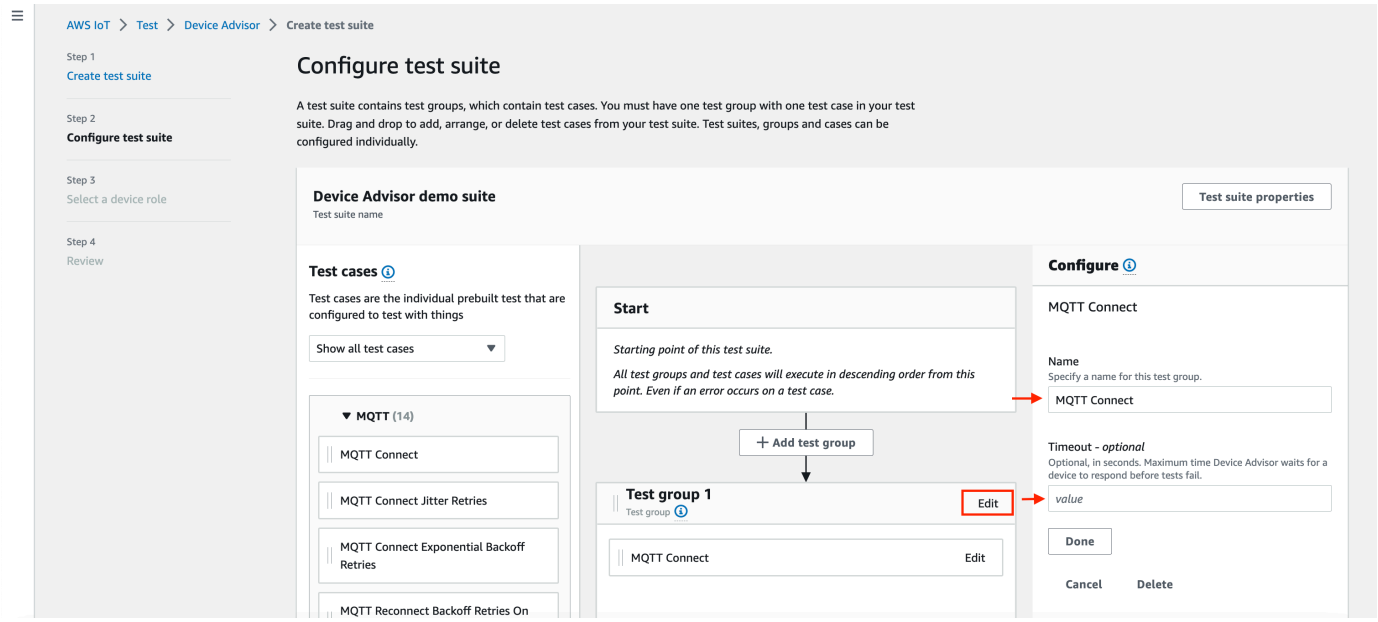

Wählen Sie Erledigt aus.

5. Ziehen Sie einen der verfügbaren Testfälle aus Testfälle in die Testgruppe.




6. Um die Konfiguration auf Testfallebene für den Testfall zu ändern, den Sie Ihrer Testgruppe hinzugefügt haben, wählen Sie Bearbeiten aus. Geben Sie dann einen Namen ein, um der Gruppe einen benutzerdefinierten Namen zu geben.

   Optional können Sie unter der ausgewählten Testgruppe auch einen Timeout-Wert in Sekunden eingeben. Wenn Sie keinen Timeout-Wert angeben, wird der Standardwert verwendet.



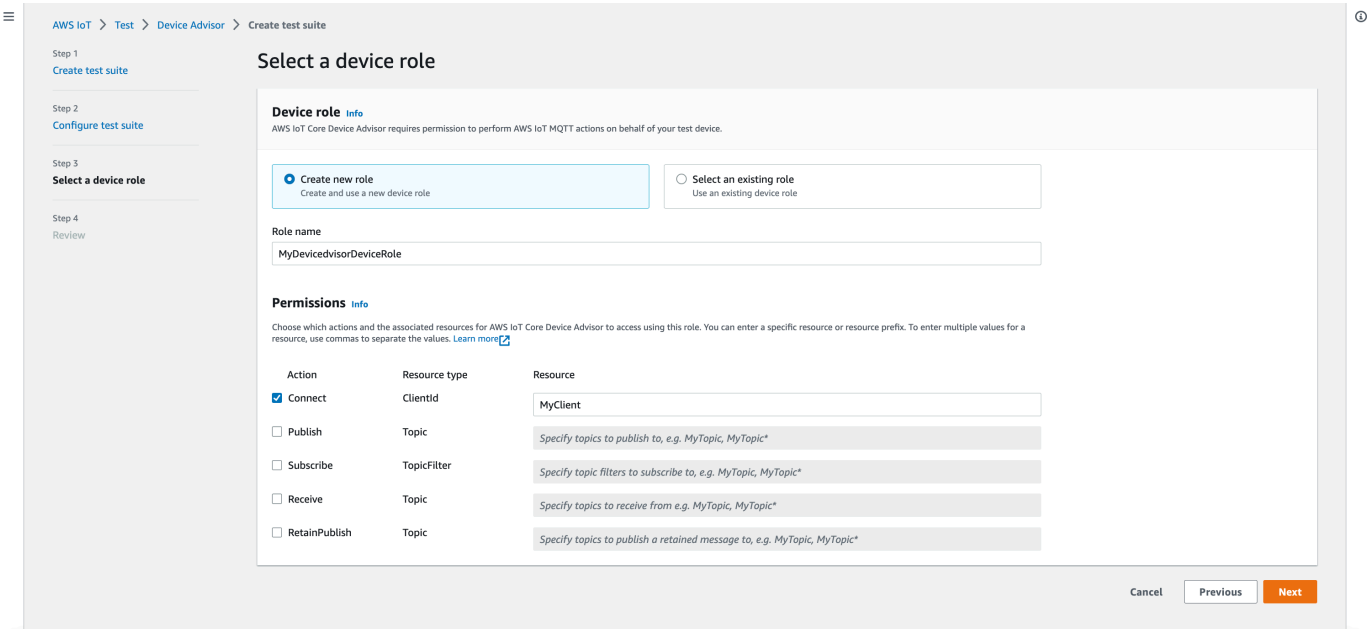

Wählen Sie Erledigt aus.

> **Note**
>
> Um der Testsuite weitere Testgruppen hinzuzufügen, wählen Sie Testgruppe hinzufügen aus. Folgen Sie den vorherigen Schritten, um weitere Testgruppen zu erstellen und zu konfigurieren oder um einer oder mehreren Testgruppen weitere Testfälle hinzuzufügen. Testgruppen und Testfälle können neu angeordnet werden, indem Sie einen Testfall auswählen und an die gewünschte Position ziehen. Device Advisor führt Tests in der Reihenfolge aus, in der Sie die Testgruppen und Testfälle definieren.

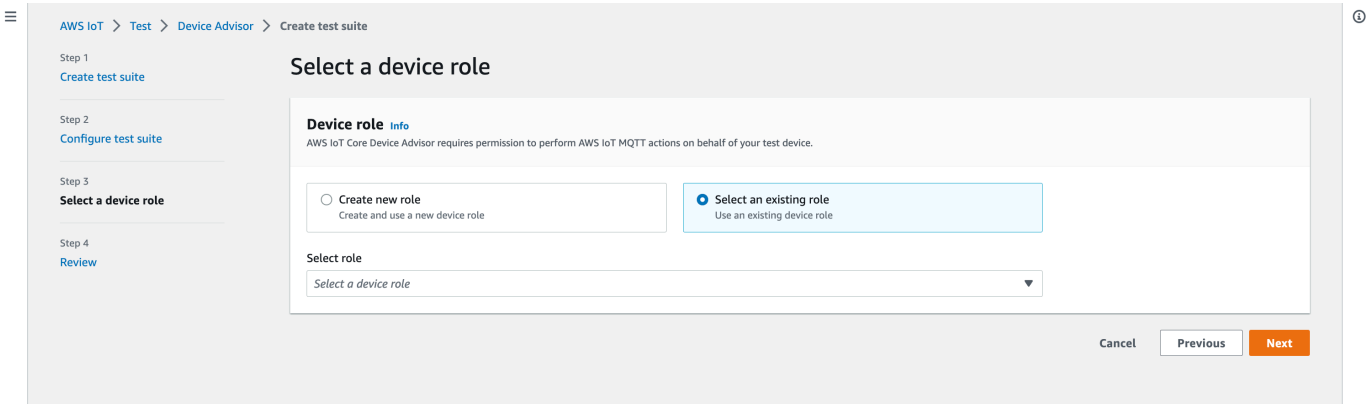
7. Wählen Sie Weiter.
8. Konfigurieren Sie in Schritt 3 eine Geräterolle, die Device Advisor verwendet, um AWS IoT MQTT Aktionen im Namen Ihres Testgeräts auszuführen.

   Wenn Sie in Schritt 2 nur MQTTConnect-Testfall ausgewählt haben, wird die Connect-Aktion automatisch aktiviert, da diese Berechtigung für die Geräterolle erforderlich ist, um diese Testsuite auszuführen. Wenn Sie andere Testfälle ausgewählt haben, werden die entsprechenden erforderlichen Aktionen überprüft. Stellen Sie sicher, dass die Ressourcenwerte für jede der Aktionen angegeben werden. Geben Sie beispielsweise für die Connect-Aktion die Client-ID an, mit der sich Ihr Gerät mit dem Device-Advisor-Endpunkt verbindet. Sie können mehrere Werte angeben, indem Sie die Werte durch Kommas trennen, und Sie können Präfixwerte auch mit einem Platzhalterzeichen (*) angeben. Um beispielsweise die Erlaubnis zur

Veröffentlichung zu einem beliebigen Thema zu erteilen, das mit `MyTopic` beginnt, können Sie „`MyTopic*`“ als Ressourcenwert eingeben.




Wenn Sie bereits zuvor eine Geräterolle erstellt haben und diese Rolle verwenden möchten, wählen Sie Eine vorhandene Rolle auswählen und anschließend unter Rolle auswählen Ihre Geräterolle aus.




Konfigurieren Sie Ihre Geräterolle mit einer der beiden verfügbaren Optionen und wählen Sie dann Weiter aus.

9. Stellen Sie in Schritt 4 sicher, dass die in jedem der Schritte angegebene Konfiguration korrekt ist. Um die für einen bestimmten Schritt bereitgestellte Konfiguration zu bearbeiten, wählen Sie Bearbeiten für den entsprechenden Schritt aus.

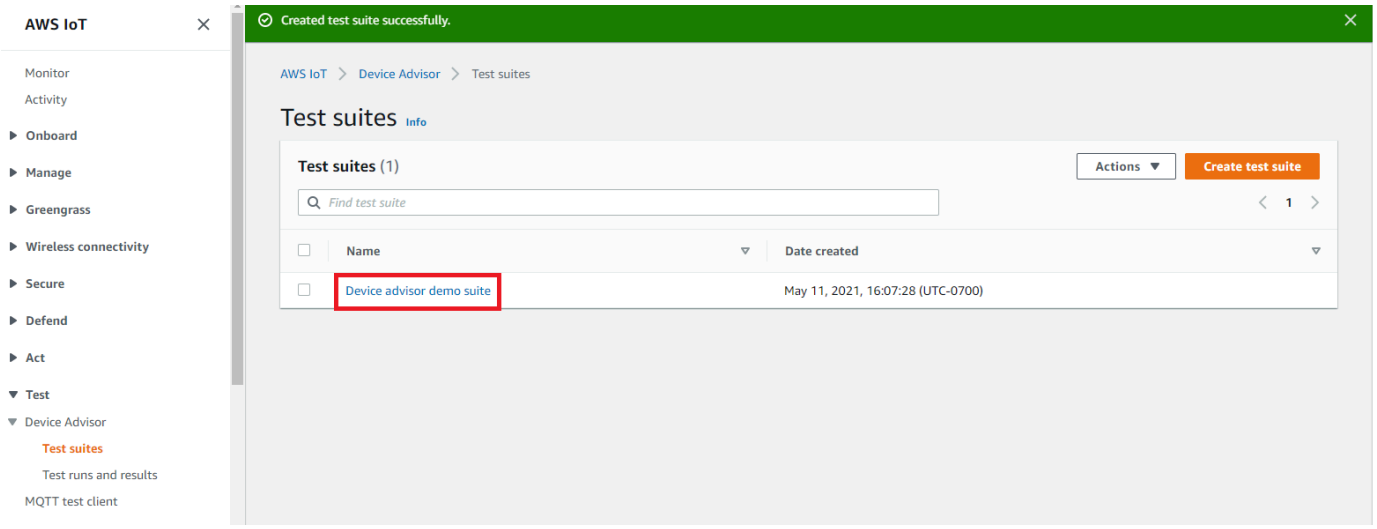
   Nachdem Sie die Konfiguration überprüft haben, wählen Sie Testsuite erstellen aus.

Die Testsuite sollte erfolgreich erstellt worden sein und Sie werden zur Seite Testsuites weitergeleitet, auf der Sie alle erstellten Testsuites anzeigen können.

Wenn die Erstellung der Testsuite fehlgeschlagen ist, stellen Sie sicher, dass die Testsuite, die Testgruppen, die Testfälle und die Geräterolle gemäß den vorherigen Anweisungen konfiguriert wurden.

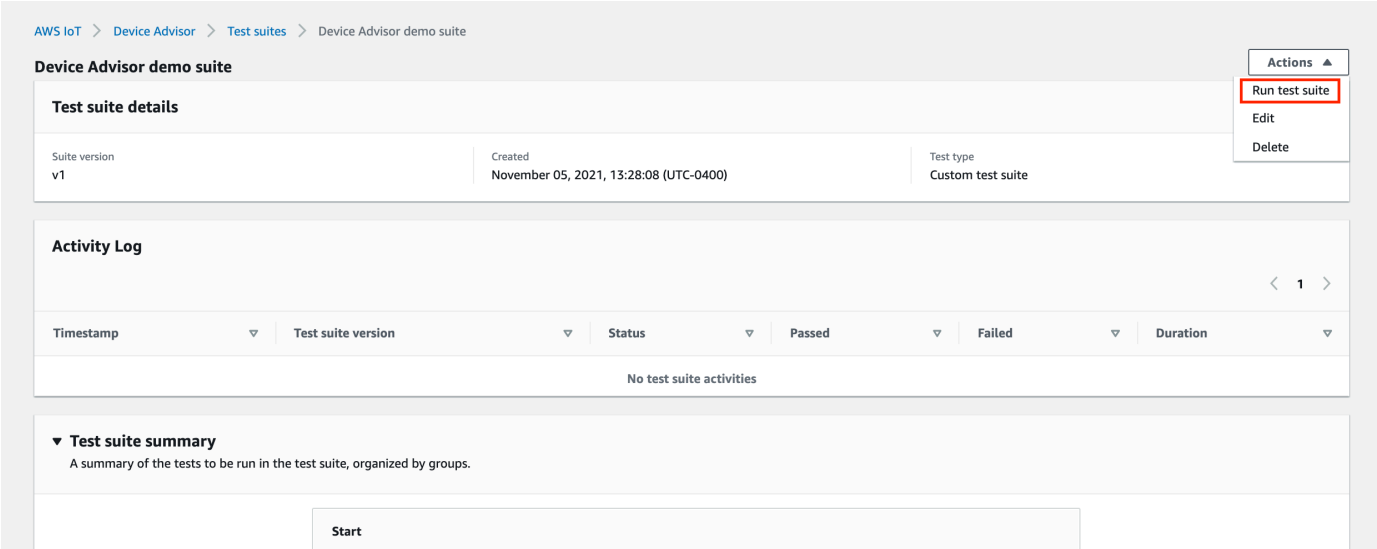
## Ausführen einer Testsuite

1. Erweitern Sie im Navigationsbereich in der AWS IoT -Konsole die Optionen Test, Device Advisor und wählen Sie dann Testsuites aus.
2. Wählen Sie die Testsuite aus, für die Sie die Details der Testsuite anzeigen möchten.




Auf der Detailseite der Testsuite werden alle Informationen zur Testsuite angezeigt.

3. Wählen Sie Aktionen und dann Testsuite ausführen aus.

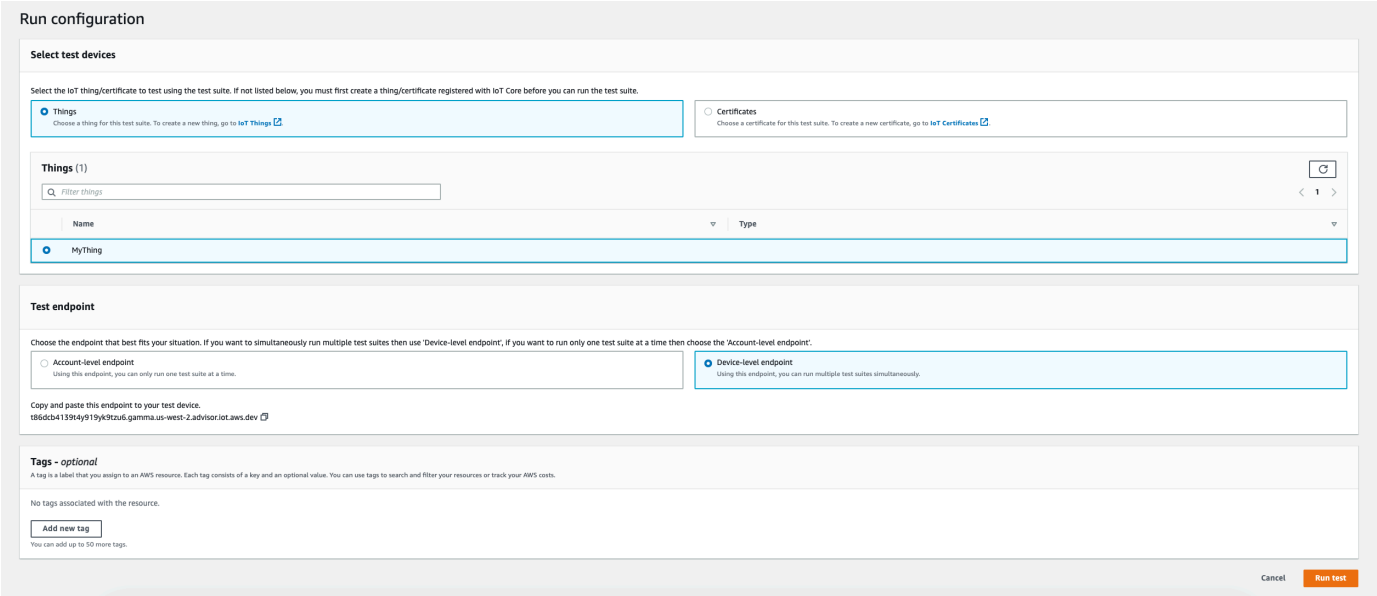



4. Unter Konfiguration ausführen müssen Sie eine AWS IoT Sache oder ein Zertifikat auswählen, das Sie mit Device Advisor testen möchten. Wenn Sie noch keine vorhandenen Dinge oder Zertifikate haben, erstellen Sie zunächst AWS IoT Core Ressourcen.

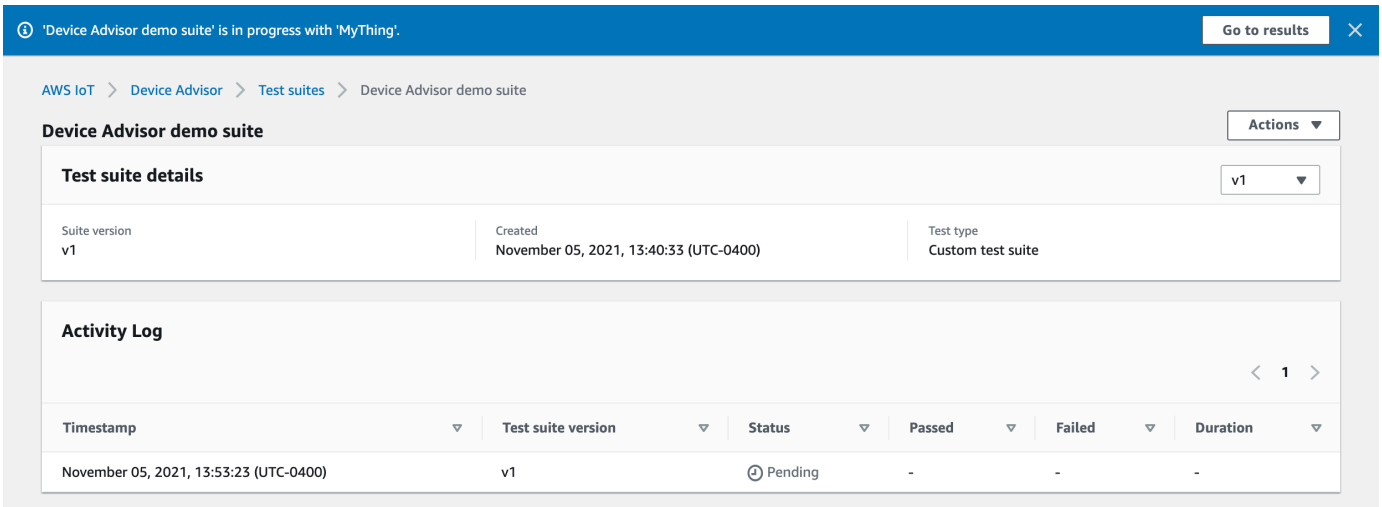
   Wählen Sie im Abschnitt Testendpunkt den Endpunkt aus, der am besten zu Ihrem Fall passt. Wenn Sie in future mehrere Testsuiten gleichzeitig mit demselben AWS Konto ausführen möchten, wählen Sie Endpunkt auf Geräteebene aus. Wenn Sie allerdings planen, jeweils nur eine Testsuite auszuführen, wählen Sie Endpunkt auf Kontoebene aus, um jeweils eine Testsuite auszuführen.

   Konfigurieren Sie Ihr Testgerät mit dem Testendpunkt des ausgewählten Device Advisors.

   Nachdem Sie ein Ding oder ein Zertifikat und einen Device-Advisor-Endpunkt ausgewählt haben, wählen Sie Test ausführen aus.

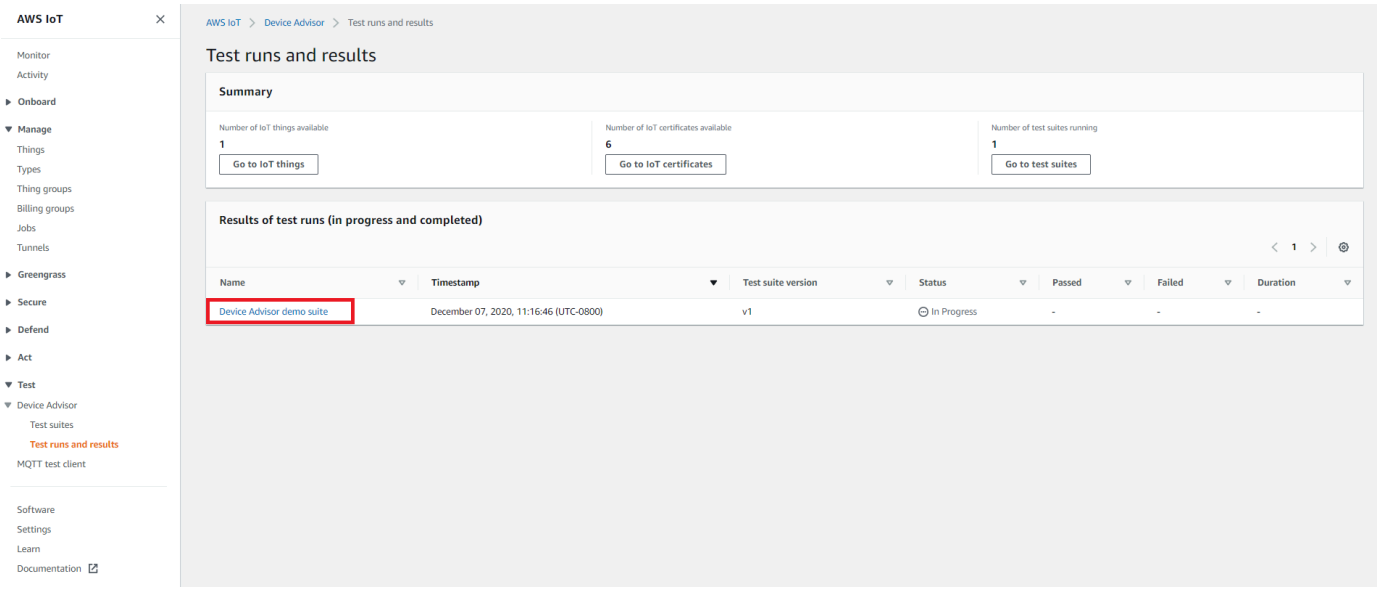



5. Wählen Sie im oberen Banner die Option Gehe zu den Ergebnissen, um die Details des Testlaufs anzuzeigen.

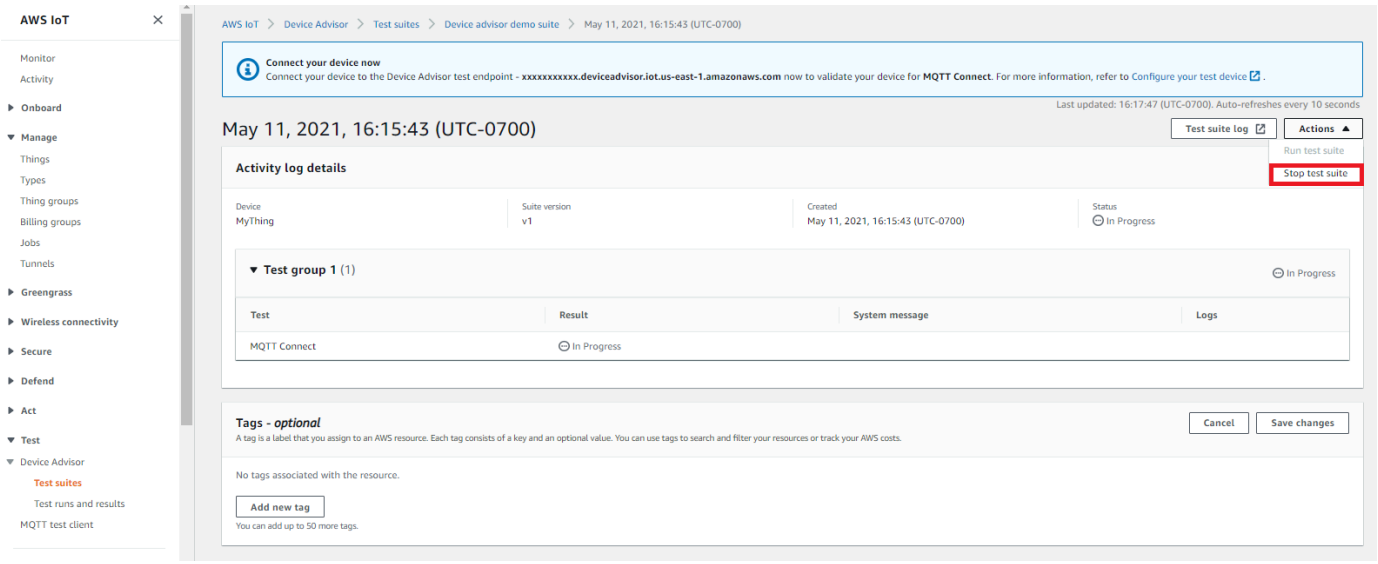



# Beenden einer Testsuite-Ausführung (optional)

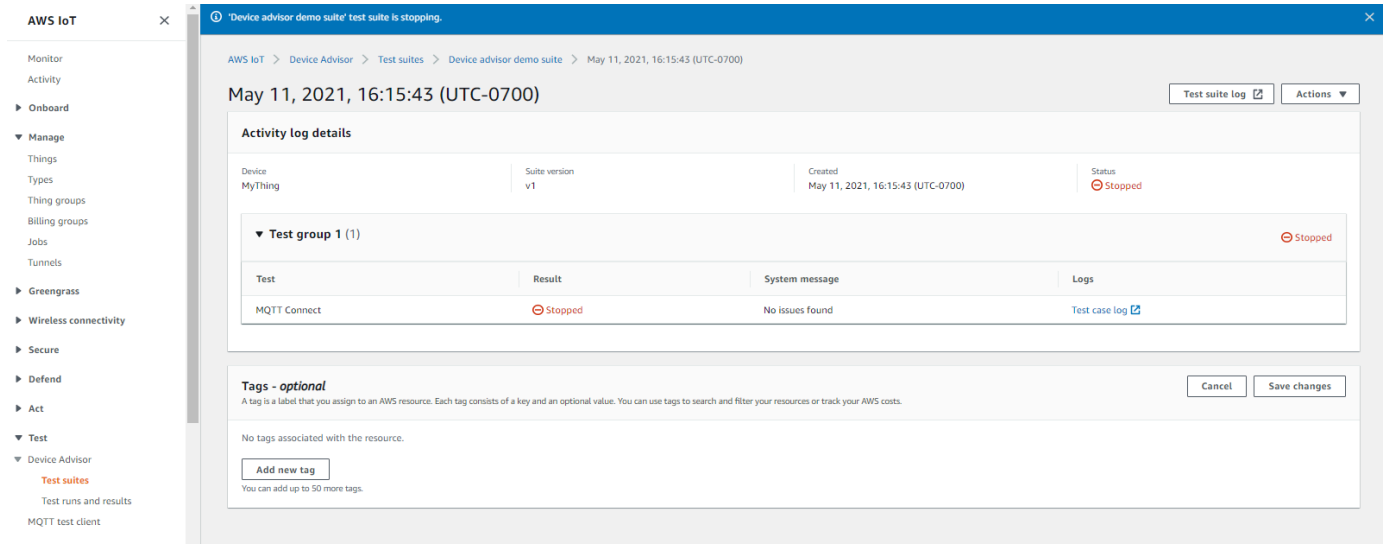
1. Erweitern Sie im Navigationsbereich in der AWS IoT -Konsole die Optionen Test, Device Advisor und wählen Sie dann Testläufe und Ergebnisse aus.
2. Wählen Sie die laufende Testsuite, die Sie beenden möchten.




3. Wählen Sie Aktionen und dann Testsuite beenden aus.




4. Der Bereinigungsvorgang nimmt einige Minuten in Anspruch. Während der Bereinigungsvorgang läuft, ist der Status des Testlaufs `STOPPING`. Warten Sie, bis der Bereinigungsprozess abgeschlossen ist und sich der Status der Testsuite in den `STOPPED`-Status ändert, bevor Sie eine neue Suite ausführen.

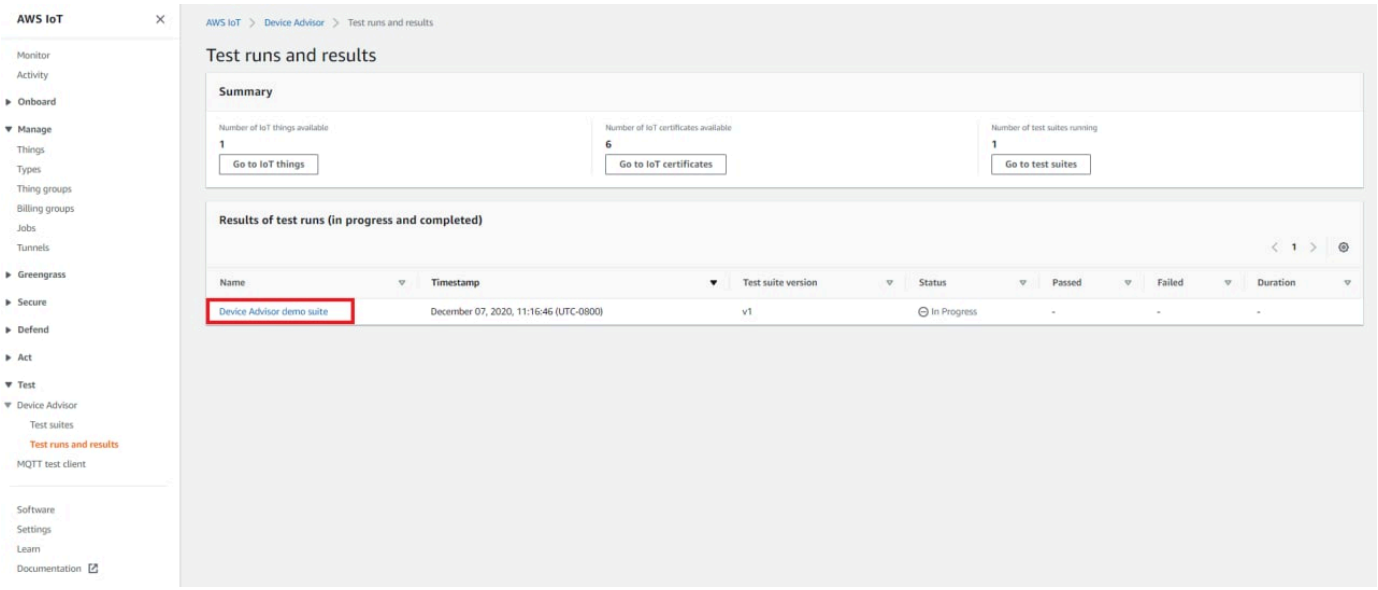



# Anzeigen von Details und Protokolle der Testsuite-Ausführung

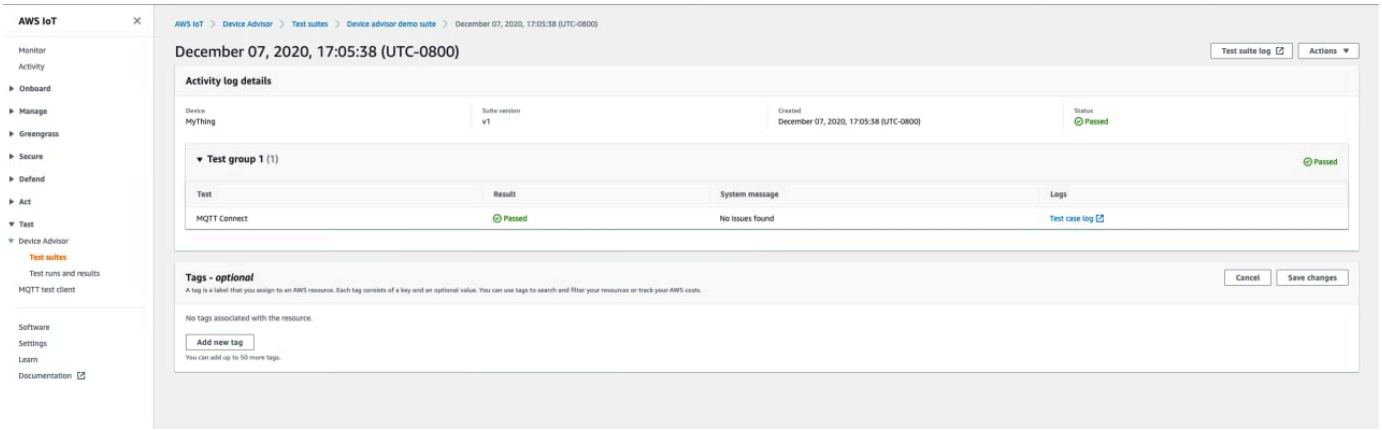
1. Erweitern Sie im Navigationsbereich in der AWS IoT -Konsole die Optionen Test, Device Advisor und wählen Sie dann Testläufe und Ergebnisse aus.

   Diese Seite zeigt Folgendes an:

   - Anzahl der IoT-Dinge
   - Anzahl der IoT-Zertifikate
   - Anzahl der derzeit ausgeführten Testsuites
   - Alle Testsuite-Ausführungen, die erstellt wurden
2. Wählen Sie die Testsuite aus, für die Sie die Details der Ausführung und die Protokolle anzeigen möchten.




Auf der Seite mit der Zusammenfassung der Testsuite wird der Status der aktuellen Testsuite-Ausführung angezeigt. Diese Seite wird automatisch alle 10 Sekunden aktualisiert. Wir empfehlen, dass Sie für Ihr Gerät einen Mechanismus entwickeln, mit dem Sie alle fünf Sekunden ein bis zwei Minuten lang versuchen können, eine Verbindung zu unserem Testendpunkt herzustellen. Sie können dann mehrere Testfälle nacheinander automatisiert ausführen.



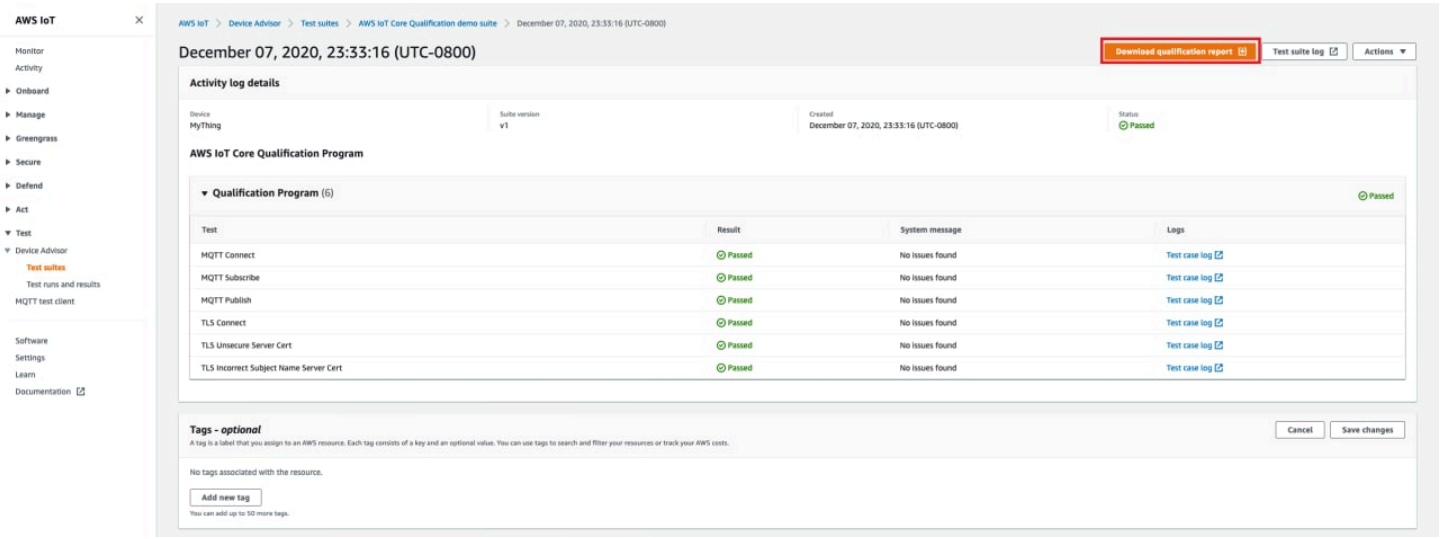

3. Um auf die CloudWatch Protokolle für den Testsuite-Lauf zuzugreifen, wählen Sie Test Suite Log.

   Um auf die CloudWatch Protokolle für einen beliebigen Testfall zuzugreifen, wählen Sie Testfallprotokoll.

4. Führen Sie auf der Grundlage Ihrer Testergebnisse eine Fehlerbehebung auf Ihrem Gerät durch, bis alle Tests bestanden sind.

## Herunterladen eines AWS IoT -Qualifikationsberichts

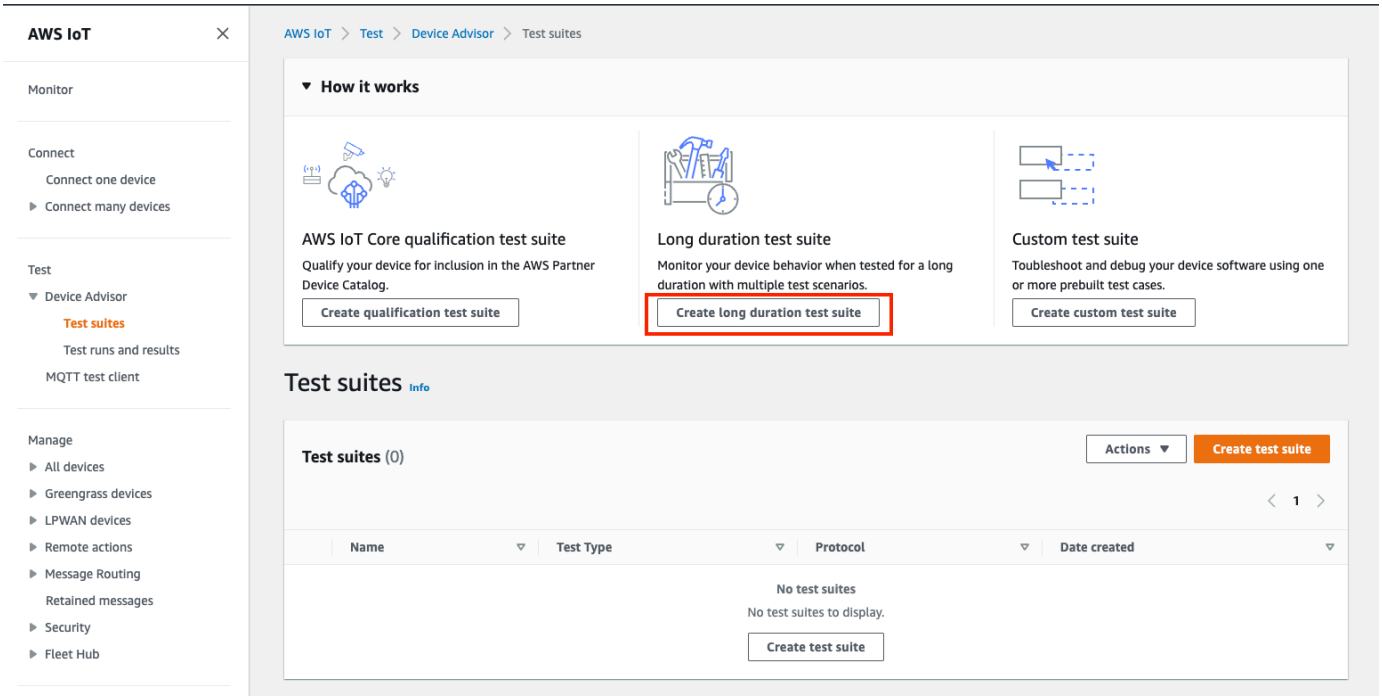
Wenn Sie bei der Erstellung einer Testsuite die Option AWS IoT Qualifizierungstestsuite verwenden ausgewählt haben und eine Qualifizierungstestsuite ausführen konnten, können Sie einen Qualifizierungsbericht herunterladen, indem Sie auf der Übersichtsseite des Testlaufs die Option Qualifikationsbericht herunterladen wählen.




# Konsolen-Workflow für Tests mit langer Dauer

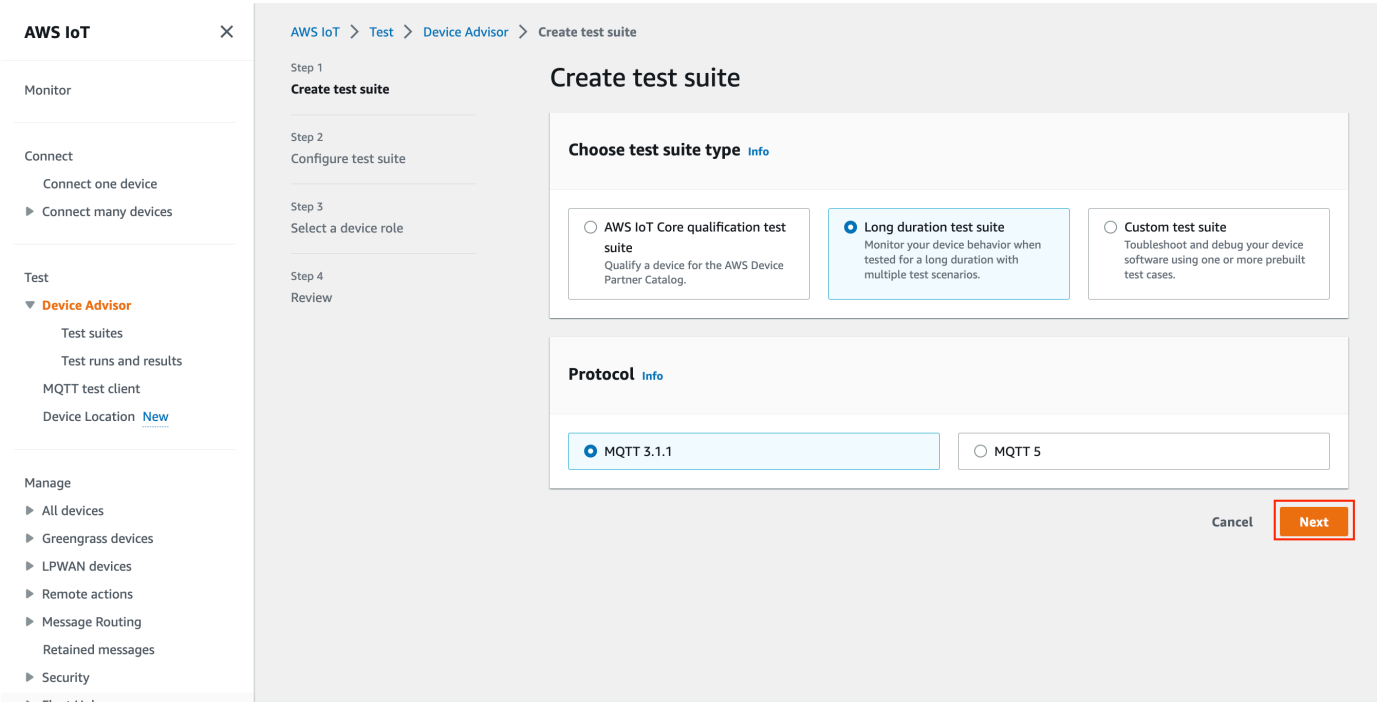
Dieses Tutorial hilft Ihnen bei den ersten Schritten mit der Durchführung von Tests mit langer Dauer auf Device Advisor mithilfe der Konsole. Folgen Sie den Schritten unter Einrichtung, um das Tutorial abzuschließen.

1. Erweitern Sie im Navigationsbereich in der AWS IoT -Konsole die Optionen Test, dann Device Advisor und dann Testsuites. Wählen Sie auf der Seite die Option Create long duration test suite (Testsuite mit langer Dauer erstellen) aus.




2. Wählen Sie auf der Seite Testsuite erstellen die Option Testsuite mit langer Dauer und dann Weiter aus.

   Wählen Sie als Protokoll entweder MQTT3.1.1 oder MQTT5.



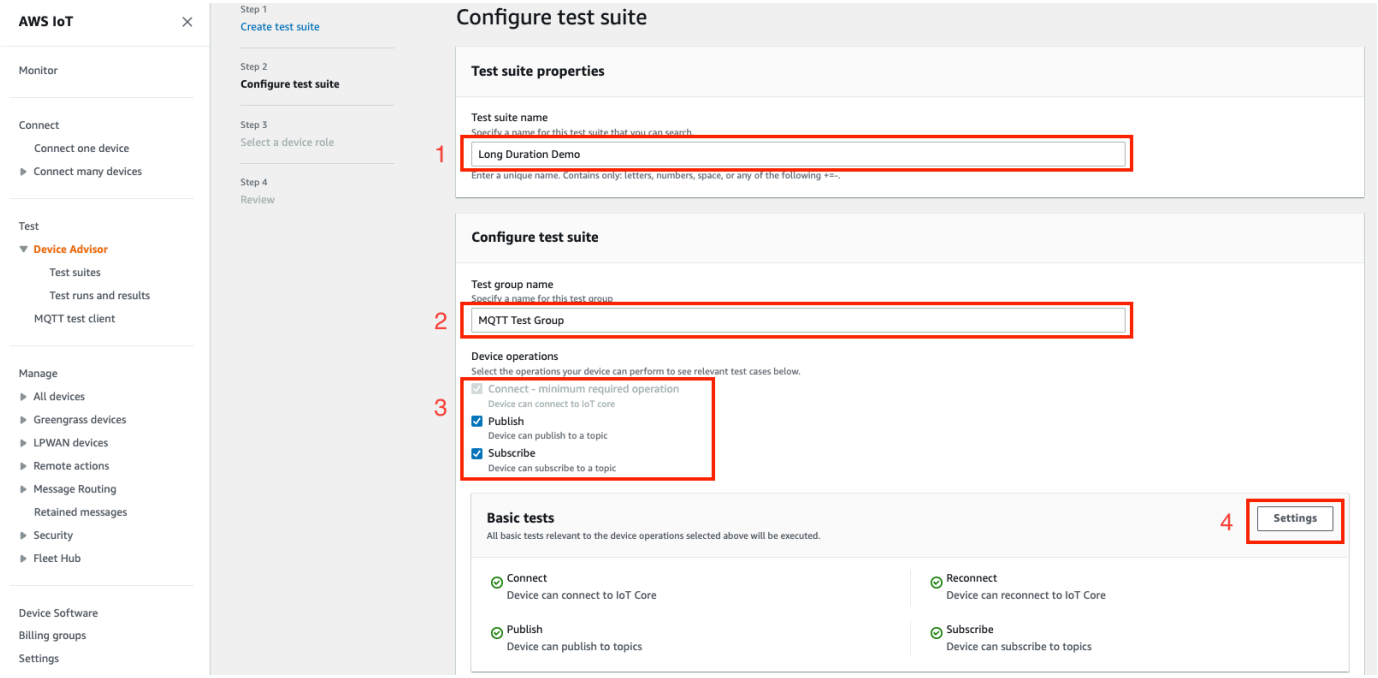

3. Führen Sie auf der Seite Testsuite konfigurieren die folgenden Schritte aus:

   a. Aktualisieren Sie das Feld Name der Testsuite.

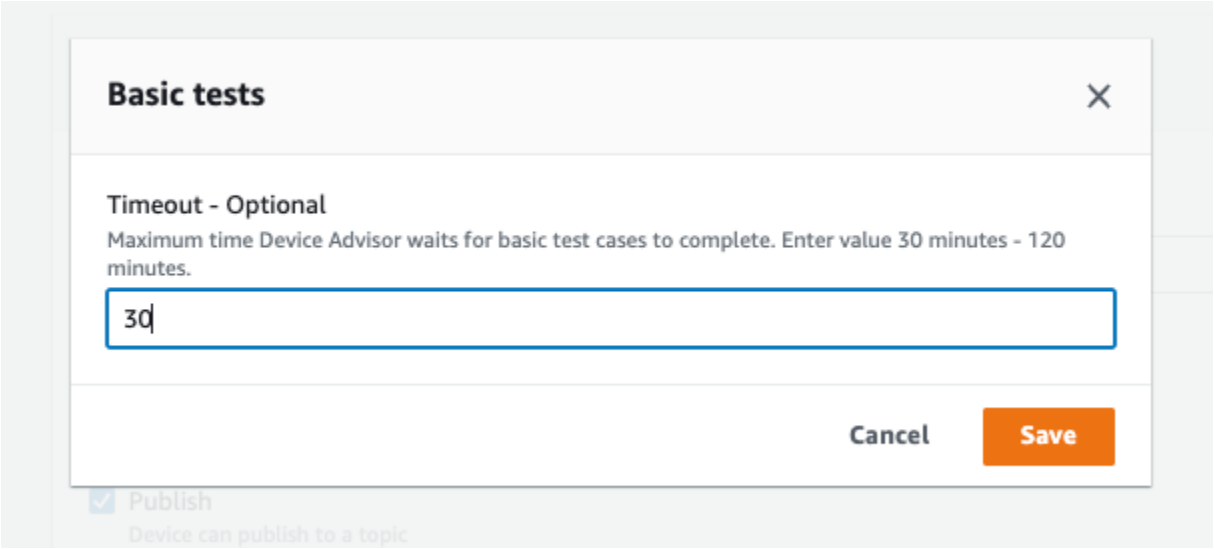
b. Aktualisieren Sie das Feld Name der Testgruppe.

c. Wählen Sie die Geräteoperationen aus, die das Gerät ausführen kann. Dadurch werden die auszuführenden Tests ausgewählt.

d. Wählen Sie die Option Einstellungen aus.




4. (Optional) Geben Sie die maximale Zeit ein, die Device Advisor warten muss, bis die Basistests abgeschlossen sind. Wählen Sie Speichern.



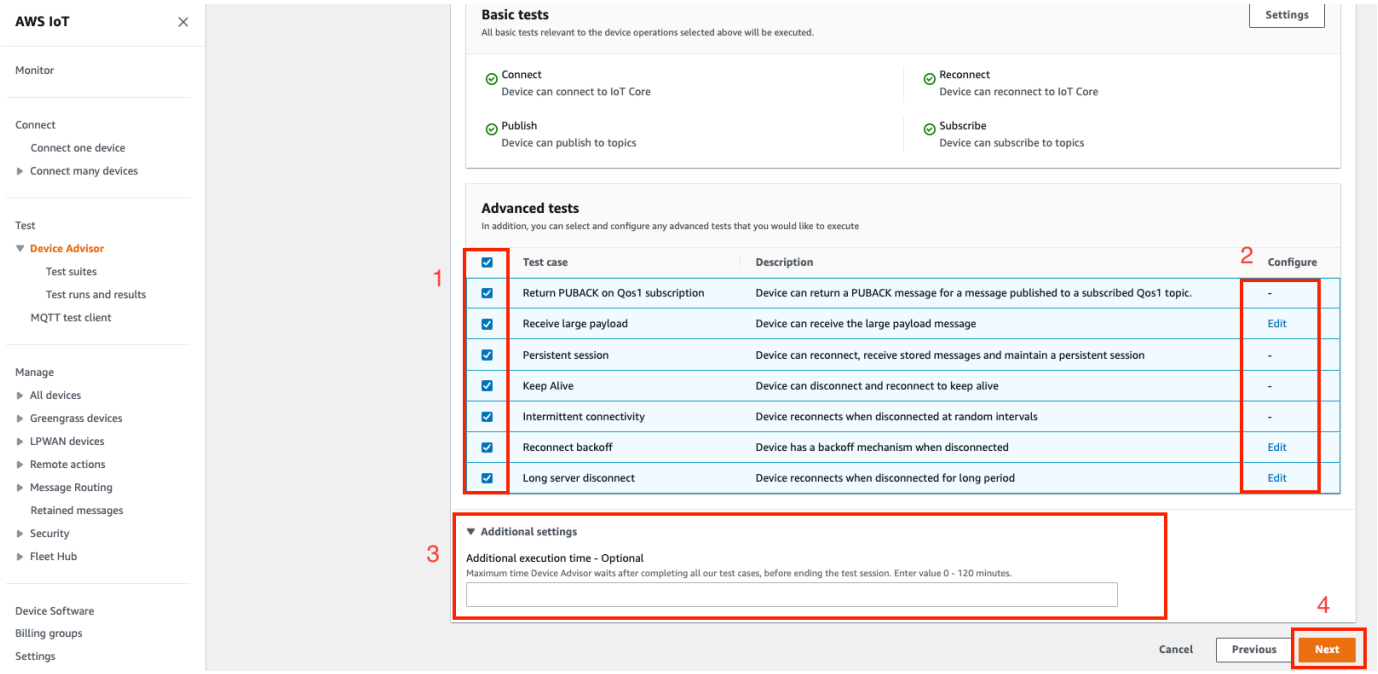

5. Gehen Sie in den Abschnitten Advanced tests (Erweiterte Tests) und Zusätzliche Einstellungen wie folgt vor.

a. Wählen Sie die erweiterten Tests aus, die Sie im Rahmen dieses Tests ausführen möchten, bzw. heben Sie die Auswahl auf.

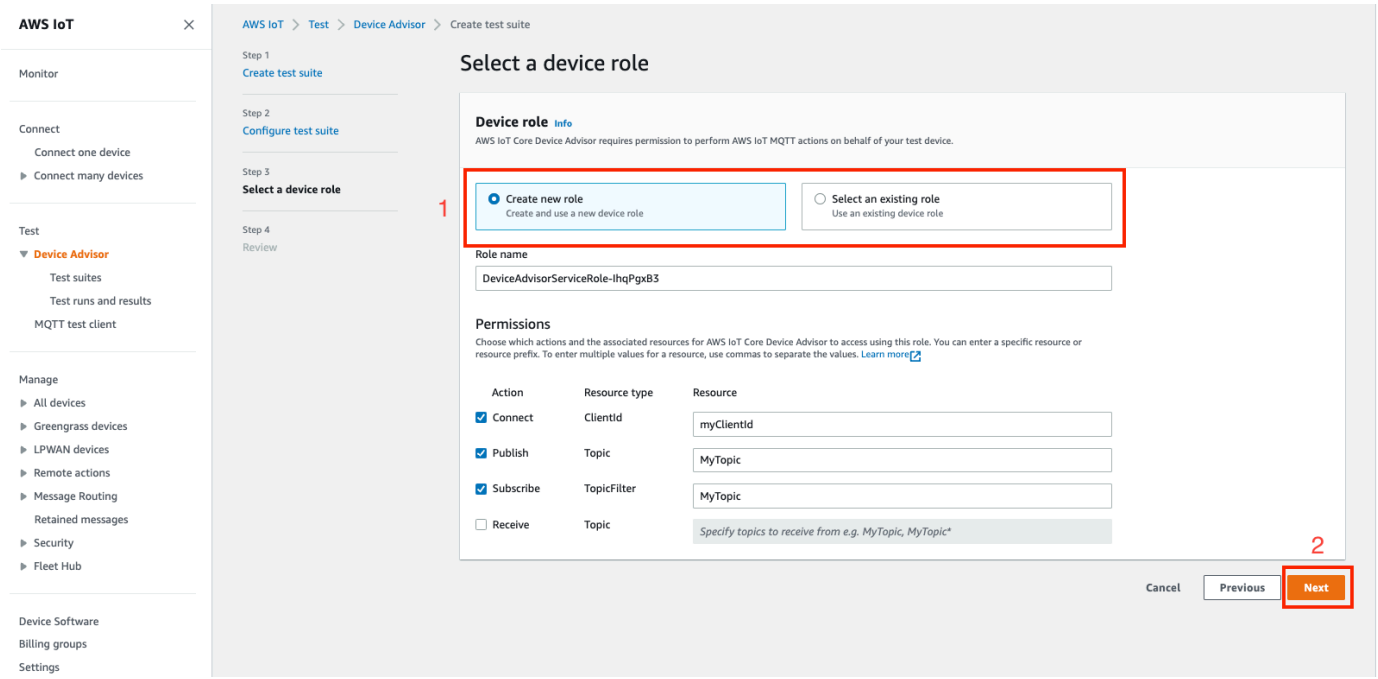
b. Bearbeiten Sie gegebenenfalls die Konfigurationen für die Tests.

c. Konfigurieren Sie die zusätzliche Ausführungszeit im Abschnitt Zusätzliche Einstellungen.

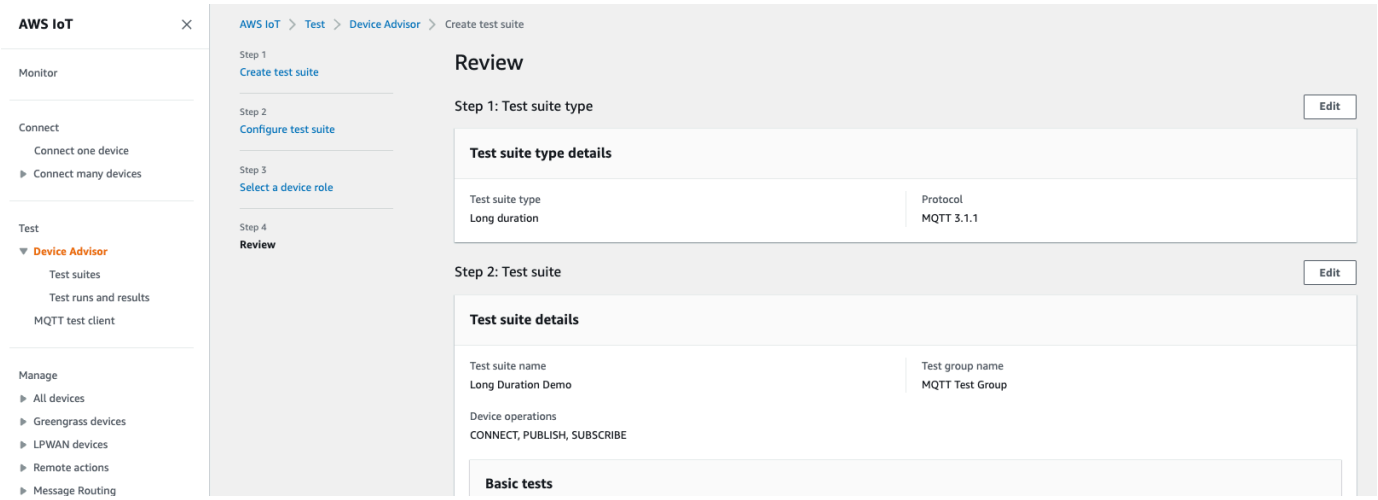
d. Wählen Sie Weiter aus, um mit dem nächsten Schritt fortzufahren.

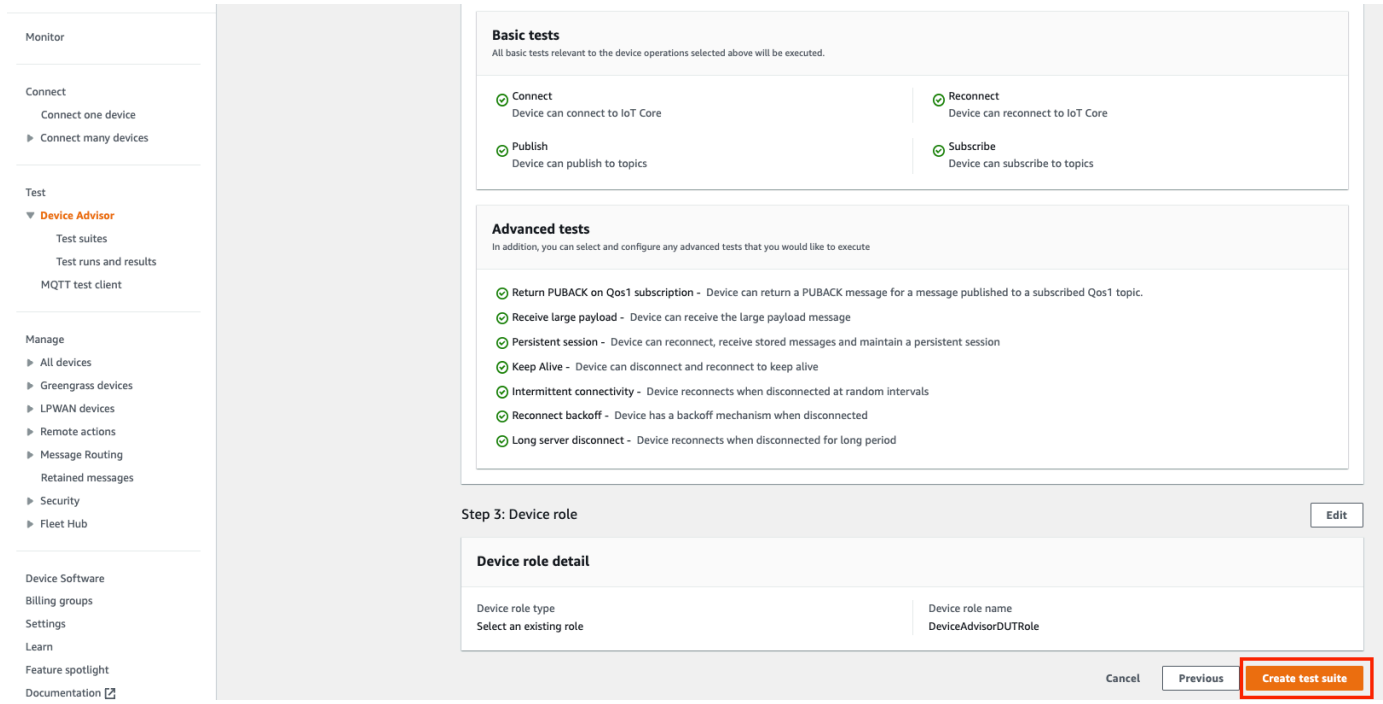



6. Erstellen Sie in diesem Schritt eine neue Rolle oder wählen Sie eine vorhandene Rolle aus. Details dazu finden Sie unter Erstellen Sie eine IAM Rolle, die Sie als Ihre Geräterolle verwenden möchten.

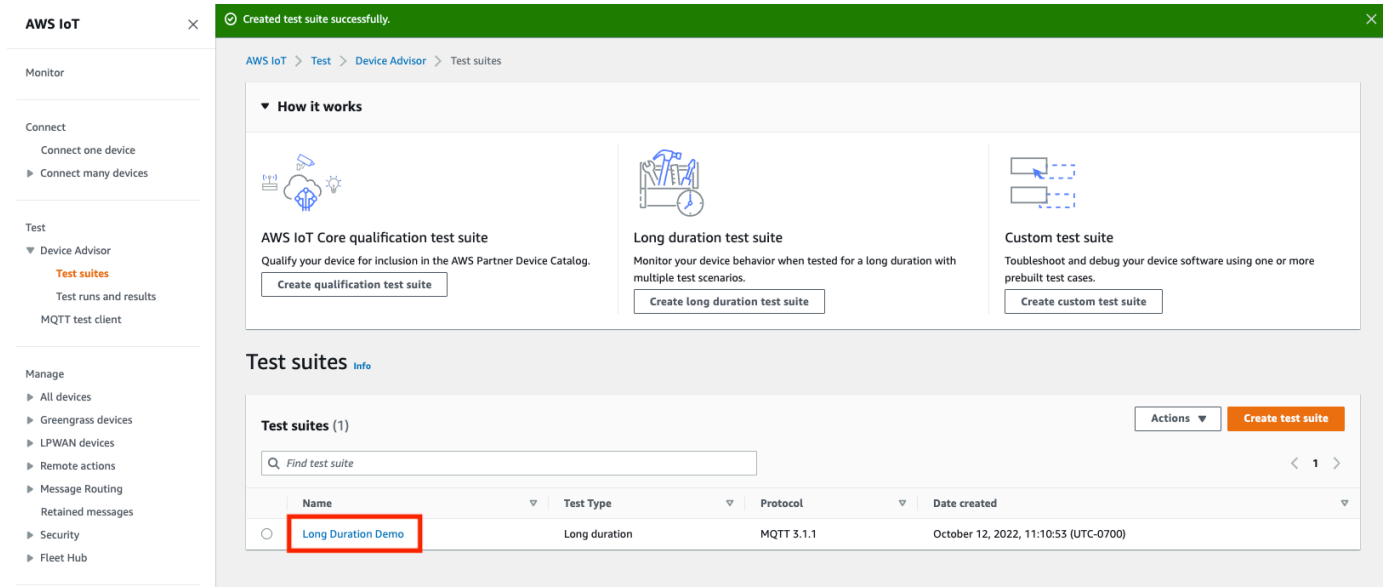



7. Überprüfen Sie alle bis zu diesem Schritt erstellten Konfigurationen und wählen Sie Testsuite erstellen aus.

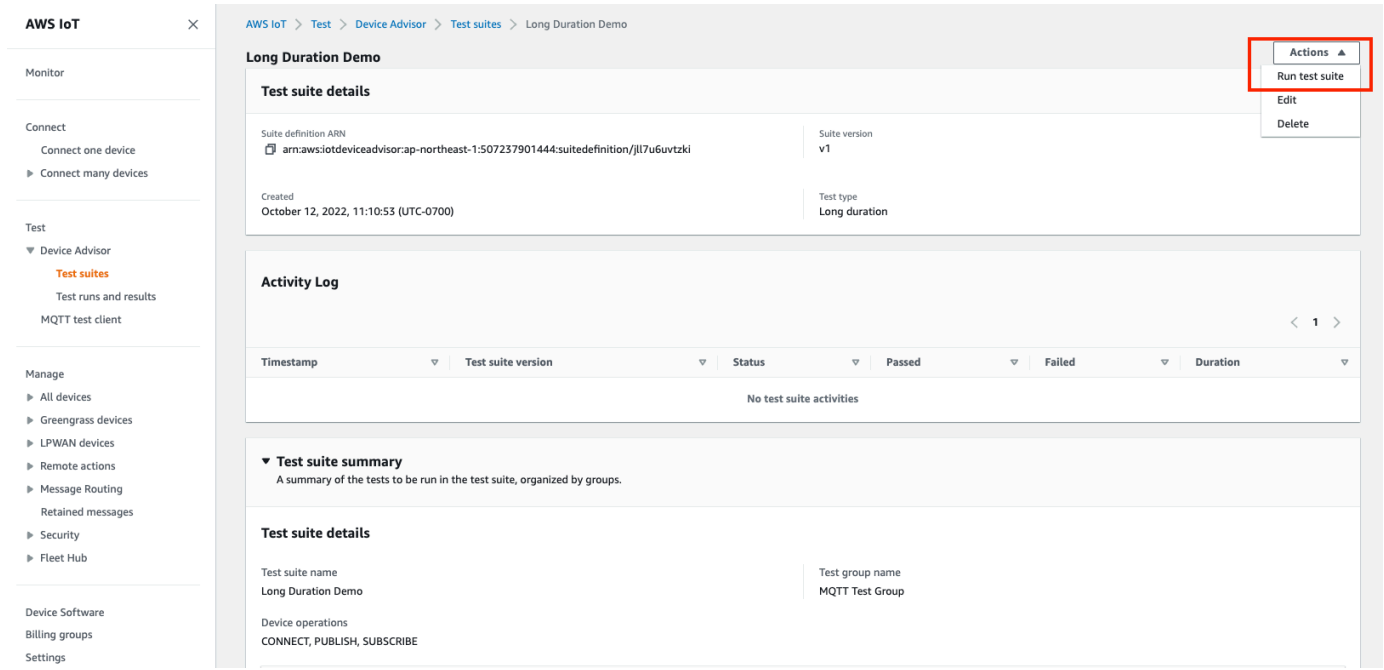





8. Die erstellte Testsuite befindet sich im Abschnitt Testsuites. Wählen Sie die Suite aus, um Details dazu anzuzeigen.




9. Um die erstellte Testsuite auszuführen, wählen Sie Aktionen und dann Testsuite ausführen aus.

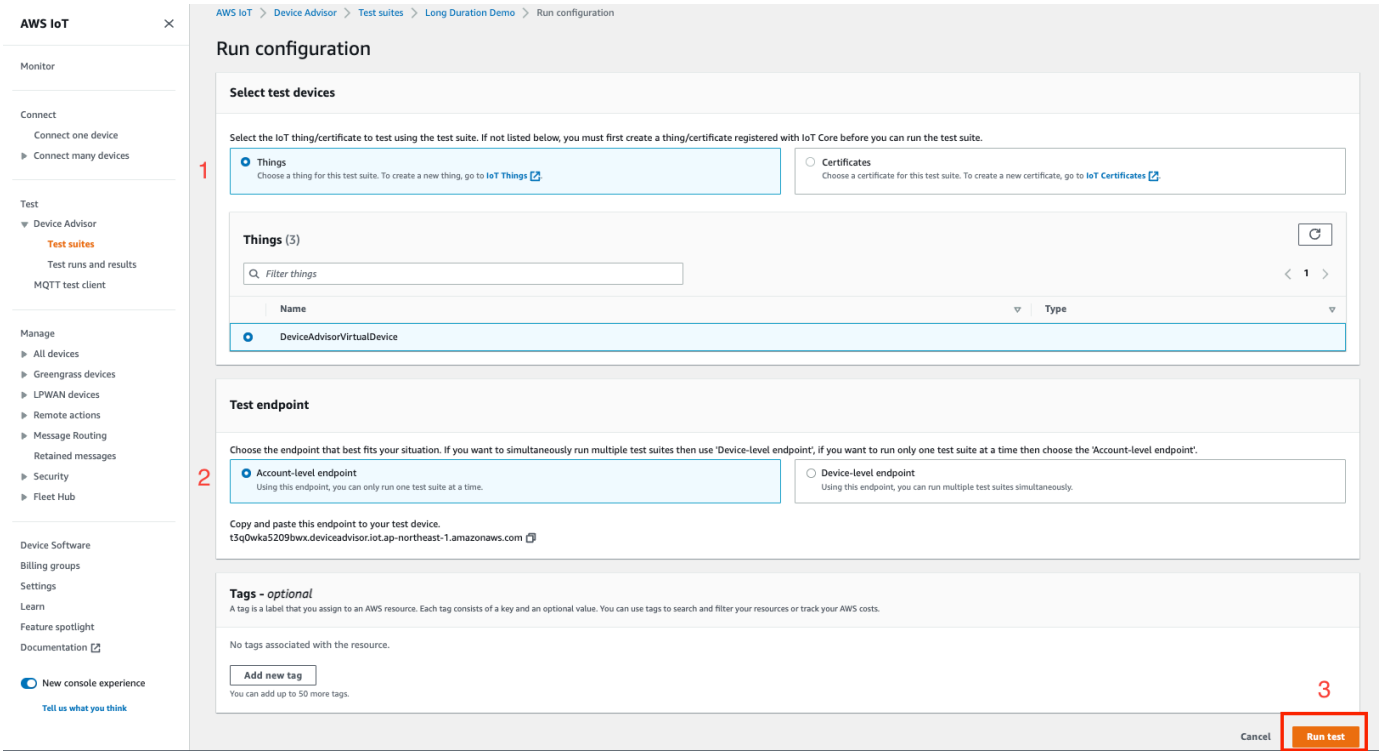



10. Wählen Sie die Konfigurationsoptionen auf der Seite Konfiguration ausführen aus.

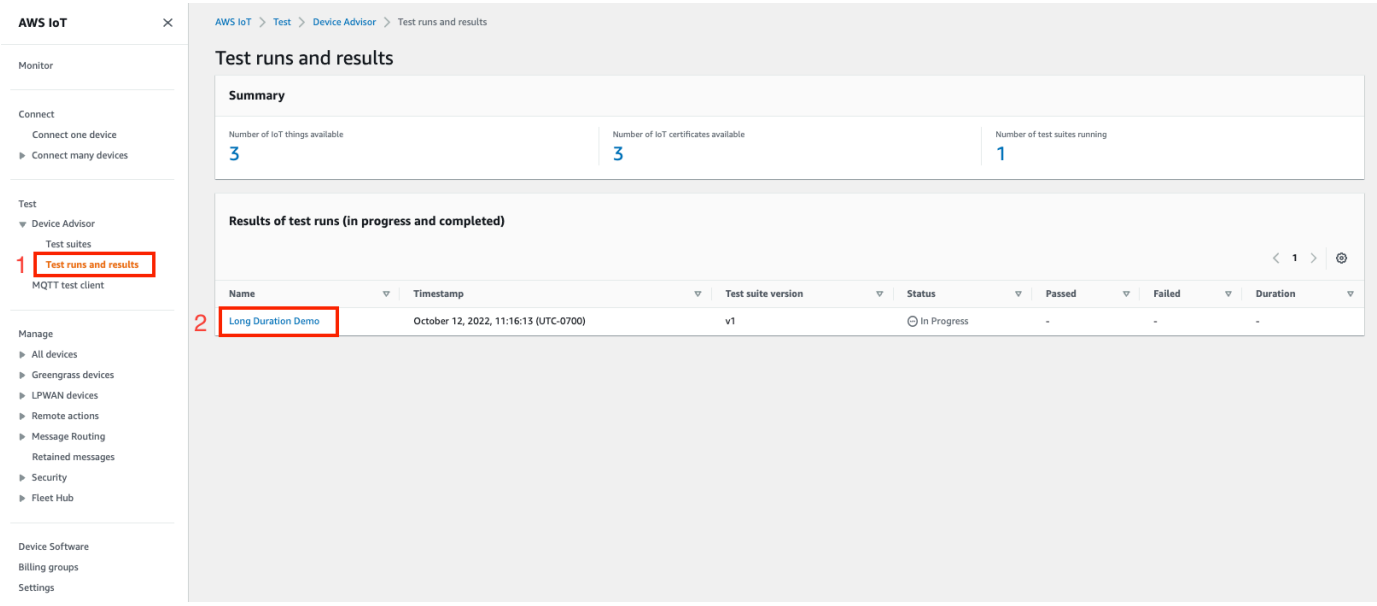
    a. Wählen Sie die Dinge oder das Zertifikat aus, für das der Test ausgeführt werden soll.

    b. Wählen Sie entweder den Endpunkt auf Kontoebene oder den Endpunkt auf Geräteebene aus.

    c. Wählen Sie zum Ausführen des Tests die Option Test ausführen aus.

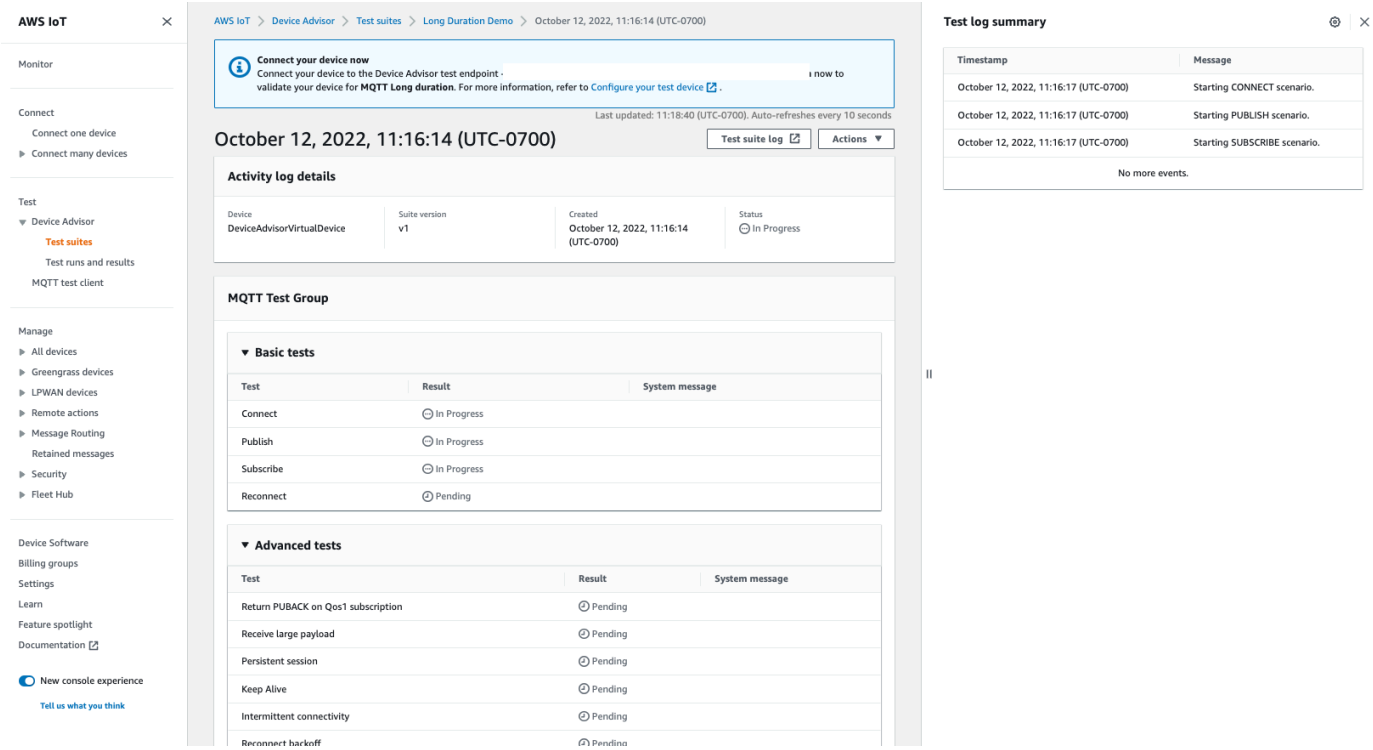



11. Um die Ergebnisse der Testsuite-Ausführung anzuzeigen, wählen Sie im linken Navigationsbereich Testläufe und Ergebnisse aus. Wählen Sie die Testsuite aus, die ausgeführt wurde, um die Details der Ergebnisse anzuzeigen.

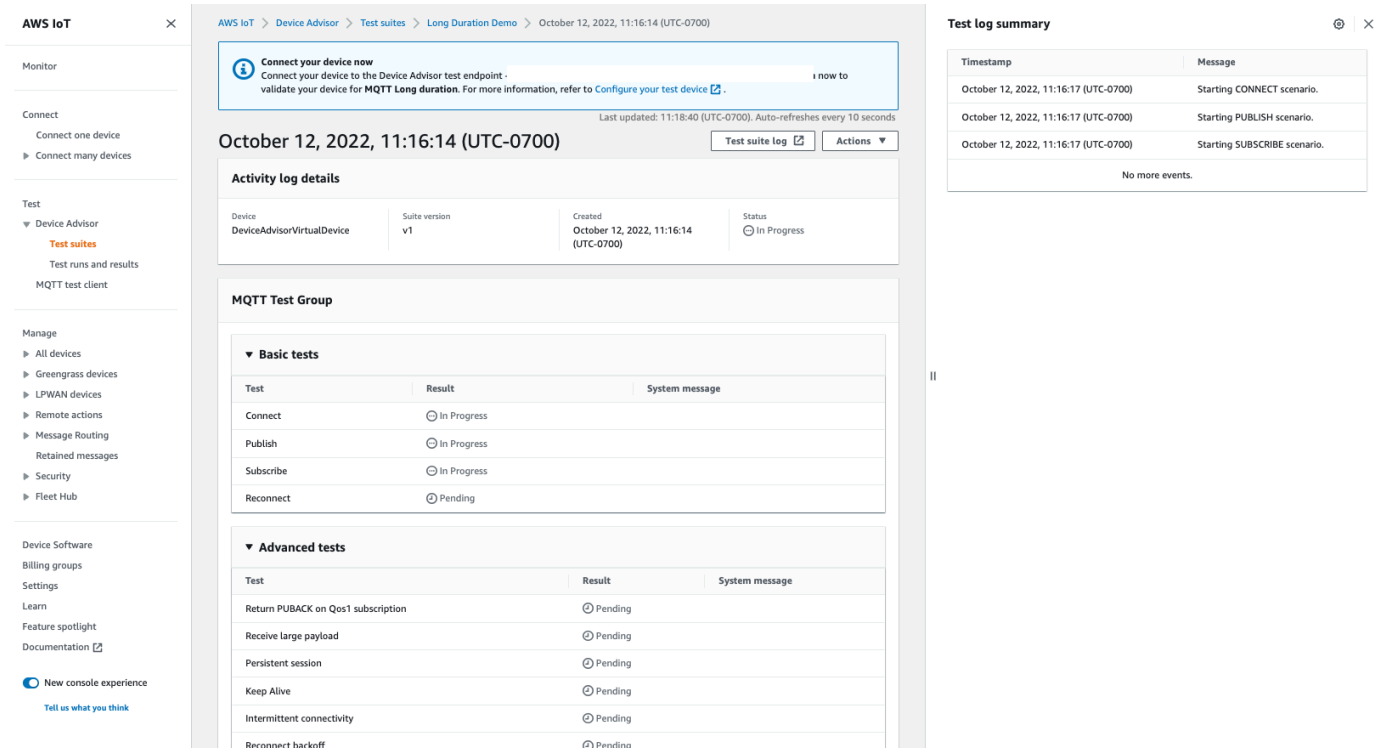



12. Im vorherigen Schritt wird die Seite mit der Testzusammenfassung aufgerufen. Alle Details des Testlaufs werden auf dieser Seite angezeigt. Wenn Sie in der Konsole aufgefordert werden, die

Geräteverbindung herzustellen, verbinden Sie Ihr Gerät mit dem angegebenen Endpunkt. Der Fortschritt der Tests ist auf dieser Seite zu sehen.




13. Der Test mit langer Dauer bietet eine zusätzliche Zusammenfassung des Testprotokolls im Seitenbereich, in der alle wichtigen Ereignisse zwischen dem Gerät und dem Broker nahezu in Echtzeit angezeigt werden. Um detailliertere Protokolle anzuzeigen, klicken Sie auf Testfallprotokoll.




# Device VPC Advisor-Endpunkte ()AWS PrivateLink

Sie können eine private Verbindung zwischen Ihrem Endpunkt VPC und dem AWS IoT Core Device Advisor Testendpunkt (Datenebene) herstellen, indem Sie einen VPCSchnittstellenendpunkt erstellen. Sie können diesen Endpunkt verwenden, um zu überprüfen, ob AWS IoT Geräte zuverlässig und sicher miteinander verbunden sind, AWS IoT Core bevor Sie sie in der Produktion einsetzen. Die vorgefertigten Tests von Device Advisor helfen Ihnen dabei, Ihre Gerätesoftware anhand von Best Practices für die Verwendung von TLSMQTT, Device Shadow und AWS IoT Jobs zu validieren.

AWS PrivateLinkversorgt die Schnittstellenendpunkte, die mit Ihren IoT-Geräten verwendet werden. Mit diesem Dienst können Sie privat auf den AWS IoT Core Device Advisor Testendpunkt zugreifen, ohne dass ein Internet-Gateway, ein NAT Gerät, eine VPN Verbindung oder eine AWS Direct Connect Verbindung erforderlich ist. Instances in Ihrem VPC That Send TCP and MQTT Packets benötigen keine öffentlichen IP-Adressen, um mit AWS IoT Core Device Advisor Testendpunkten zu kommunizieren. Der Verkehr zwischen Ihnen VPC und AWS IoT Core Device Advisor geht nicht weg AWS Cloud. Jegliche TLS MQTT Kommunikation zwischen IoT-Geräten und Device Advisor-Testfällen bleibt innerhalb der Ressourcen in Ihrem AWS-Konto.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen in Ihren Subnetzen dargestellt.

Weitere Informationen zur Verwendung von VPC Schnittstellenendpunkten finden Sie unter VPCSchnittstellenendpunkte (AWS PrivateLink) im VPCAmazon-Benutzerhandbuch.

## Überlegungen zu Endpunkten AWS IoT Core Device Advisor VPC

Lesen Sie die Eigenschaften und Einschränkungen der Schnittstellenendpunkte im VPCAmazon-Benutzerhandbuch, bevor Sie VPC Schnittstellen-Endpunkte einrichten. Beachten Sie Folgendes, bevor Sie fortfahren:

- AWS IoT Core Device Advisor unterstützt derzeit Aufrufe an den Device Advisor-Testendpunkt (Datenebene) von Ihrem VPC aus. Ein Message Broker verwendet Kommunikation auf Datenebene, um Daten zu senden und zu empfangen. Dies geschieht mit Hilfe von TLS MQTT UND-Paketen. VPCEndpunkte für die AWS IoT Core Device Advisor Verbindung Ihres AWS IoT Geräts mit Device Advisor-Testendpunkten. APIAktionen auf der Steuerungsebene werden von diesem VPC Endpunkt nicht verwendet. Verwenden Sie die Konsole, eine oder eine AWS Befehlszeilenschnittstelle über das öffentliche InternetAPIs, um eine AWS SDK Testsuite oder eine andere Steuerungsebene zu erstellen oder auszuführen.
- Die folgenden AWS-Regionen VPC Support-Endpunkte für AWS IoT Core Device Advisor:
  - USA Ost (Nord-Virginia)
  - USA West (Oregon)
  - Asien-Pazifik (Tokio)
  - Europa (Irland)
- Device Advisor unterstützt MQTT X.509-Clientzertifikate und RSA Serverzertifikate.
- VPCEndpunktrichtlinien werden derzeit nicht unterstützt.
- Anweisungen zum Erstellen von Ressourcen, die VPC Endgeräte verbinden, finden Sie unter Voraussetzungen für VPC Endgeräte. Sie müssen private Subnetze erstellenVPC, um Endgeräte verwenden zu können AWS IoT Core Device Advisor VPC.
- Es gibt Kontingente für Ihre AWS PrivateLink Ressourcen. Weitere Informationen finden Sie unter AWS PrivateLink -Kontingente.
- VPCEndgeräte unterstützen nur IPv4 Datenverkehr.

## Erstellen Sie einen VPC Schnittstellenendpunkt für AWS IoT Core Device Advisor

Um mit VPC Endpunkten zu beginnen, erstellen Sie einen VPC Schnittstellenendpunkt. Wählen Sie AWS IoT Core Device Advisor als Nächstes als. AWS-Service Wenn Sie den verwenden AWS CLI, rufen Sie an, describe-vpc-endpoint-servicesum zu bestätigen, dass er AWS IoT Core Device Advisor sich in einer Availability Zone in Ihrem befindet AWS-Region. Vergewissern Sie sich, dass die dem Endpunkt zugeordnete Sicherheitsgruppe die TCPProtokollkommunikation MQTT und den TLS Datenverkehr zulässt. Verwenden Sie zum Beispiel in der Region USA Ost (Nord-Virginia) den folgenden Befehl:

```
aws ec2 describe-vpc-endpoint-services --service-name com.amazonaws.us-
east-1.deviceadvisor.iot
```

Sie können einen VPC Endpunkt für die AWS IoT Core Verwendung des folgenden Dienstnamens erstellen:

- com.amazonaws.region.deviceadvisor.iot

Standardmäßig DNS ist privat für den Endpunkt aktiviert. Dadurch wird sichergestellt, dass der Standard-Testendpunkt weiterhin in Ihren privaten Subnetzen verwendet wird. Um Ihren Endpunkt auf Konto- oder Geräteebene zu erhalten, verwenden Sie die Konsole AWS CLI oder einen AWS SDK. Wenn Sie beispielsweise get-endpoint in einem öffentlichen Subnetz oder im öffentlichen Internet ausführen, können Sie Ihren Endpunkt abrufen und ihn verwenden, um eine Verbindung zu Device Advisor herzustellen. Weitere Informationen finden Sie unter Zugreifen auf einen Service über einen Schnittstellenendpunkt im VPCAmazon-Benutzerhandbuch.

Um MQTT Clients mit den VPC Endpunktschnittstellen zu verbinden, erstellt der AWS PrivateLink Service DNS Datensätze in einer privaten, gehosteten Zone, die an Ihre angehängt istVPC. Diese DNS Aufzeichnungen leiten die Anfragen des AWS IoT Geräts an den VPC Endpunkt weiter.

## Kontrolle des Zugriffs auf AWS IoT Core Device Advisor mehrere VPC Endpunkte

Sie können den Gerätezugriff auf Endpunkte einschränken AWS IoT Core Device Advisor und den Zugriff nur über VPC Endpunkte zulassen, indem Sie VPC Bedingungskontextschlüssel verwenden. AWS IoT Core unterstützt die folgenden VPC verwandten Kontextschlüssel:

- SourceVpc
- SourceVpce
- VPCSourceIp

> **Note**
>
> AWS IoT Core Device Advisor unterstützt derzeit keine VPCEndpunktrichtlinien.

Die folgende Richtlinie gewährt die Erlaubnis, AWS IoT Core Device Advisor mithilfe einer Client-ID, die dem Namen des Dings entspricht, eine Verbindung herzustellen. Außerdem veröffentlicht sie zu jedem Thema, dem der Dingname vorangestellt ist. Die Richtlinie ist abhängig davon, dass das Gerät eine Verbindung zu einem VPC Endpunkt mit einer bestimmten VPC Endpunkt-ID herstellt. Diese Richtlinie verweigert Verbindungsversuche zu Ihrem öffentlichen AWS IoT Core Device Advisor -Testendpunkt.

```
{
"Version": "2012-10-17",
    "Statement": [
        {
"Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/
${iot:Connection.Thing.ThingName}"
            ],
            "Condition": {
"StringEquals": {
"aws:SourceVpce": "vpce-1a2b3c4d"
                }
            }

        },
        {
"Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
```

```
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/
${iot:Connection.Thing.ThingName}/*"
            ]
        }
    ]
}
```

# Device-Advisor-Testfälle

Device Advisor bietet vorgefertigte Tests in sechs Kategorien.

- TLS
- MQTT
- Shadow
- Auftragsausführung
- Berechtigungen und Richtlinien
- Tests mit langer Dauer

## Device Advisor-Testfälle, um sich für das AWS Gerätequalifizierungsprogramm zu qualifizieren.

Ihr Gerät muss die folgenden Tests bestehen, um sich gemäß dem AWS - Gerätequalifizierungsprogramm zu qualifizieren.

> **Note**
>
> Dies ist eine überarbeitete Liste der Qualifizierungstests.

- TLSConnect (“ TLS Connect“)
- TLSServerzertifikat für falschen Betreffnamen („Falscher allgemeiner Name des Antragstellers (CN) /Alternativer Name des Antragstellers (SAN)“)
- TLSUnsicheres Serverzertifikat („Nicht von einer anerkannten Zertifizierungsstelle signiert“)

- TLSGeräteunterstützung für AWS IoT Cipher Suites (“ TLS Geräteunterstützung für AWS IoT empfohlene Cipher Suites“)
- TLSFragmente mit maximaler Größe empfangen (“ Fragmente mit maximaler Größe TLS empfangen“)
- TLSAbgelaufenes Serverzertifikat („Abgelaufenes Serverzertifikat“)
- TLSGroßes Serverzertifikat („TLSgroßes Serverzertifikat“)
- MQTTConnect („Gerät senden CONNECT an AWS IoT Core (Happy Case)“)
- MQTTAbonnieren („Kann abonnieren (Happy Case)“)
- MQTTVeröffentlichen („QoS0 (Happy Case)“)
- MQTTVerbindungs-Jitter-Wiederholungen („Geräteverbindung versucht erneut mit Jitter-Backoff — keine Antwort“) CONNACK

## TLS

Verwenden Sie diese Tests, um festzustellen, ob das Transport Layer Security Protocol (TLS) zwischen Ihren Geräten sicher ist. AWS IoT

> **Note**
>
> Device Advisor unterstützt jetzt TLS 1.3.

### Happy Path

TLSConnect

Überprüft, ob das zu testende Gerät den TLS Handshake abschließen kann. AWS IoT Dieser Test validiert nicht die MQTT Implementierung des Client-Geräts.

Example APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Für optimale Ergebnisse empfehlen wir einen Timeout-Wert von 2 Minuten.

```
"tests":[
   {
      "name":"my_tls_connect_test",
      "configuration": {
         // optional:
         "EXECUTION_TIMEOUT":"300",  //in seconds
      },
      "test":{
         "id":"TLS_Connect",
         "version":"0.0.0"
      }
   }
]
```

Example Ergebnisse des Testfalls:

- Bestanden — Das zu testende Gerät hat den TLS Handshake mit AWS IoT abgeschlossen.
- Mit Warnungen bestanden — Das zu testende Gerät hat den TLS Handshake mit abgeschlossen AWS IoT, es wurden jedoch TLS Warnmeldungen vom Gerät ausgegeben oder. AWS IoT
- Fehlgeschlagen — Das getestete Gerät konnte den TLS Handshake mit AWS IoT aufgrund eines Handshake-Fehlers nicht abschließen.

### TLSFragmente mit maximaler Größe empfangen

Dieser Testfall bestätigt, dass Ihr Gerät Fragmente mit TLS maximaler Größe empfangen und verarbeiten kann. Ihr Testgerät muss ein vorkonfiguriertes Thema mit QoS 1 abonnieren, um eine große Nutzlast zu empfangen. Sie können die Nutzlast mit der Konfiguration `${payload}` anpassen.

Example APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Für optimale Ergebnisse empfehlen wir einen Timeout-Wert von 2 Minuten.

```
"tests":[
```

```
   {
      "name":"TLS Receive Maximum Size Fragments",
      "configuration": {
         // optional:
         "EXECUTION_TIMEOUT":"300",  //in seconds
         "PAYLOAD_FORMAT":"{"message":"${payload}"}", // A string with a placeholder
 ${payload}, or leave it empty to receive a plain string.
         "TRIGGER_TOPIC": "test_1" // A topic to which a device will subscribe, and
 to which a test case will publish a large payload.
      },
      "test":{
         "id":"TLS_Receive_Maximum_Size_Fragments",
         "version":"0.0.0"
      }
   }
]
```

## Cipher Suites

TLSGeräteunterstützung für AWS IoT empfohlene Cipher Suites

Überprüft, ob die Cipher Suites in der TLS Client Hello-Nachricht des getesteten Geräts die empfohlenen Verschlüsselungssammlungen enthalten.AWS IoT Es bietet mehr Einblicke in die vom Gerät unterstützten Verschlüsselungssammlungen.

Example APIDefinition des Testfalls:

> **Note**
>
> EXECUTION_TIMEOUT hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten.

```
"tests":[
   {
      "name":"my_tls_support_aws_iot_cipher_suites_test",
      "configuration": {
         // optional:
         "EXECUTION_TIMEOUT":"300",  // in seconds
      },
      "test":{
```

```
        "id":"TLS_Support_AWS_IoT_Cipher_Suites",
        "version":"0.0.0"
      }
   }
]
```

Example Ergebnisse des Testfalls:

- Bestanden — Das zu testende Gerät enthält mindestens eine der empfohlenen Verschlüsselungssammlungen und keine AWS IoT Verschlüsselungssammlungen, die nicht unterstützt werden.
- Pass with warnings (Mit Warnungen bestanden): Die Cipher Suites des Geräts enthalten mindestens eine AWS IoT -Cipher-Suite, aber:

  1. sie enthält keine der empfohlenen Cipher Suites.
  2. Es enthält Verschlüsselungssammlungen, die von nicht unterstützt werden. AWS IoT

  Wir empfehlen Ihnen, zu überprüfen, ob alle nicht unterstützten Cipher Suites sicher sind.
- Fehlgeschlagen — Das zu testende Gerät enthält keine der unterstützten Verschlüsselungssammlungen. AWS IoT

## Größeres Serverzertifikat

TLSgroßes Serverzertifikat

Wird auf Ihrem Gerät validiert und kann den TLS Handshake abschließen AWS IoT , wenn es ein größeres Serverzertifikat empfängt und verarbeitet. Die Größe des von diesem Test verwendeten Serverzertifikats (in Byte) ist um 20 größer als die derzeit im TLSConnect-Testfall und in IoT Core verwendete Größe. In diesem Testfall wird der Pufferspeicher Ihres Geräts auf TLS Wenn der Pufferspeicher groß genug ist, wird der TLS Handshake ohne Fehler abgeschlossen. AWS IoT Dieser Test validiert nicht die MQTT Implementierung des Geräts. Der Testfall tritt nach Abschluss des TLS Handshake-Vorgangs auf.

Example APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Für optimale Ergebnisse empfehlen wir einen Timeout-Wert von 2 Minuten. Wenn dieser Testfall fehlschlägt, der

TLSConnect-Testfall jedoch erfolgreich ist, empfehlen wir Ihnen, das Pufferspeicherlimit Ihres Geräts zu erhöhen. TLS Durch die Erhöhung des Pufferspeicherlimits wird sichergestellt, dass Ihr Gerät ein größeres Serverzertifikat verarbeiten kann, falls die Größe zunimmt.

```
"tests":[
   {
      "name":"my_tls_large_size_server_cert_test",
      "configuration": {
         // optional:
         "EXECUTION_TIMEOUT":"300",  // in seconds
      },
      "test":{
         "id":"TLS_Large_Size_Server_Cert",
         "version":"0.0.0"
      }
   }
]
```

Example Ergebnisse des Testfalls:

- Bestanden — Das getestete Gerät hat den TLS Handshake mit AWS IoT abgeschlossen.
- Mit Warnungen bestanden — Das getestete Gerät hat den TLS Handshake mit abgeschlossen AWS IoT, es gibt jedoch TLS Warnmeldungen entweder vom Gerät oder. AWS IoT
- Fehlgeschlagen — Das getestete Gerät konnte den TLS Handshake AWS IoT aufgrund eines Fehlers während des Handshake-Vorgangs nicht abschließen.

## TLSUnsicheres Serverzertifikat

Nicht von einer anerkannten Zertifizierungsstelle signiert

Überprüft, ob das zu testende Gerät die Verbindung schließt, wenn ihm ein Serverzertifikat ohne gültige Signatur der CA vorgelegt wird. ATS Ein Gerät sollte nur eine Verbindung zu einem Endpunkt herstellen, der ein gültiges Zertifikat vorlegt.

Example APIDefinition des Testfalls:

> **Note**
>
> EXECUTION_TIMEOUT hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten.

```
"tests":[
   {
      "name":"my_tls_unsecure_server_cert_test",
      "configuration": {
         // optional:
         "EXECUTION_TIMEOUT":"300",  //in seconds
      },
      "test":{
         "id":"TLS_Unsecure_Server_Cert",
         "version":"0.0.0"
      }
   }
]
```

Example Ergebnisse des Testfalls:

- Pass (Bestanden): Das getestete Gerät hat die Verbindung geschlossen.
- Fehlgeschlagen — Das getestete Gerät hat den TLS Handshake mit AWS IoT abgeschlossen.

TLSFalscher Betreffname, Serverzertifikat//Falscher allgemeiner Name (CN) /Alternativer Name des Antragstellers () SAN

Überprüft, ob das getestete Gerät die Verbindung schließt, wenn ihm ein Serverzertifikat für einen anderen Domainnamen als den angeforderten vorgelegt wird.

Example APIDefinition des Testfalls:

> **Note**
>
> EXECUTION_TIMEOUT hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten.

```
"tests":[
   {
      "name":"my_tls_incorrect_subject_name_cert_test",
      "configuration": {
         // optional:
         "EXECUTION_TIMEOUT":"300",   // in seconds
      },
      "test":{
         "id":"TLS_Incorrect_Subject_Name_Server_Cert",
         "version":"0.0.0"
      }
   }
]
```

Example Ergebnisse des Testfalls:

- Pass (Bestanden): Das getestete Gerät hat die Verbindung geschlossen.
- Fehlgeschlagen — Das getestete Gerät hat den TLS Handshake mit AWS IoT abgeschlossen.

## TLSAbgelaufenes Serverzertifikat

Abgelaufenes Serverzertifikat

Überprüft, ob das getestete Gerät die Verbindung schließt, wenn ihm ein abgelaufenes Serverzertifikat vorgelegt wird.

Example APITestfalldefinition:

> **Note**
>
> EXECUTION_TIMEOUT hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten.

```
"tests":[
   {
      "name":"my_tls_expired_cert_test",
      "configuration": {
         // optional:
         "EXECUTION_TIMEOUT":"300",  //in seconds
```

```
      },
      "test":{
         "id":"TLS_Expired_Server_Cert",
         "version":"0.0.0"
      }
   }
]
```

Example Ergebnisse des Testfalls:

- Bestanden — Das zu testende Gerät weigert sich, den TLS Handshake mit AWS IoT abzuschließen. Das Gerät sendet eine TLS Warnmeldung, bevor es die Verbindung schließt.
- Mit Warnungen bestanden — Das getestete Gerät weigert sich, den TLS Handshake mit AWS IoT abzuschließen. Es sendet jedoch keine TLS Warnmeldung, bevor die Verbindung geschlossen wird.
- Fehlgeschlagen — Das getestete Gerät schließt den TLS Handshake mit AWS IoT ab.

# MQTT

## CONNECT, DISCONNECT und RECONNECT

„Gerät gesendet CONNECT an AWS IoT Core (Happy Case)“

Überprüft, ob das zu testende Gerät eine CONNECT Anfrage sendet.

APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten.

```
"tests":[
   {
      "name":"my_mqtt_connect_test",
      "configuration": {
         // optional:
         "EXECUTION_TIMEOUT":"300",   // in seconds
```

```
      },
      "test":{
         "id":"MQTT_Connect",
         "version":"0.0.0"
      }
   }
]
```

„Das Gerät kann PUBACK zu einem beliebigen Thema für QoS zurückkehren“

In diesem Testfall wird geprüft, ob das Gerät (Client) eine PUBACK Nachricht zurückgeben kann, wenn es nach dem Abonnieren eines Themas mit QoS1 eine Veröffentlichungsnachricht vom Broker erhalten hat.

Der Inhalt der Nutzlast und die Größe der Nutzlast sind für diesen Testfall konfigurierbar. Wenn die Nutzlastgröße konfiguriert ist, überschreibt Device Advisor den Wert für den Nutzlastinhalt und sendet eine vordefinierte Nutzlast mit der gewünschten Größe an das Gerät. Die Nutzlastgröße ist ein Wert zwischen 0 und 128 und darf 128 KB nicht überschreiten. AWS IoT Core lehnt Veröffentlichungs- und Verbindungsanfragen ab, die größer als 128 KB sind, wie auf der Seite Grenzwerte und Kontingente für AWS IoT Core -Message-Broker und -Protokolle beschrieben.

APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten. `PAYLOAD_SIZE` kann auf einen Wert zwischen 0 und 128 Kilobyte konfiguriert werden. Die Definition einer Nutzlastgröße hat Vorrang vor dem Nutzlastinhalt, da Device Advisor eine vordefinierte Nutzlast mit der angegebenen Größe zurück an das Gerät sendet.

```
"tests":[
{
        "name":"my_mqtt_client_puback_qos1",
        "configuration": {
            // optional:"TRIGGER_TOPIC": "myTopic",
            "EXECUTION_TIMEOUT":"300", // in seconds
            "PAYLOAD_FOR_PUBLISH_VALIDATION":"custom payload",
            "PAYLOAD_SIZE":"100" // in kilobytes
```

```
        },
        "test": {
            "id": "MQTT_Client_Puback_QoS1",
            "version": "0.0.0"
        }
    }
]
```

„Die Geräteverbindung wird erneut mit Jitter-Backoff versucht — keine Antwort“ CONNACK

Überprüft, ob das getestete Gerät den richtigen Jitter-Backoff verwendet, wenn es mindestens fünfmal erneut eine Verbindung zum Broker herstellt. Der Broker protokolliert den Zeitstempel der CONNECT Anfrage des zu testenden Geräts, führt eine Paketvalidierung durch, hält an, ohne eine Nachricht an das zu testende Gerät CONNACK zu senden, und wartet, bis das zu testende Gerät die Anfrage erneut sendet. Der sechste Verbindungsversuch wird durchgelassen und darf zum CONNACK getesteten Gerät zurückfließen.

Der vorherige Vorgang wird erneut ausgeführt. Insgesamt erfordert dieser Testfall, dass das Gerät insgesamt mindestens 12 Mal eine Verbindung herstellt. Die gesammelten Zeitstempel werden verwendet, um zu überprüfen, ob das getestete Gerät den Jitter-Backoff verwendet. Wenn das getestete Gerät eine streng exponentielle Backoff-Verzögerung aufweist, wird dieser Testfall mit Warnungen bestanden.

Wir empfehlen, den Mechanismus Exponential Backoff And Jitter (Exponentielles Backoff und Jitter) auf dem getesteten Gerät zu implementieren, um diesen Testfall zu bestehen.

APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 4 Minuten.

```
"tests":[
   {
      "name":"my_mqtt_jitter_backoff_retries_test",
      "configuration": {
         // optional:
         "EXECUTION_TIMEOUT":"300",    // in seconds
```

```
      },
      "test":{
         "id":"MQTT_Connect_Jitter_Backoff_Retries",
         "version":"0.0.0"
      }
   }
]
```

„Erneute Geräteverbindungsversuche mit exponentiellem Backoff — Keine Antwort“ CONNACK

Überprüft, ob das getestete Gerät das richtige exponentielle Backoff verwendet, wenn es mindestens fünfmal erneut eine Verbindung zum Broker herstellt. Der Broker protokolliert den Zeitstempel der CONNECT Anfrage des zu testenden Geräts, führt eine Paketvalidierung durch, hält an, ohne eine Nachricht an das Client-Gerät CONNACK zu senden, und wartet, bis das zu testende Gerät die Anfrage erneut sendet. Die gesammelten Zeitstempel werden verwendet, um zu überprüfen, ob das getestete Gerät ein exponentielles Backoff verwendet.

Wir empfehlen, den Mechanismus Exponential Backoff And Jitter (Exponentielles Backoff und Jitter) auf dem getesteten Gerät zu implementieren, um diesen Testfall zu bestehen.

APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 4 Minuten.

```
"tests":[
   {
      "name":"my_mqtt_exponential_backoff_retries_test",
      "configuration": {
         // optional:
         "EXECUTION_TIMEOUT":"600",  // in seconds
      },
      "test":{
         "id":"MQTT_Connect_Exponential_Backoff_Retries",
         "version":"0.0.0"
      }
   }
]
```

„Device re-connect with jitter backoff - After server disconnect“

Überprüft, ob ein getestetes Gerät bei der Wiederherstellung der Verbindung, nachdem es vom Server getrennt wurde, die erforderlichen Jitter- und Backoff-Werte verwendet. Device Advisor trennt das Gerät mindestens fünfmal vom Server und beobachtet das Verhalten des Geräts bei MQTT der Wiederverbindung. Device Advisor protokolliert den Zeitstempel der CONNECT Anfrage für das zu testende Gerät, führt eine Paketvalidierung durch, hält an, ohne eine Nachricht an das Client-Gerät CONNACK zu senden, und wartet, bis das zu testende Gerät die Anfrage erneut sendet. Die gesammelten Zeitstempel werden verwendet, um zu überprüfen, ob das getestete Gerät den Jitter-Backoff verwendet. Wenn das getestete Gerät eine streng exponentielle Backoff-Verzögerung aufweist oder keinen ordnungsgemäßen Jitter-Backoff-Mechanismus implementiert, wird dieser Testfall mit Warnungen bestanden. Wenn das getestete Gerät entweder einen linearen Backoff-Mechanismus oder einen konstanten Backoff-Mechanismus implementiert hat, schlägt der Test fehl.

Damit dieser Testfall bestanden wird, empfehlen wir, den Mechanismus Exponential Backoff And Jitter (Exponentielles Backoff und Jitter) auf dem getesteten Gerät zu implementieren.

APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 4 Minuten.
> Die Anzahl der Wiederverbindungsversuche zur Überprüfung des Backoffs kann durch Angabe der `RECONNECTION_ATTEMPTS` geändert werden. Die Zahl muss zwischen 5 und 10 liegen. Der Standardwert ist 5.

```
"tests":[
   {
      "name":"my_mqtt_reconnect_backoff_retries_on_server_disconnect",
      "configuration":{
         // optional:
         "EXECUTION_TIMEOUT":"300",  // in seconds
         "RECONNECTION_ATTEMPTS": 5
      },
      "test":{
         "id":"MQTT_Reconnect_Backoff_Retries_On_Server_Disconnect",
```

```
         "version":"0.0.0"
      }
   }
]
```

„Device re-connect with jitter backoff - On unstable connection“

Überprüft, ob ein getestetes Gerät beim erneuten Herstellen der Verbindung über eine instabile Verbindung die erforderlichen Jitter- und Backoff-Werte verwendet. Device Advisor trennt das Gerät nach fünf erfolgreichen Verbindungen vom Server und beobachtet das Verhalten des Geräts bei MQTT der Wiederverbindung. Device Advisor protokolliert den Zeitstempel der CONNECT Anfrage für das zu testende Gerät, führt eine Paketvalidierung durch, sendet zurück, trennt die VerbindungCONNACK, protokolliert den Zeitstempel der Verbindungsunterbrechung und wartet, bis das zu testende Gerät die Anfrage erneut sendet. Die gesammelten Zeitstempel werden verwendet, um zu überprüfen, ob das getestete Gerät Jitter und Backoff verwendet, während es nach erfolgreichen, aber instabilen Verbindungen erneut eine Verbindung herstellt. Wenn das getestete Gerät eine streng exponentielle Backoff-Verzögerung aufweist oder keinen ordnungsgemäßen Jitter-Backoff-Mechanismus implementiert, wird dieser Testfall mit Warnungen bestanden. Wenn das getestete Gerät entweder einen linearen Backoff-Mechanismus oder einen konstanten Backoff-Mechanismus implementiert hat, schlägt der Test fehl.

Damit dieser Testfall bestanden wird, empfehlen wir, den Mechanismus Exponential Backoff And Jitter (Exponentielles Backoff und Jitter) auf dem getesteten Gerät zu implementieren.

APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 4 Minuten.
> Die Anzahl der Wiederverbindungsversuche zur Überprüfung des Backoffs kann durch Angabe der `RECONNECTION_ATTEMPTS` geändert werden. Die Zahl muss zwischen 5 und 10 liegen. Der Standardwert ist 5.

```
"tests":[
   {
      "name":"my_mqtt_reconnect_backoff_retries_on_unstable_connection",
      "configuration":{
```

```
         // optional:
         "EXECUTION_TIMEOUT":"300",  // in seconds
         "RECONNECTION_ATTEMPTS": 5
      },
      "test":{
         "id":"MQTT_Reconnect_Backoff_Retries_On_Unstable_Connection",
         "version":"0.0.0"
      }
   }
]
```

## Veröffentlichen

„QoS0 (Happy Case)“

Überprüft, ob das getestete Gerät eine Nachricht mit QoS0 oder QoS1 veröffentlicht. Sie können auch das Thema der Nachricht und die Nutzlast überprüfen, indem Sie den Themenwert und die Nutzlast in den Testeinstellungen angeben.

> **Note**
>
> EXECUTION_TIMEOUT hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten.

```
"tests":[
   {
      "name":"my_mqtt_publish_test",
      "configuration":{
         // optional:
         "EXECUTION_TIMEOUT":"300",  // in seconds
         "TOPIC_FOR_PUBLISH_VALIDATION": "my_TOPIC_FOR_PUBLISH_VALIDATION",
         "PAYLOAD_FOR_PUBLISH_VALIDATION": "my_PAYLOAD_FOR_PUBLISH_VALIDATION",
      },
      "test":{
         "id":"MQTT_Publish",
         "version":"0.0.0"
      }
   }
]
```

„Wiederholung der QoS1-Veröffentlichung — Nein“ PUBACK

Überprüft, ob das zu testende Gerät eine mit QoS1 gesendete Nachricht erneut veröffentlicht, falls der Broker sie nicht sendet. PUBACK Sie können auch das Thema der Nachricht überprüfen, indem Sie dieses Thema in den Testeinstellungen angeben. Das Client-Gerät darf die Verbindung nicht trennen, bevor die Nachricht erneut veröffentlicht wird. Mit diesem Test wird auch überprüft, ob die erneut veröffentlichte Nachricht dieselbe Paket-ID wie das Original hat. Wenn das Gerät während der Testausführung die Verbindung verliert und die Verbindung wiederherstellt, wird der Testfall ohne Fehler zurückgesetzt und das Gerät muss die Testfallschritte erneut ausführen.

APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Es wird eine Dauer von mindestens 4 Minuten empfohlen.

```
"tests":[
   {
      "name":"my_mqtt_publish_retry_test",
      "configuration":{
         // optional:
         "EXECUTION_TIMEOUT":"300",  // in seconds
         "TOPIC_FOR_PUBLISH_VALIDATION": "my_TOPIC_FOR_PUBLISH_VALIDATION",
         "PAYLOAD_FOR_PUBLISH_VALIDATION": "my_PAYLOAD_FOR_PUBLISH_VALIDATION",
      },
      "test":{
         "id":"MQTT_Publish_Retry_No_Puback",
         "version":"0.0.0"
      }
   }
]
```

„Publish Retained messages“

Überprüft, ob das getestete Gerät eine Nachricht veröffentlicht, bei der `retainFlag` auf „true“ gesetzt ist. Sie können das Thema der Nachricht und die Nutzlast überprüfen, indem Sie den Themenwert und die Nutzlast in den Testeinstellungen angeben. Wenn der im PUBLISH Paket `retainFlag` gesendete Wert nicht auf true gesetzt ist, schlägt der Testfall fehl.

APITestfalldefinition:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten. Um diesen Testfall auszuführen, fügen Sie die `iot:RetainPublish`-Aktion zu Ihrer Geräterolle hinzu.

```
"tests":[
   {
      "name":"my_mqtt_publish_retained_messages_test",
      "configuration":{
         // optional:
         "EXECUTION_TIMEOUT":"300",  // in seconds

 "TOPIC_FOR_PUBLISH_RETAINED_VALIDATION": "my_TOPIC_FOR_PUBLISH_RETAINED_VALIDATION",

 "PAYLOAD_FOR_PUBLISH_RETAINED_VALIDATION": "my_PAYLOAD_FOR_PUBLISH_RETAINED_VALIDATION",
      },
      "test":{
         "id":"MQTT_Publish_Retained_Messages",
         "version":"0.0.0"
      }
   }
]
```

„Publish with User Property“

Überprüft, ob das getestete Gerät eine Nachricht mit der korrekten Benutzereigenschaft veröffentlicht. Sie können die Benutzereigenschaft überprüfen, indem Sie das Name-Wert-Paar in den Testeinstellungen festlegen. Wenn die Benutzereigenschaft nicht bereitgestellt wird oder nicht übereinstimmt, schlägt der Testfall fehl.

APIDefinition des Testfalls:

> **Note**
>
> Dies ist MQTT5 nur ein Testfall.

EXECUTION_TIMEOUT hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten.

```
"tests":[
   {
      "name":"my_mqtt_user_property_test",
      "test":{
        "USER_PROPERTIES": [
            {"name": "name1", "value":"value1"},
            {"name": "name2", "value":"value2"}
        ],
        "EXECUTION_TIMEOUT":"300",  // in seconds
      },
      "test":{
         "id":"MQTT_Publish_User_Property",
         "version":"0.0.0"
      }
   }
]
```

## Abonnieren

„Can Subscribe (Happy Case)“

Überprüft, ob das zu testende Gerät Themen abonniert hat. MQTT Sie können auch das Thema überprüfen, das das getestete Gerät abonniert, indem Sie dieses Thema in den Testeinstellungen angeben.

APIDefinition des Testfalls:

> **Note**
>
> EXECUTION_TIMEOUT hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten.

```
"tests":[
   {
      "name":"my_mqtt_subscribe_test",
```

```
      "configuration":{
         // optional:
         "EXECUTION_TIMEOUT":"300",  // in seconds
         "TOPIC_LIST_FOR_SUBSCRIPTION_VALIDATION":
["my_TOPIC_FOR_PUBLISH_VALIDATION_a","my_TOPIC_FOR_PUBLISH_VALIDATION_b"]
      },
      "test":{
         "id":"MQTT_Subscribe",
         "version":"0.0.0"
      }
   }
]
```

„Abonnieren, erneut versuchen — NeinSUBACK“

Überprüft, ob das getestete Gerät erneut versucht, Themen zu abonnieren, die fehlgeschlagen sind. MQTT Der Server wartet dann und sendet keine. SUBACK Wenn das Client-Gerät das Abonnement nicht erneut versucht, schlägt der Test fehl. Das Client-Gerät muss das fehlgeschlagene Abonnement mit derselben Paket-ID erneut versuchen. Sie können auch das Thema überprüfen, das das getestete Gerät abonniert, indem Sie dieses Thema in den Testeinstellungen angeben. Wenn das Gerät während der Testausführung die Verbindung verliert und die Verbindung wiederherstellt, wird der Testfall ohne Fehler zurückgesetzt und das Gerät muss die Testfallschritte erneut ausführen.

APITestfalldefinition:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 4 Minuten.

```
"tests":[
   {
      "name":"my_mqtt_subscribe_retry_test",
      "configuration":{
         "EXECUTION_TIMEOUT":"300",  // in seconds
         // optional:
         "TOPIC_LIST_FOR_SUBSCRIPTION_VALIDATION":
["myTOPIC_FOR_PUBLISH_VALIDATION_a","my_TOPIC_FOR_PUBLISH_VALIDATION_b"]
      },
```

```
      "test":{
         "id":"MQTT_Subscribe_Retry_No_Suback",
         "version":"0.0.0"
      }
   }
]
```

## Keep-Alive

„Matt Nein Ack“ PingResp

Dieser Testfall überprüft, ob das getestete Gerät die Verbindung trennt, wenn es keine Ping-Antwort erhält. Im Rahmen dieses Testfalls blockiert Device Advisor Antworten von AWS IoT Core Veröffentlichungs-, Abonnement- und Ping-Anfragen. Außerdem wird überprüft, ob das getestete Gerät die MQTT Verbindung unterbricht.

APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen ein Timeout, das mehr als das 1,5-fache des `keepAliveTime`-Werts beträgt.
> Die maximale `keepAliveTime` darf für diesen Test nicht länger als 230 Sekunden betragen.

```
"tests":[
    {
       "name":"Mqtt No Ack PingResp",
       "configuration":
          //optional:
          "EXECUTION_TIMEOUT":"306",   // in seconds
       },
       "test":{
          "id":"MQTT_No_Ack_PingResp",
          "version":"0.0.0"
       }
    }
]
```

## Persistente Sitzung

„Persistent Session (Happy Case)“

Dieser Testfall validiert das Geräteverhalten, wenn die Verbindung zu einer persistenten Sitzung getrennt wird. Der Testfall prüft, ob das Gerät erneut eine Verbindung herstellen kann, die Abonnements für seine Trigger-Themen fortsetzen kann, ohne sich explizit erneut anzumelden, die in den Themen gespeicherten Nachrichten empfangen kann und während einer persistenten Sitzung erwartungsgemäß funktionieren kann. Wenn dieser Testfall erfolgreich ist, bedeutet dies, dass das Client-Gerät in der Lage ist, eine dauerhafte Sitzung mit dem AWS IoT Core Broker wie erwartet aufrechtzuerhalten. Weitere Informationen zu AWS IoT persistenten Sitzungen finden Sie unter Verwenden MQTT persistenter Sitzungen.

In diesem Testfall wird erwartet, dass das Client-Gerät das Flag AWS IoT Core with a clean session auf false gesetzt hat und dann ein Trigger-Thema abonniert. CONNECT Nach einem erfolgreichen Abonnement wird das Gerät von AWS IoT Core Device Advisor getrennt. Solange sich das Gerät in einem getrennten Zustand befindet, wird eine QoS 1-Nachrichtennutzlast in diesem Thema gespeichert. Device Advisor ermöglicht dem Client-Gerät dann, erneut eine Verbindung mit dem Testendpunkt herzustellen. Da zu diesem Zeitpunkt eine persistente Sitzung besteht, wird erwartet, dass das Client-Gerät seine Themenabonnements wieder aufnimmt, ohne zusätzliche SUBSCRIBE Pakete zu senden, und die QoS 1-Nachricht vom Broker empfängt. Wenn das Client-Gerät nach der erneuten Verbindung sein Trigger-Thema erneut abonniert, indem es ein zusätzliches SUBSCRIBE Paket sendet und/oder wenn der Client die gespeicherte Nachricht vom Trigger-Thema nicht empfängt, schlägt der Testfall fehl.

APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von mindestens 4 Minuten. Bei der ersten Verbindung muss das Client-Gerät explizit ein `TRIGGER_TOPIC` abonnieren, die zuvor nicht abonniert wurde. Um den Testfall zu bestehen, muss das Client-Gerät erfolgreich `TRIGGER_TOPIC` mit einer QoS 1 abonnieren. Nach dem erneuten Herstellen der Verbindung wird erwartet, dass das Client-Gerät erkennt, dass eine aktive persistente Sitzung besteht. Daher sollte es die gespeicherte Nachricht akzeptieren, die vom Trigger-Thema gesendet wurde, und PUBACK für diese spezifische Nachricht zurückkehren.

```
"tests":[
   {
      "name":"my_mqtt_persistent_session_happy_case",
      "configuration":{
         //required:
         "TRIGGER_TOPIC": "myTrigger/topic",
         // optional:
         // if Payload not provided, a string will be stored in the trigger topic to
 be sent back to the client device
         "PAYLOAD": "The message which should be received from AWS IoT Broker after
 re-connecting to a persistent session from the specified trigger topic.",

         "EXECUTION_TIMEOUT":"300" // in seconds
      },
      "test":{
         "id":"MQTT_Persistent_Session_Happy_Case",
         "version":"0.0.0"
      }
   }
]
```

„Persistent Session - Session Expiry“

Dieser Testfall hilft bei der Überprüfung des Geräteverhaltens, wenn ein getrenntes Gerät erneut eine Verbindung zu einer abgelaufenen persistenten Sitzung herstellt. Nach Ablauf der Sitzung erwarten wir, dass das Gerät die zuvor abonnierten Themen erneut abonniert, indem es explizit ein neues Paket sendet. SUBSCRIBE

Während der ersten Verbindung erwarten wir, dass das Testgerät CONNECT mit dem AWS IoT-Broker verbunden ist, da sein `CleanSession` Flag auf False gesetzt ist, um eine persistente Sitzung zu initiieren. Das Gerät sollte dann ein Trigger-Thema abonnieren. Nach einem erfolgreichen Abonnement und der Initiierung einer dauerhaften Sitzung wird das AWS IoT Core Gerät dann von Device Advisor getrennt. Nach dem Trennen der Verbindung ermöglicht AWS IoT Core Device Advisor dem Testgerät, sich wieder mit dem Testendpunkt zu verbinden. Wenn das Testgerät zu diesem Zeitpunkt ein weiteres CONNECT Paket sendet, sendet AWS IoT Core Device Advisor ein CONNACK Paket zurück, das angibt, dass die persistente Sitzung abgelaufen ist. Das Testgerät muss dieses Paket richtig interpretieren und es wird erwartet, dass es dasselbe Trigger-Thema erneut abonniert, wenn die persistente Sitzung beendet wird. Wenn das Testgerät seinen Themen-Trigger nicht erneut abonniert, schlägt der Testfall fehl. Damit der

Test erfolgreich ist, muss das Gerät erkennen, dass die persistente Sitzung beendet ist, und in der zweiten Verbindung ein neues SUBSCRIBE Paket für dasselbe Trigger-Thema zurücksenden.

Wenn dieser Testfall für ein Testgerät erfolgreich ist, bedeutet dies, dass das Gerät in der Lage ist, die erneute Verbindung nach Ablauf der persistenten Sitzung erwartungsgemäß zu handhaben.

APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von mindestens 4 Minuten. Das Testgerät muss explizit ein `TRIGGER_TOPIC` abonnieren, das es zuvor nicht abonniert hatte. Um den Testfall zu bestehen, muss das Testgerät ein CONNECT Paket mit einem auf False gesetzten `CleanSession` Flag senden und erfolgreich ein Trigger-Thema mit QoS 1 abonnieren. Nach einer erfolgreichen Verbindung trennt AWS IoT Core Device Advisor die Verbindung zum Gerät. Nach dem Trennen der Verbindung ermöglicht AWS IoT Core Device Advisor dem Gerät, wieder eine Verbindung herzustellen, und es wird erwartet, dass das Gerät dieselbe erneut abonniert, `TRIGGER_TOPIC` da AWS IoT Core Device Advisor die persistente Sitzung beendet hätte.

```
"tests":[
   {
      "name":"my_expired_persistent_session_test",
      "configuration":{
         //required:
         "TRIGGER_TOPIC": "myTrigger/topic",
         // optional:
         "EXECUTION_TIMEOUT":"300" // in seconds
      },
      "test":{
         "id":"MQTT_Expired_Persistent_Session",
         "version":"0.0.0"
      }
   }
]
```

# Shadow

Verwenden Sie diese Tests, um zu überprüfen, ob Ihre getesteten Geräte den AWS IoT Device Shadow-Dienst korrekt verwenden. Weitere Informationen finden Sie unter AWS IoT Device Shadow-Dienst. Wenn diese Testfälle in Ihrer Testsuite konfiguriert sind, müssen Sie beim Start der Suite-Ausführung etwas angeben.

MQTTOver WebSocket wird derzeit nicht unterstützt.

## Veröffentlichen

„Device publishes state after it connects (Happy case)“

Überprüft, ob ein Gerät seinen Status veröffentlichen kann, nachdem es eine Verbindung hergestellt hat AWS IoT Core

APITestfalldefinition:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten.

```
"tests":[
   {
      "name":"my_shadow_publish_reported_state",
      "configuration": {
         // optional:
         "EXECUTION_TIMEOUT":"300", // in seconds
         "SHADOW_NAME": "SHADOW_NAME",
         "REPORTED_STATE": {
            "STATE_ATTRIBUTE": "STATE_VALUE"
         }
      },
      "test":{
         "id":"Shadow_Publish_Reported_State",
         "version":"0.0.0"
      }
   }
]
```

Der `REPORTED_STATE` kann für eine zusätzliche Überprüfung des exakten Shadow-Status Ihres Geräts bereitgestellt werden, nachdem es eine Verbindung hergestellt hat. Standardmäßig überprüft dieser Testfall den Veröffentlichungsstatus Ihres Geräts.

Falls *`SHADOW_NAME`* nicht angegeben, sucht der Testfall standardmäßig nach Nachrichten, die mit Themenpräfixen des Shadow-Typs Unbenannt (klassisch) veröffentlicht wurden. Geben Sie einen Shadow-Namen an, wenn Ihr Gerät den benannten Shadow-Typ verwendet. Weitere Informationen finden Sie unter Verwenden von Shadows in Geräten.

## Aktualisierung

„Device updates reported state to desired state (Happy case)“

Überprüft, ob Ihr Gerät alle empfangenen Aktualisierungsnachrichten liest, und synchronisiert den Status des Geräts so, dass er mit den gewünschten Statuseigenschaften übereinstimmt. Ihr Gerät sollte nach der Synchronisierung den zuletzt gemeldeten Status veröffentlichen. Wenn auf Ihrem Gerät bereits ein Shadow vorhanden ist, bevor Sie den Test ausführen, stellen Sie sicher, dass der für den Testfall konfigurierte gewünschte Status und der vorhandene gemeldete Status nicht bereits übereinstimmen. Sie können die von Device Advisor gesendeten Shadow-Aktualisierungsnachrichten anhand des ClientTokenFelds im Shadow-Dokument erkennen, wie es sein wird`DeviceAdvisorShadowTestCaseSetup`.

APIDefinition des Testfalls:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 2 Minuten.

```
"tests":[
   {
      "name":"my_shadow_update_reported_state",
      "configuration": {
         "DESIRED_STATE": {
            "STATE_ATTRIBUTE": "STATE_VALUE"
         },
         // optional:
         "EXECUTION_TIMEOUT":"300", // in seconds
```

```
            "SHADOW_NAME": "SHADOW_NAME"
        },
        "test":{
            "id":"Shadow_Update_Reported_State",
            "version":"0.0.0"
        }
    }
]
```

Der `DESIRED_STATE` sollte mindestens ein Attribut und einen zugehörigen Wert haben.

Falls `SHADOW_NAME` nicht angegeben, sucht der Testfall standardmäßig nach Nachrichten, die mit Themenpräfixen des Shadow-Typs Unbenannt (klassisch) veröffentlicht wurden. Geben Sie einen Shadow-Namen an, wenn Ihr Gerät den benannten Shadow-Typ verwendet. Weitere Informationen finden Sie unter Verwenden von Shadows in Geräten.

## Auftragsausführung

„Device can complete a job execution“

Mit diesem Testfall können Sie überprüfen, ob Ihr Gerät Updates mithilfe von AWS IoT Jobs empfangen kann, und den Status erfolgreicher Updates veröffentlichen. Weitere Informationen zu AWS IoT Jobs finden Sie unter Jobs.

Um diesen Testfall erfolgreich ausführen zu können, gibt es zwei reservierte AWS Themen, denen Sie Ihre Geräterolle zuweisen müssen. Verwenden Sie die Themen notify und notify-next, um Nachrichten zu Auftragsaktivitäten zu abonnieren. Ihre Geräterolle muss PUBLISH Aktionen für die folgenden Themen gewähren:

- $aws/things/ /jobs/ /get thingNamejobId
- $aws/things/ /jobs/ thingName/update jobId

Es wird empfohlen, Zuschüsse und Maßnahmen für die folgenden Themen bereitzustellen: SUBSCRIBE RECEIVE

- $aws/things//thingNamejobs/get/accepted
- $aws/things/ /jobs/ thingName/get/rejected jobId
- $aws/things/ /jobs/ thingName/update/akzeptiert jobId
- $aws/things/ /jobs/ thingName/update/abgelehnt jobId

Es wird empfohlen, Maßnahmen für das folgende Thema zu gewähren: SUBSCRIBE

- $aws/things/ /jobs/notify-next thingName

Weitere Informationen zu diesen reservierten Themen finden Sie unter Reservierte Themen für AWS IoT -Aufträge.

MQTTOver wird WebSocket derzeit nicht unterstützt.

APITestfalldefinition:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 5 Minuten. Wir empfehlen einen Timeout-Wert von 3 Minuten. Passen Sie je nach dem bereitgestellten AWS IoT Jobdokument oder der angegebenen Quelle den Timeout-Wert an (wenn die Ausführung eines Jobs beispielsweise lange dauert, definieren Sie einen längeren Timeout-Wert für den Testfall). Um den Test auszuführen, ist entweder ein gültiges AWS IoT Jobdokument oder eine bereits vorhandene Job-ID erforderlich. Ein AWS IoT Jobdokument kann als JSON Dokument oder als S3-Link bereitgestellt werden. Wenn ein Auftragsdokument bereitgestellt wird, ist die Angabe einer Auftrags-ID optional. Wenn eine Job-ID angegeben wird, verwendet Device Advisor diese ID bei der Erstellung des AWS IoT Jobs in Ihrem Namen. Wenn das Auftragsdokument nicht bereitgestellt wird, können Sie eine vorhandene ID angeben, die sich in derselben Region befindet, in der Sie den Testfall ausführen. In diesem Fall verwendet Device Advisor diesen AWS IoT Job bei der Ausführung des Testfalls.

```
"tests": [
   {
      "name":"my_job_execution",
      "configuration": {
         // optional:
         // Test case will create a job task by using either JOB_DOCUMENT or
 JOB_DOCUMENT_SOURCE.
         // If you manage the job task on your own, leave it empty and provide the
 JOB_JOBID (self-managed job task).
         // JOB_DOCUMENT is a JSON formatted string
         "JOB_DOCUMENT": "{
            \"operation\":\"reboot\",
            \"files\" : {
```

```
                \"fileName\" : \"install.py\",
                \"url\" : \"${aws:iot:s3-presigned-url:https://s3.amazonaws.com/
bucket-name/key}\"
             }
          }",
          // JOB_DOCUMENT_SOURCE is an S3 link to the job document. It will be used
 only if JOB_DOCUMENT is not provided.
          "JOB_DOCUMENT_SOURCE": "https://s3.amazonaws.com/bucket-name/key",
          // JOB_JOBID is mandatory, only if neither document nor document source is
 provided. (Test case needs to know the self-managed job task id).
          "JOB_JOBID": "String",
          // JOB_PRESIGN_ROLE_ARN is used for the presign Url, which will replace the
 placeholder in the JOB_DOCUMENT field
          "JOB_PRESIGN_ROLE_ARN": "String",
          // Presigned Url expiration time. It must be between 60 and 3600 seconds,
 with the default value being 3600.
          "JOB_PRESIGN_EXPIRES_IN_SEC": "Long"
          "EXECUTION_TIMEOUT": "300", // in seconds
      },
      "test": {
         "id": "Job_Execution",
         "version": "0.0.0"
      }
   }
]
```

Weitere Informationen zum Erstellen und Verwenden von Auftragsdokumenten finden Sie im Auftragsdokument.

## Berechtigungen und Richtlinien

Mithilfe der folgenden Tests können Sie feststellen, ob die mit den Zertifikaten Ihrer Geräte verknüpften Richtlinien den bewährten Standardmethoden entsprechen.

MQTTOver WebSocket wird derzeit nicht unterstützt.

„Device certificate attached policies don’t contain wildcards“

Überprüft, ob die mit einem Gerät verknüpften Berechtigungsrichtlinien bewährten Methoden entsprechen und dem Gerät nicht mehr Berechtigungen als erforderlich gewähren.

APITestfalldefinition:

> **Note**
>
> `EXECUTION_TIMEOUT` hat einen Standardwert von 1 Minute. Wir empfehlen, ein Timeout von mindestens 30 Sekunden festzulegen.

```
"tests":[
   {
        "name":"my_security_device_policies",
        "configuration": {
            // optional:
            "EXECUTION_TIMEOUT":"60"    // in seconds
        },
        "test": {
            "id": "Security_Device_Policies",
            "version": "0.0.0"
        }
    }
]
```

## Tests mit langer Dauer

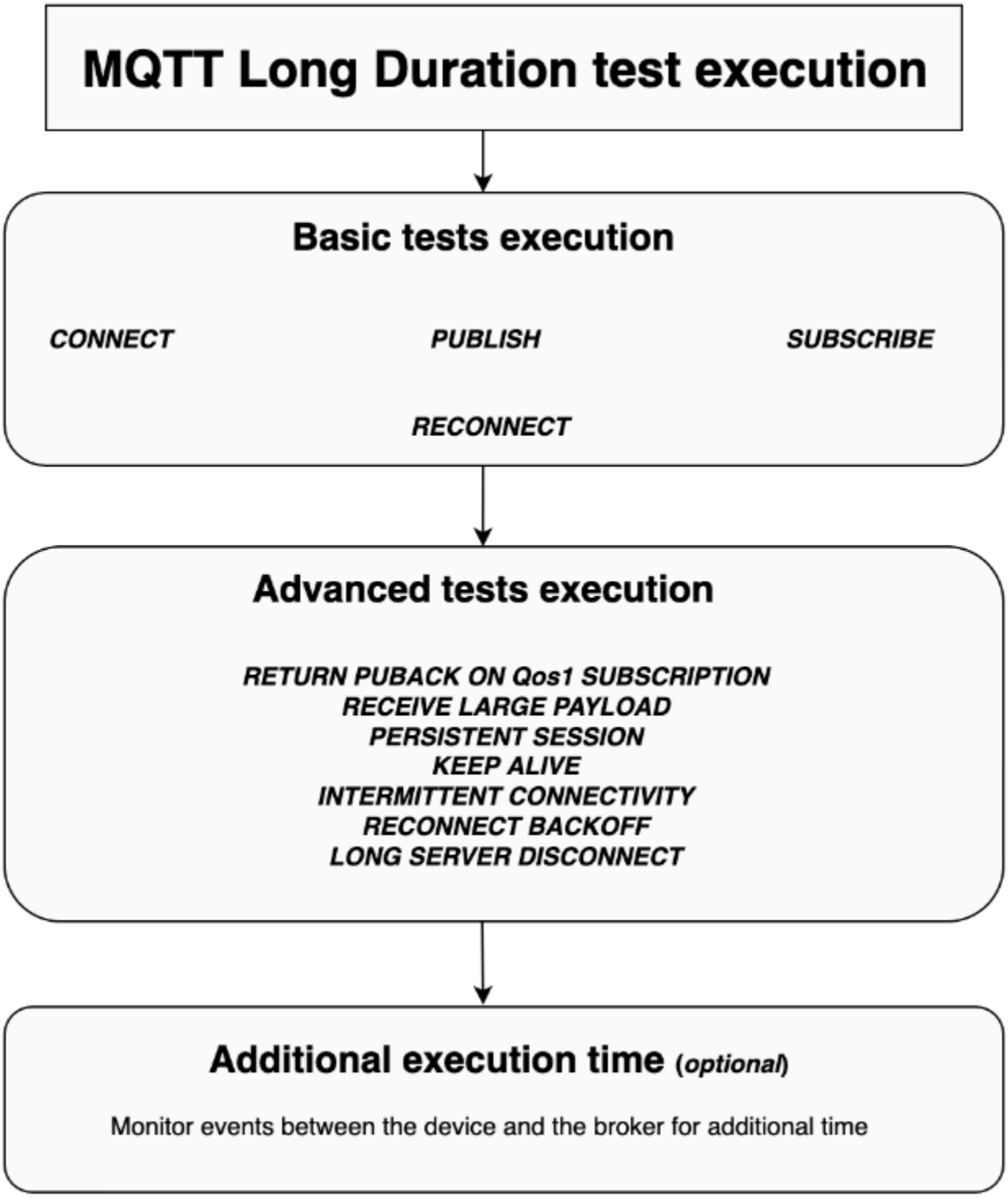
Tests mit langer Dauer sind eine neue Testsuite, die das Verhalten eines Geräts überwacht, wenn es über einen längeren Zeitraum betrieben wird. Im Vergleich zur Durchführung einzelner Tests, die sich auf bestimmte Verhaltensweisen eines Geräts konzentrieren, untersucht der Tests mit langer Dauer das Verhalten des Geräts in einer Vielzahl von realen Szenarien über die gesamte Lebensdauer des Geräts. Device Advisor orchestriert die Tests in der effizientesten Reihenfolge. Der Test generiert Ergebnisse und Protokolle, einschließlich eines Übersichtsprotokolls mit nützlichen Messwerten zur Leistung des Geräts während des Tests.

### MQTTTestfall mit langer Dauer

Im MQTT Langzeittestfall wird das Verhalten des Geräts zunächst in Happy Case-Szenarien wie MQTT Connect, Subscribe, Publish und Reconnect beobachtet. Anschließend wird das Gerät in mehreren komplexen Ausfallszenarien wie MQTT Reconnect Backoff, Long Server Disconnect und Intermittent Connectivity beobachtet.

## MQTTAblauf der Ausführung von Testfällen mit langer Dauer

Die Ausführung eines Testfalls mit MQTT langer Dauer besteht aus drei Phasen:



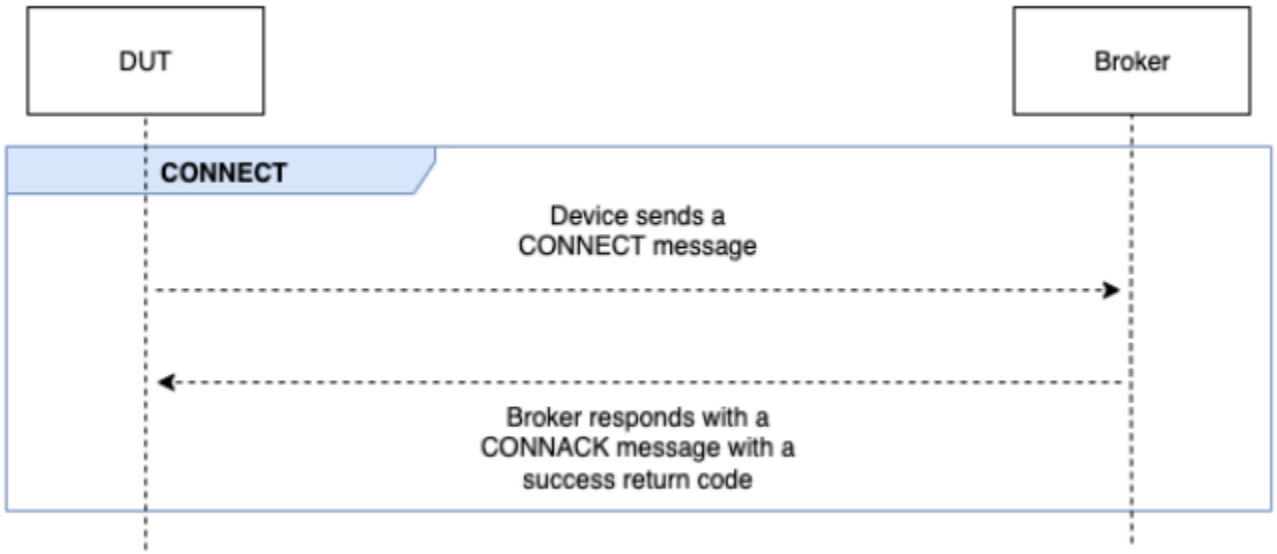
Grundlegende Testausführung

In dieser Phase führt der Testfall einfache Tests parallel durch. Der Test überprüft, ob für das Gerät die in der Konfiguration ausgewählten Operationen ausgewählt wurden.

Die grundlegenden Tests können je nach den ausgewählten Vorgängen Folgendes umfassen:

CONNECT

In diesem Szenario wird überprüft, ob das Gerät eine erfolgreiche Verbindung mit dem Broker herstellen kann.

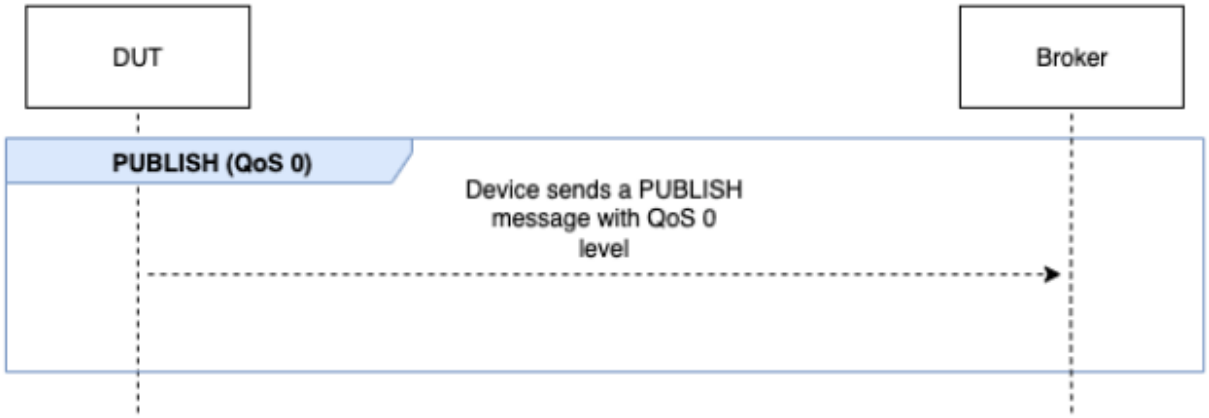



PUBLISH

In diesem Szenario wird überprüft, ob das Gerät erfolgreich beim Broker veröffentlicht.

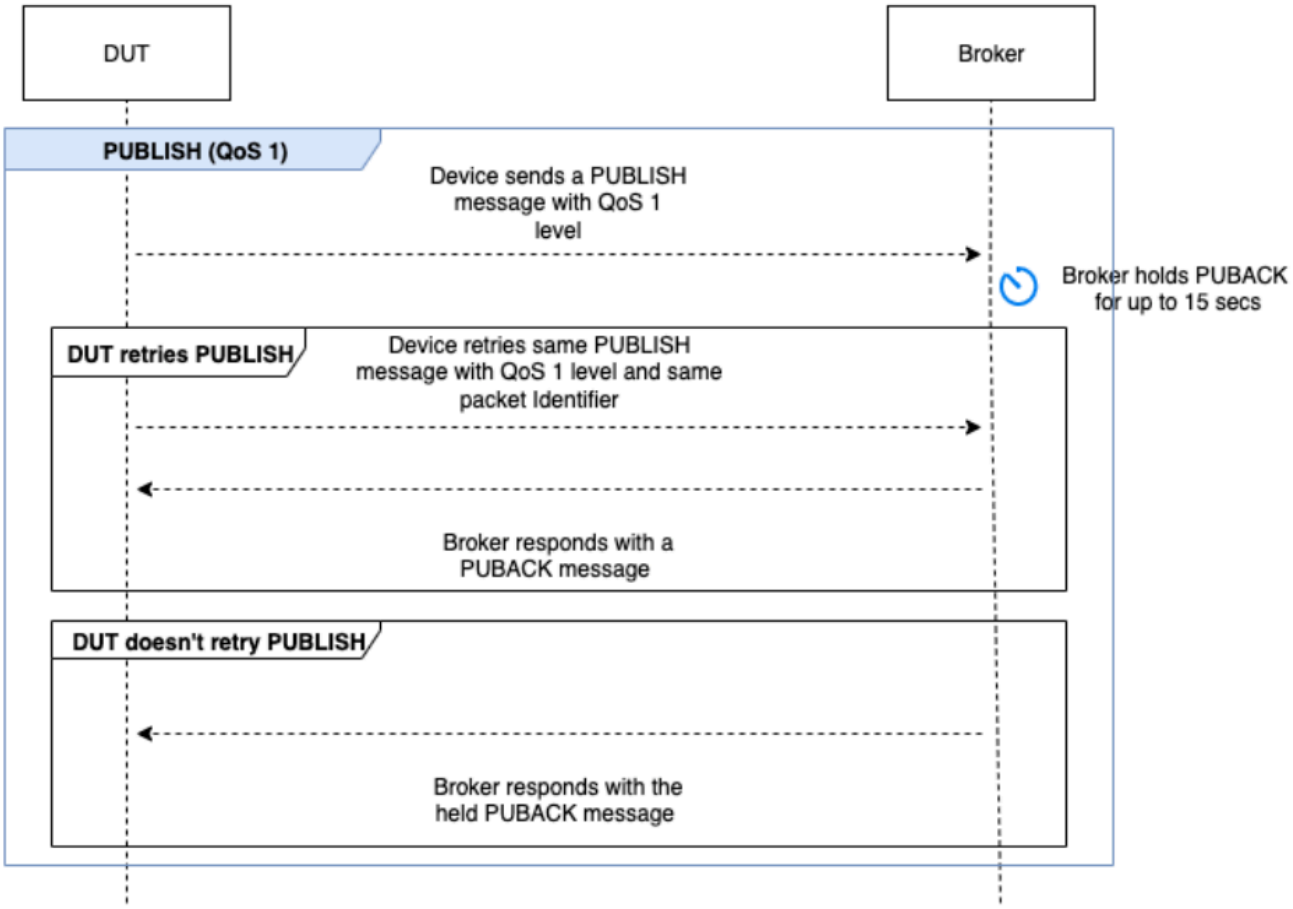
QoS 0

Dieser Testfall überprüft, ob das Gerät während einer Veröffentlichung mit QoS 0 erfolgreich eine `PUBLISH`-Nachricht an den Broker sendet. Der Test wartet nicht darauf, dass die `PUBACK`-Nachricht vom Gerät empfangen wird.




QoS 0

In diesem Testfall wird erwartet, dass das Gerät zwei PUBLISH-Nachrichten mit QoS 1 an den Broker sendet. Nach der ersten PUBLISH-Nachricht wartet der Broker bis zu 15 Sekunden, bevor er antwortet. Das Gerät muss innerhalb des 15-Sekunden-Fensters die ursprüngliche PUBLISH-Nachricht mit derselben Paket-ID erneut versuchen. Ist dies der Fall, antwortet der Broker mit einer PUBACK-Nachricht und der Test wird validiert. Wenn das Gerät den PUBLISH-Versuch nicht wiederholt, wird das Original-PUBACK an das Gerät gesendet und der Test wird als Pass with warnings (Mit Warnungen bestanden) markiert, zusammen mit einer Systemnachricht. Wenn das Gerät während der Testausführung die Verbindung verliert und die Verbindung wiederherstellt, wird der Testszenario ohne Fehler zurückgesetzt und das Gerät muss die Schritte des Testszenarios erneut ausführen.

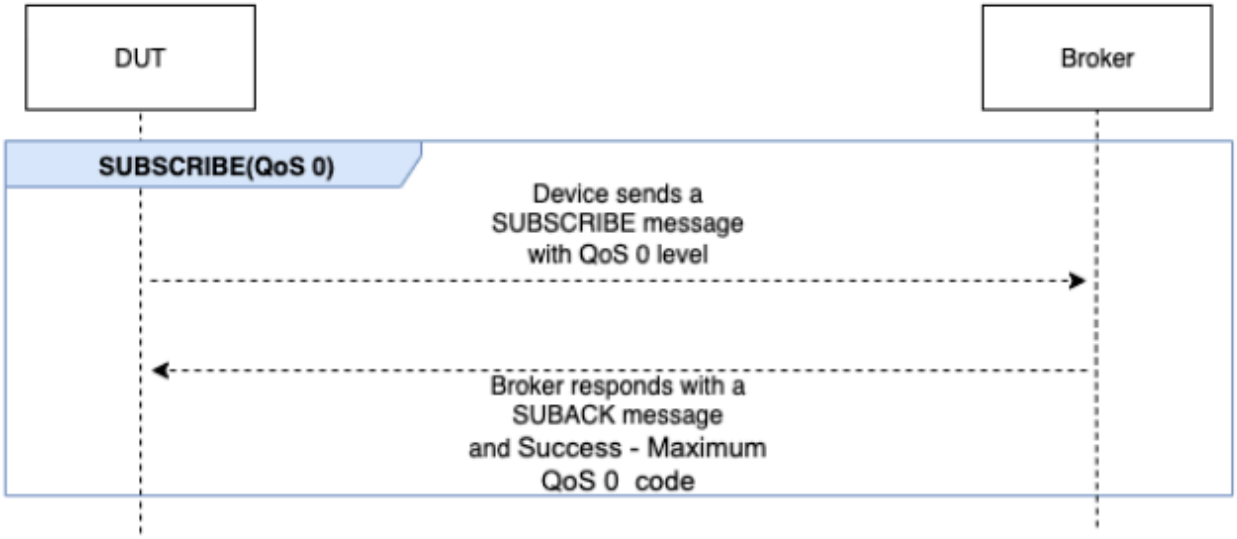



SUBSCRIBE

In diesem Szenario wird überprüft, ob das Gerät erfolgreich beim Broker abonniert.

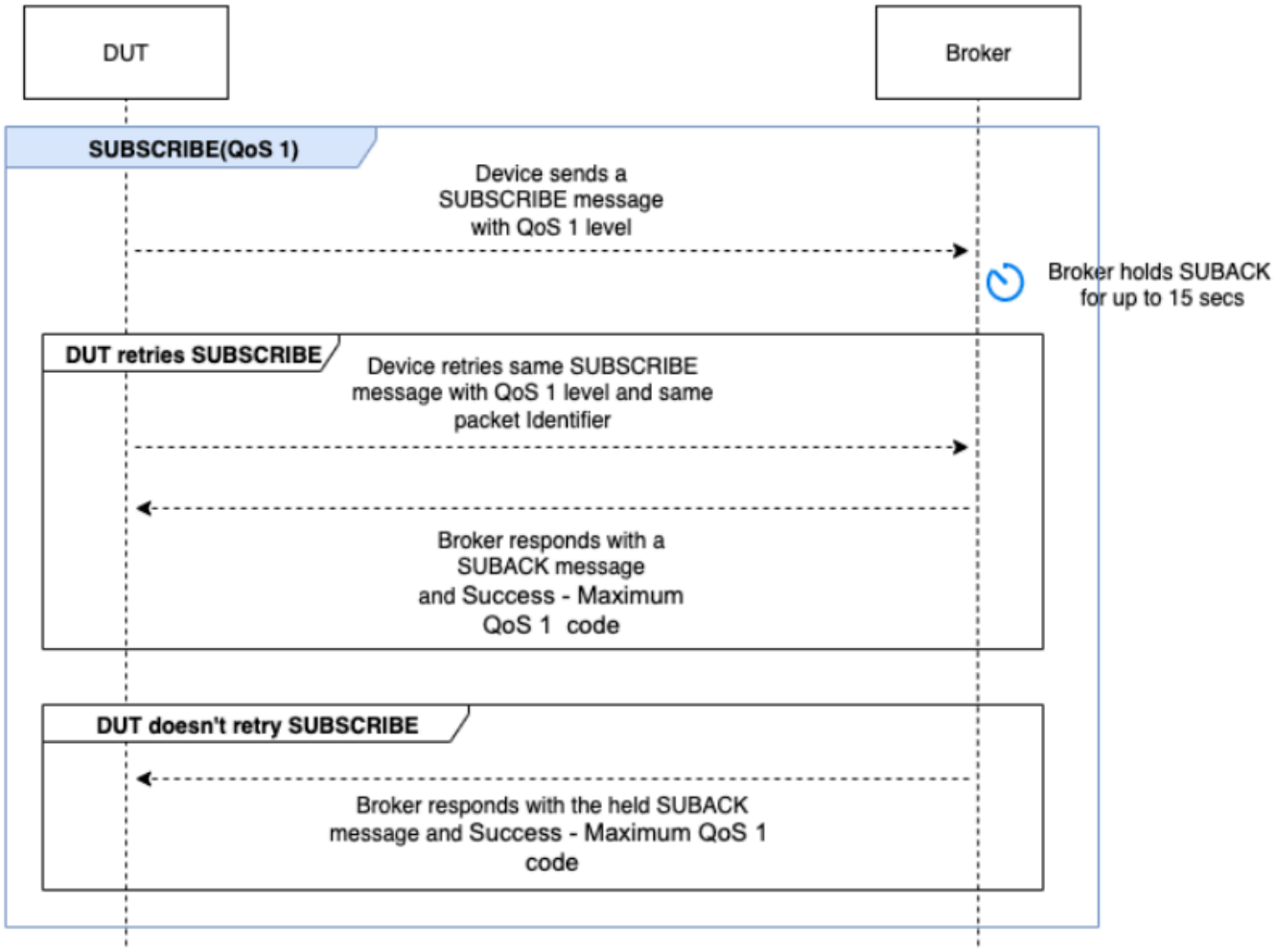
QoS 0

Dieser Testfall überprüft, ob das Gerät während eines Abonnements mit QoS 0 erfolgreich eine `SUBSCRIBE`-Nachricht an den Broker sendet. Der Test wartet nicht darauf, dass das Gerät eine SUBACK Nachricht empfängt.



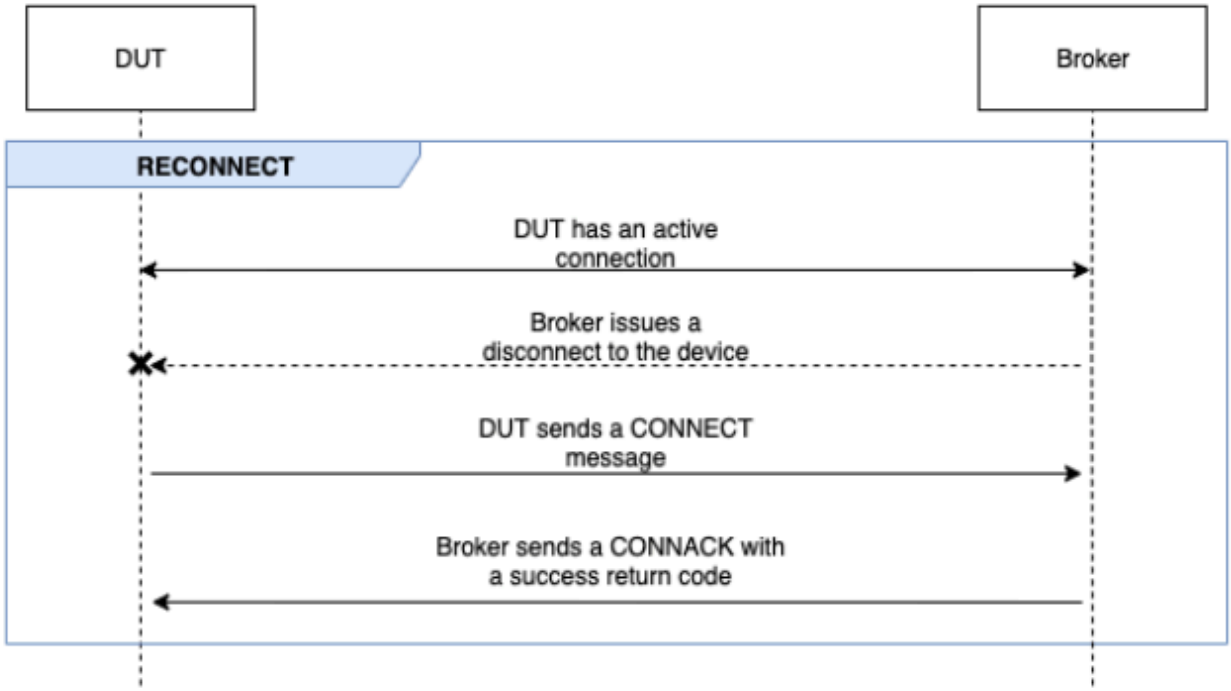

QoS 0

In diesem Testfall wird erwartet, dass das Gerät zwei SUBSCRIBE-Nachrichten mit QoS 1 an den Broker sendet. Nach der ersten SUBSCRIBE-Nachricht wartet der Broker bis zu 15 Sekunden, bevor er antwortet. Das Gerät muss innerhalb des 15-Sekunden-Fensters die ursprüngliche SUBSCRIBE-Nachricht mit derselben Paket-ID erneut versuchen. Ist dies der Fall, antwortet der Broker mit einer SUBACK-Nachricht und der Test wird validiert. Wenn das Gerät den SUBSCRIBE-Versuch nicht wiederholt, wird das Original-SUBACK an das Gerät gesendet und der Test wird als Pass with warnings (Mit Warnungen bestanden) markiert, zusammen mit einer Systemnachricht. Wenn das Gerät während der Testausführung die Verbindung verliert und die Verbindung wiederherstellt, wird der Testszenario ohne Fehler zurückgesetzt und das Gerät muss die Schritte des Testszenarios erneut ausführen.




RECONNECT

In diesem Szenario wird überprüft, ob das Gerät erfolgreich wieder eine Verbindung zum Broker herstellt, nachdem das Gerät von einer erfolgreichen Verbindung getrennt wurde. Device Advisor trennt das Gerät nicht, wenn es zuvor während der Testsuite mehr als einmal eine Verbindung hergestellt hat. Stattdessen wird der Test als Pass (Bestanden) markiert.



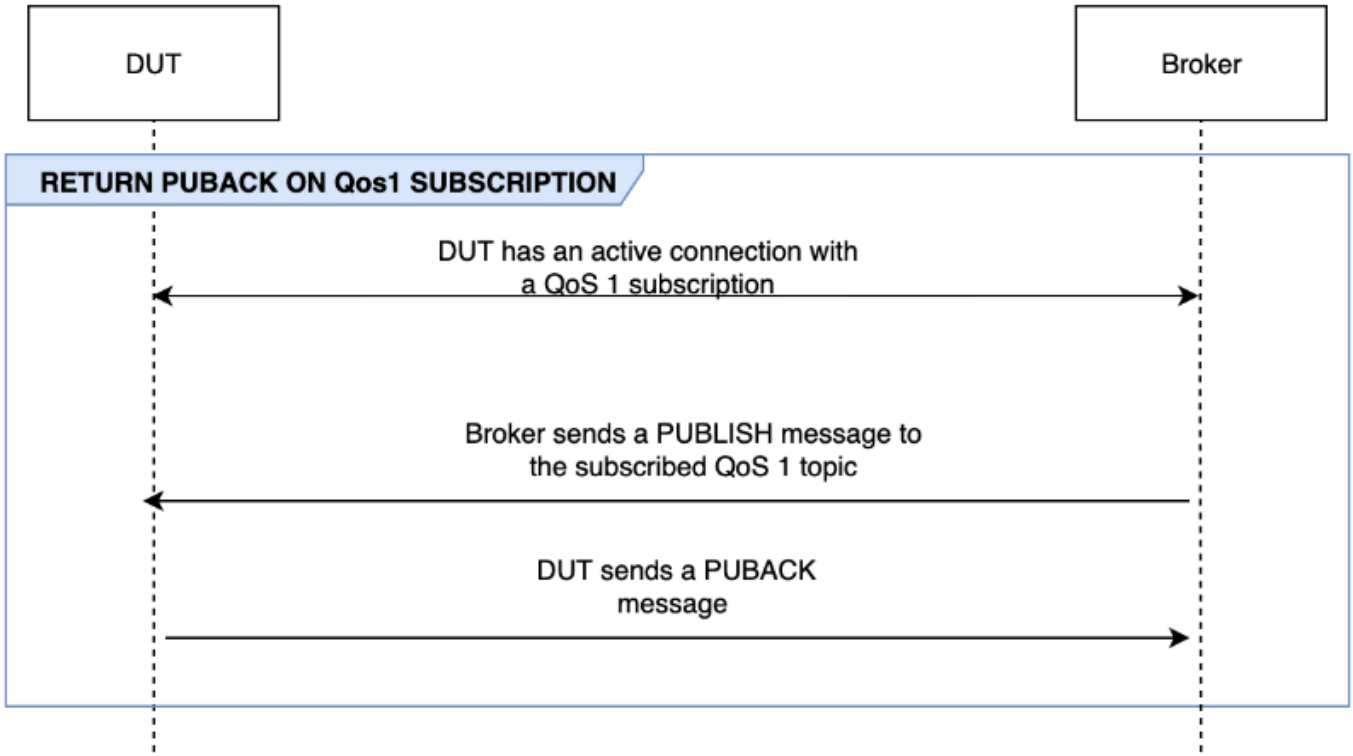

Erweiterte Testausführung

In dieser Phase führt der Testfall komplexere Tests seriell durch, um zu überprüfen, ob das Gerät den bewährten Methoden entspricht. Diese erweiterten Tests stehen zur Auswahl und können deaktiviert werden, falls sie nicht erforderlich sind. Jeder erweiterte Test hat seinen eigenen Timeout-Wert, der auf den Anforderungen des Szenarios basiert.

RETURNPUBACKAUF QoS 1 SUBSCRIPTION

> **Note**
>
> Wählen Sie dieses Szenario nur aus, wenn Ihr Gerät QoS 1-Abonnements ausführen kann.

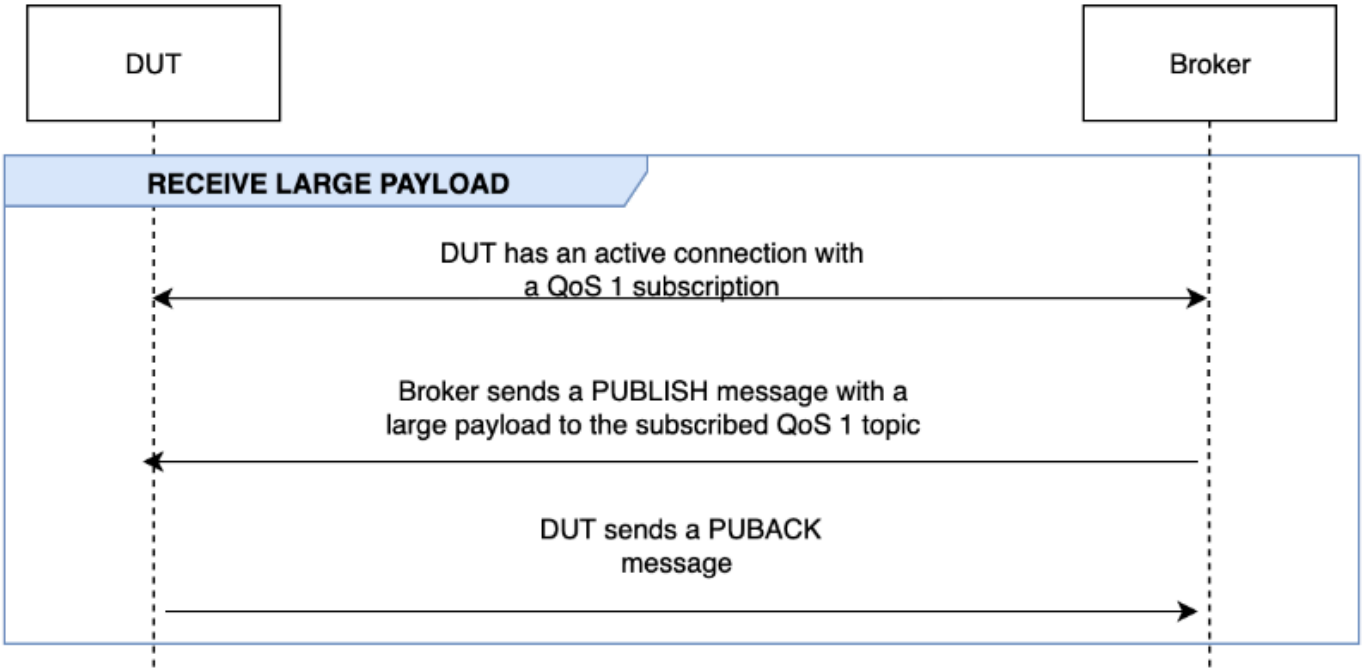
In diesem Szenario wird überprüft, ob das Gerät, nachdem es ein Thema abonniert und eine `PUBLISH`-Nachricht vom Broker erhalten hat, eine `PUBACK`-Nachricht zurückgibt.




RECEIVE LARGE PAYLOAD

> **Note**
>
> Wählen Sie dieses Szenario nur aus, wenn Ihr Gerät QoS 1-Abonnements ausführen kann.

In diesem Szenario wird überprüft, ob das Gerät mit einer `PUBACK`-Nachricht antwortet, nachdem es eine `PUBLISH`-Nachricht vom Broker für ein QoS 1-Thema mit einer großen Nutzlast erhalten hat. Das Format der erwarteten Nutzlast kann mit der `LONG_PAYLOAD_FORMAT`-Option konfiguriert werden.



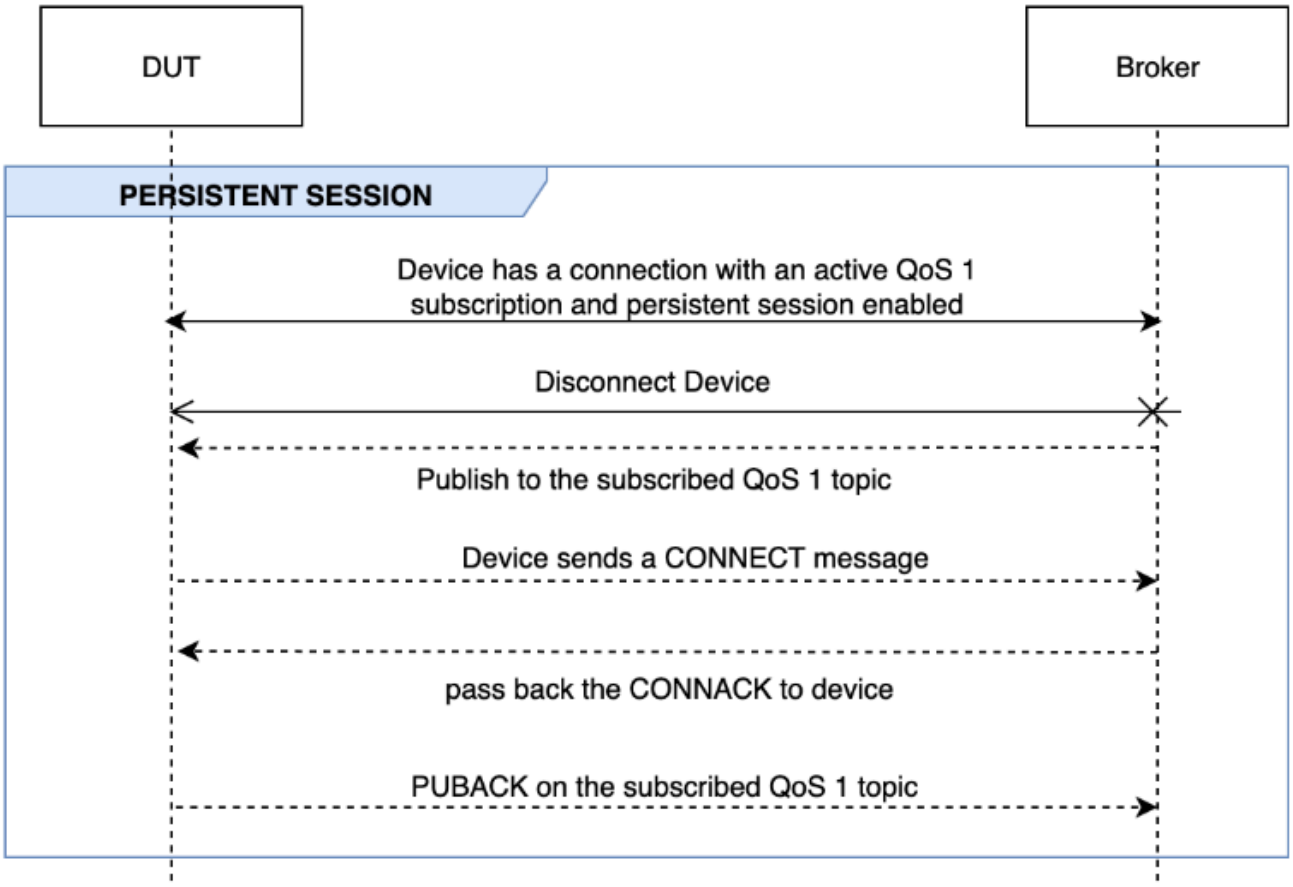

PERSISTENT SESSION

> **Note**
>
> Wählen Sie dieses Szenario nur aus, wenn Ihr Gerät QoS 1-Abonnements ausführen und eine persistente Sitzung aufrechterhalten kann.

In diesem Szenario wird das Geräteverhalten bei der Aufrechterhaltung persistenter Sitzungen validiert. Der Test validiert, wenn die folgenden Bedingungen erfüllt sind:

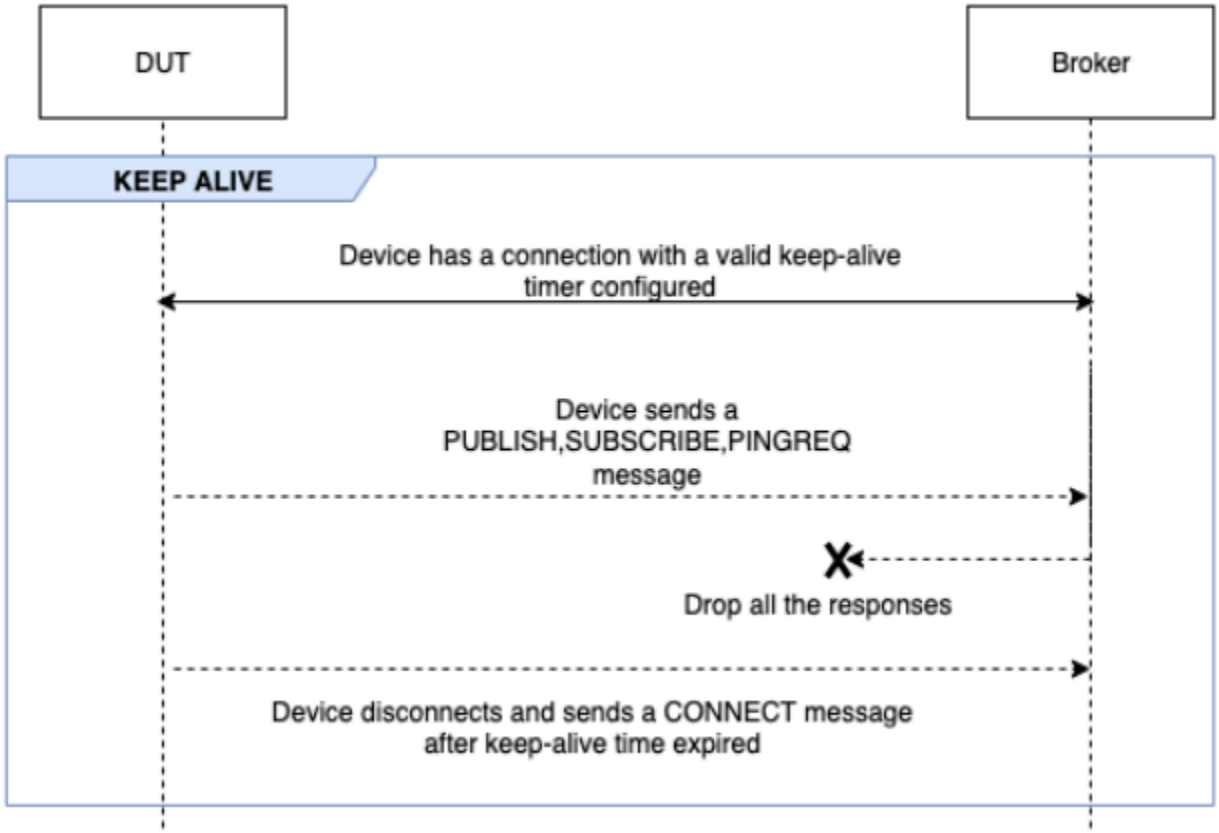
- Das Gerät stellt mit einem aktiven QoS 1-Abonnement und aktivierten persistenten Sitzungen eine Verbindung zum Broker her.
- Das Gerät trennt während der Sitzung erfolgreich die Verbindung zum Broker.
- Das Gerät stellt erneut eine Verbindung zum Broker her und nimmt die Abonnements für seine Trigger-Themen wieder auf, ohne diese Themen explizit erneut zu abonnieren.
- Das Gerät empfängt erfolgreich Nachrichten, die vom Broker für die abonnierten Themen gespeichert wurden, und läuft wie erwartet.

Weitere Informationen zu AWS IoT persistenten Sitzungen finden Sie unter Verwenden MQTT persistenter Sitzungen.



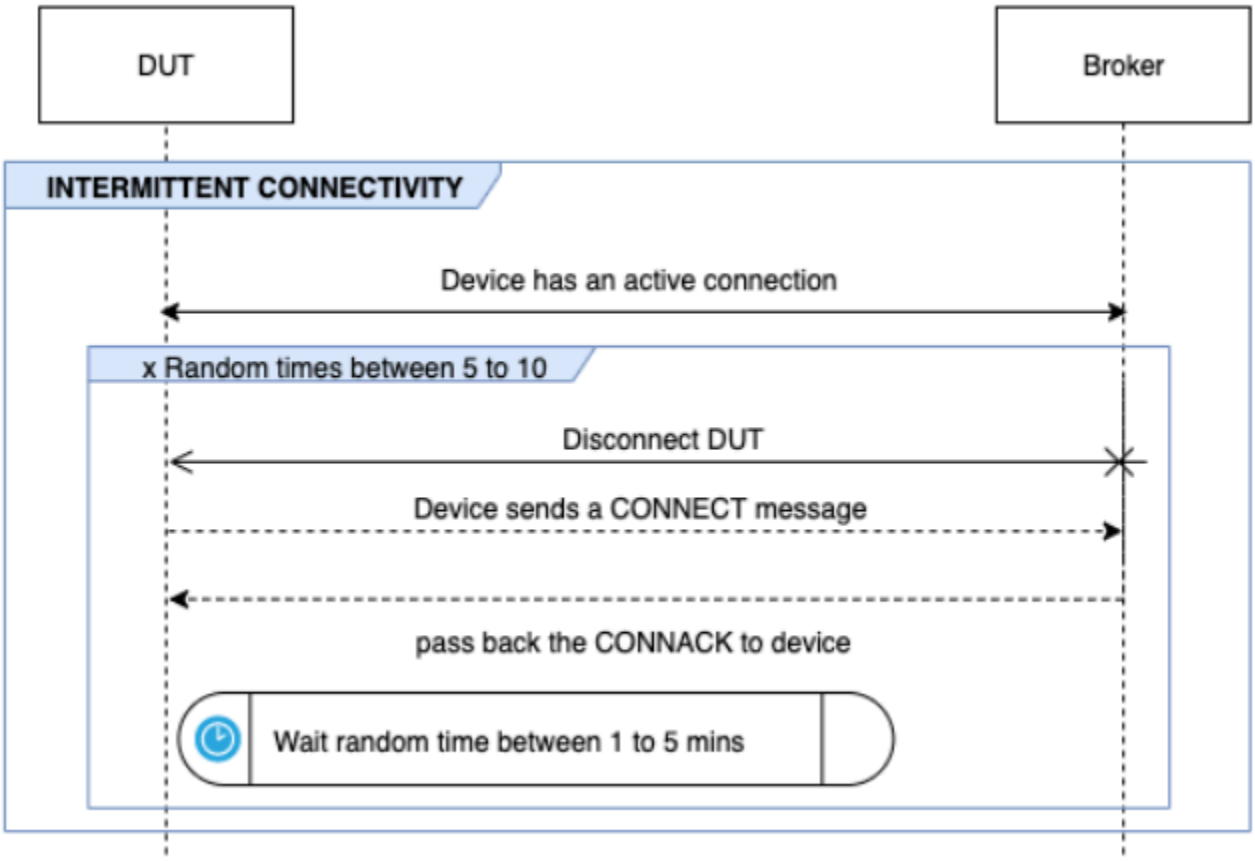

KEEP ALIVE

In diesem Szenario wird überprüft, ob das Gerät erfolgreich die Verbindung trennt, nachdem es keine Ping-Antwort vom Broker erhalten hat. Für die Verbindung muss ein gültiger Keep-Alive-Timer konfiguriert sein. Im Rahmen dieses Tests blockiert der Broker alle Antworten, die für `PUBLISH`-, `SUBSCRIBE`- und `PINGREQ`-Nachrichten gesendet wurden. Es überprüft auch, ob das getestete Gerät die MQTT Verbindung unterbricht.




INTERMITTENT CONNECTIVITY

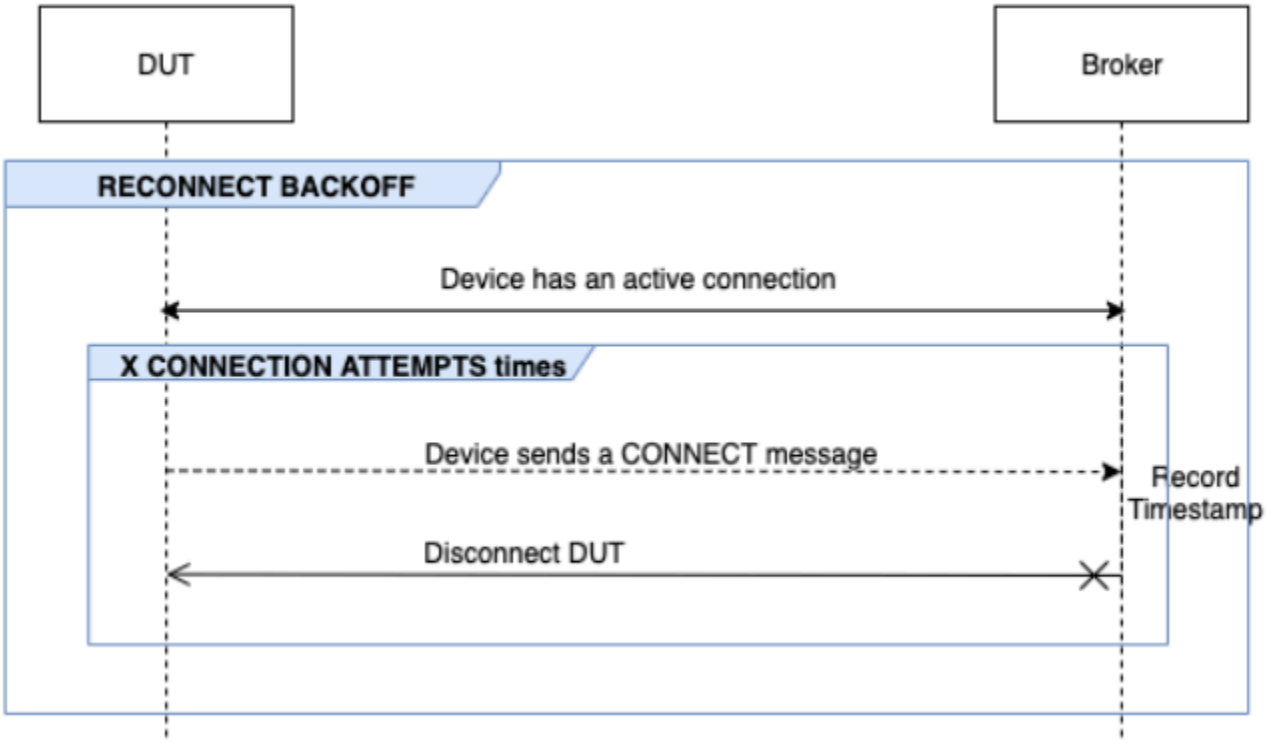
In diesem Szenario wird überprüft, ob das Gerät wieder eine Verbindung zum Broker herstellen kann, nachdem der Broker die Verbindung zum Gerät in zufälligen Intervallen für einen zufälligen Zeitraum getrennt hat.




RECONNECT BACKOFF

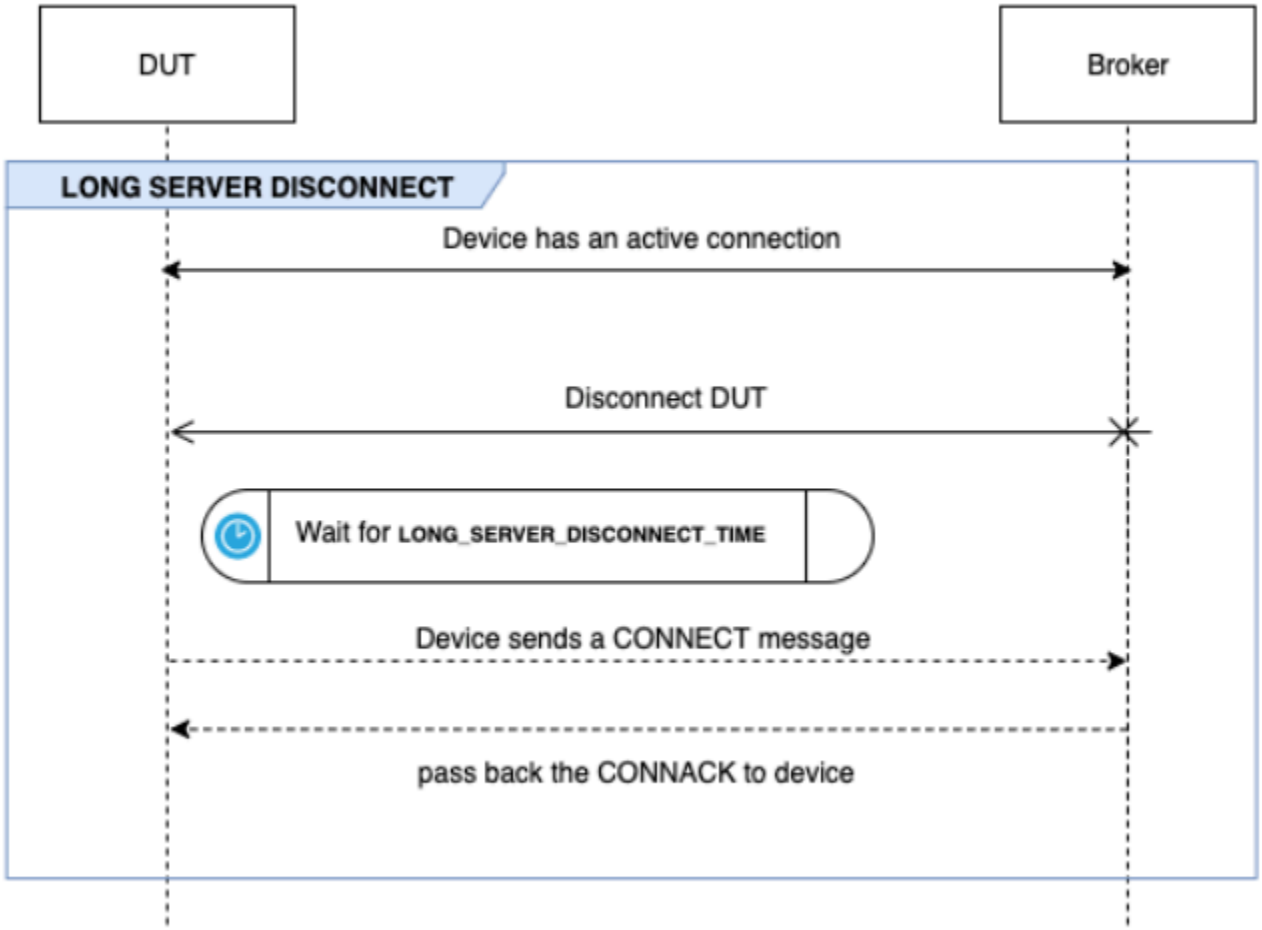
In diesem Szenario wird überprüft, ob auf dem Gerät ein Backoff-Mechanismus implementiert ist, wenn der Broker die Verbindung mehrmals trennt. Device Advisor meldet den Backoff-Typ als exponentiell, Jitter, linear oder konstant. Die Anzahl der Backoff-Versuche ist mit der `BACKOFF_CONNECTION_ATTEMPTS`-Option konfigurierbar. Der Standardwert ist 5. Der Wert ist zwischen 5 und 10 konfigurierbar.

Damit dieser Test bestanden wird, empfehlen wir, den Mechanismus Exponential Backoff And Jitter (Exponentielles Backoff und Jitter) auf dem getesteten Gerät zu implementieren.




LONG SERVER DISCONNECT

In diesem Szenario wird überprüft, ob das Gerät erfolgreich wieder eine Verbindung herstellen kann, nachdem der Broker die Verbindung zum Gerät über einen längeren Zeitraum (bis zu 120 Minuten) unterbrochen hat. Die Zeit für die Servertrennung kann mit der `LONG_SERVER_DISCONNECT_TIME`-Option konfiguriert werden. Der Standardwert beträgt 120 Minuten. Dieser Wert ist zwischen 30 und 120 Minuten konfigurierbar.




Zusätzliche Ausführungszeit

Die zusätzliche Ausführungszeit ist die Zeit, die der Test nach Abschluss aller oben genannten Tests und vor dem Beenden des Testfalls wartet. Kunden nutzen diesen zusätzlichen Zeitraum, um die gesamte Kommunikation zwischen dem Gerät und dem Broker zu überwachen und zu protokollieren. Die zusätzliche Ausführungszeit kann mit der `ADDITIONAL_EXECUTION_TIME`-Option konfiguriert werden. Standardmäßig ist diese Option auf 0 Minuten eingestellt und kann 0 bis 120 Minuten betragen.

## MQTTKonfigurationsoptionen für Langzeittests

Alle für den MQTT Langzeittest bereitgestellten Konfigurationsoptionen sind optional. Verfügbar sind die nachfolgend aufgeführten Optionen:

OPERATIONS

Die Liste der Operationen, die das Gerät ausführt, wie `CONNECT`, `PUBLISH` Uand `SUBSCRIBE`. Im Testfall werden Szenarien ausgeführt, die auf den angegebenen Operationen basieren. Operationen, die nicht angegeben sind, werden als gültig vorausgesetzt.

```
{
"OPERATIONS": ["PUBLISH", "SUBSCRIBE"]
//by default the test assumes device can CONNECT
}
```

SCENARIOS

Basierend auf den ausgewählten Operationen führt der Testfall Szenarien aus, um das Verhalten des Geräts zu überprüfen. Es gibt zwei Arten von Szenarien:

- Bei Basisszenarien handelt es sich um einfache Tests, mit denen überprüft wird, ob das Gerät die oben als Teil der Konfiguration ausgewählten Vorgänge ausführen kann. Diese werden auf der Grundlage der in der Konfiguration angegebenen Operationen vorab ausgewählt. Für die Konfiguration sind keine weiteren Eingaben erforderlich.
- Fortgeschrittene Szenarien sind komplexere Szenarien, die für das Gerät ausgeführt werden, um zu überprüfen, ob das Gerät unter realen Bedingungen bewährte Verfahren befolgt. Diese sind optional und können als eine Reihe von Szenarien an die Konfigurationseingabe der Testsuite übergeben werden.

```
{
    "SCENARIOS": [      // list of advanced scenarios
                "PUBACK_QOS_1",
                "RECEIVE_LARGE_PAYLOAD",
                "PERSISTENT_SESSION",
                "KEEP_ALIVE",
                "INTERMITTENT_CONNECTIVITY",
                "RECONNECT_BACK_OFF",
                "LONG_SERVER_DISCONNECT"
    ]
}
```

BASIC_TESTS_EXECUTION_TIME_OUT:

Die maximale Zeit, in der der Testfall auf den Abschluss aller Basistests wartet. Der Standardwert beträgt 60 Minuten. Dieser Wert ist zwischen 30 und 120 Minuten konfigurierbar.

LONG_SERVER_DISCONNECT_TIME:

Die Zeit, die der Testfall benötigt hat, um das Gerät während des Long-Server-Disconnect-Tests zu trennen und wieder zu verbinden. Der Standardwert beträgt 60 Minuten. Dieser Wert ist zwischen 30 und 120 Minuten konfigurierbar.

ADDITIONAL_EXECUTION_TIME:

Durch die Konfiguration dieser Option wird nach Abschluss aller Tests ein Zeitfenster zur Überwachung der Ereignisse zwischen dem Gerät und dem Broker bereitgestellt. Der Standardwert beträgt 0 Minuten. Dieser Wert ist zwischen 0 und 120 Minuten konfigurierbar.

BACKOFF_CONNECTION_ATTEMPTS:

Diese Option konfiguriert, wie oft das Gerät durch den Testfall getrennt wird. Dies wird vom Reconnect-Backoff-Test verwendet. Der Standardwert ist 5 Versuche. Dieser Wert ist von 5 bis 10 konfigurierbar.

LONG_PAYLOAD_FORMAT:

Das Format der Nachrichtennutzlast, die das Gerät erwartet, wenn der Testfall zu einem QoS 1-Thema veröffentlicht wird, das vom Gerät abonniert wurde.

APIDefinition des Testfalls:

```
{
"tests":[
   {
      "name":"my_mqtt_long_duration_test",
      "configuration": {
         // optional
         "OPERATIONS": ["PUBLISH", "SUBSCRIBE"],
         "SCENARIOS": [
            "LONG_SERVER_DISCONNECT",
            "RECONNECT_BACK_OFF",
            "KEEP_ALIVE",
            "RECEIVE_LARGE_PAYLOAD",
            "INTERMITTENT_CONNECTIVITY",
            "PERSISTENT_SESSION",
         ],
         "BASIC_TESTS_EXECUTION_TIMEOUT": 60, // in minutes (60 minutes by default)
         "LONG_SERVER_DISCONNECT_TIME": 60,   // in minutes (120 minutes by default)
         "ADDITIONAL_EXECUTION_TIME": 60,     // in minutes (0 minutes by default)
```

```
         "BACKOFF_CONNECTION_ATTEMPTS": "5",
         "LONG_PAYLOAD_FORMAT":"{"message":"${payload}"}"
      },
      "test":{
         "id":"MQTT_Long_Duration",
         "version":"0.0.0"
      }
   }
 ]
}
```

## MQTTÜbersichtsprotokoll für Testfälle mit langer Dauer

Der Testfall mit MQTT langer Dauer wird länger ausgeführt als normale Testfälle. Es wird ein separates Zusammenfassungsprotokoll bereitgestellt, das wichtige Ereignisse wie Geräteverbindungen, Veröffentlichungen und Abonnieren während der Ausführung auflistet. Zu den Details gehört, was getestet wurde, was nicht getestet wurde und was fehlgeschlagen ist. Am Ende des Protokolls enthält der Test eine Zusammenfassung aller Ereignisse, die während der Ausführung des Testfalls aufgetreten sind. Dies umfasst:

- Der Keep-Alive-Timer ist auf dem Gerät konfiguriert.
- Auf dem Gerät ist ein persistentes Sitzungs-Flag konfiguriert.
- Die Anzahl der Geräteverbindungen während des Testlaufs.
- Der Backoff-Typ für die Wiederverbindung des Geräts, sofern er für den Backoff-Test für die Wiederherstellung der Verbindung validiert wurde.
- Die Themen, zu denen das Gerät während der Testfallausführung veröffentlicht hat.
- Die Themen, die das Gerät während der Testfallausführung abonniert hat.

# AWS IoT Core Standort des Geräts

Bevor Sie die Funktion „ AWS IoT Core Gerätestandort“ verwenden, lesen Sie sich die Nutzungsbedingungen für diese Funktion durch. Beachten Sie, dass AWS möglicherweise die Parameter Ihrer Geolokalisierungs-Suchanfrage, wie z. B. die für die Durchführung von Suchanfragen verwendeten Standortdaten, und andere Informationen an den von Ihnen ausgewählten Drittanbieter übertragen werden, der möglicherweise nicht dem entspricht AWS-Region , den Sie derzeit verwenden. Der Drittanbieter und der zu verwendende Solver werden auf der Grundlage der empfangenen Eingabe-Payload ausgewählt. Weitere Informationen finden Sie unter AWS -Servicebedingungen.

Verwenden Sie AWS IoT Core Device Location, um den Standort Ihrer IoT-Geräte mithilfe von Solvern von Drittanbietern zu testen. Solver sind von Drittanbietern bereitgestellte Algorithmen, die Messungsdaten auflösen und den Standort Ihres Geräts schätzen. Indem Sie den Standort Ihrer Geräte ermitteln, können Sie sie vor Ort verfolgen und debuggen, um etwaige Probleme zu beheben.

Die aus verschiedenen Quellen gesammelten Messdaten werden aufgelöst, und die Geolokalisierungsinformationen werden als geografische Nutzdaten gemeldet. JSON Das JSON Geo-Format ist ein Format, das zur Kodierung geografischer Datenstrukturen verwendet wird. Die Payload enthält die Breiten- und Längengradkoordinaten Ihres Gerätestandorts, die auf dem Koordinatensystem des World Geodetic Systems () basieren. WGS84

Themen


- Messungstypen und Solver
- So funktioniert der AWS IoT Core Gerätestandort
- Wie benutzt man den Gerätestandort AWS IoT Core
- Auflösen des Standorts von IoT-Geräten
- Auflösen des Gerätestandorts mithilfe von Themen AWS IoT Core zum Gerätestandort MQTT
- Location Solver und Geräte-Payload


## Messungstypen und Solver

AWS IoT Core Device Location arbeitet mit Drittanbietern zusammen, um die Messdaten aufzulösen und einen geschätzten Gerätestandort zu ermitteln. In der folgenden Tabelle sind die Messungstypen

und die Location Solver von Drittanbietern sowie Informationen zu unterstützten Geräten aufgeführt. Informationen zu LoRa WAN Geräten und zur Konfiguration des Gerätestandorts für diese Geräte finden Sie unter Konfiguration der Position von LoRa WAN Ressourcen.

> **Note**
>
> Allgemeine IoT-Geräte und Sidewalk-Geräte können die MQTT Themen zum Gerätestandort verwenden, um die Standortinformationen abzurufen. Bei den Messarten WLAN, Mobilfunk und IP-Adresse kann der Gerätestandort den Standort des AWS IoT Core Geräts ermitteln, wenn die Geräte die Messdaten zu den reservierten Themen im definierten JSON Geoformat veröffentlichen. Für den GNSS Messtyp muss das Gerät über einen LR11xx Chip zum Scannen der Messdaten verfügen, um die aufgelösten Ortsinformationen mithilfe des GNSS Solvers zu erhalten. Informationen zum Abrufen von Standortinformationen für LoRa WAN Geräte finden Sie in der AWS IoT Wireless Dokumentation unter Konfiguration der Position für LoRa WAN Ressourcen.

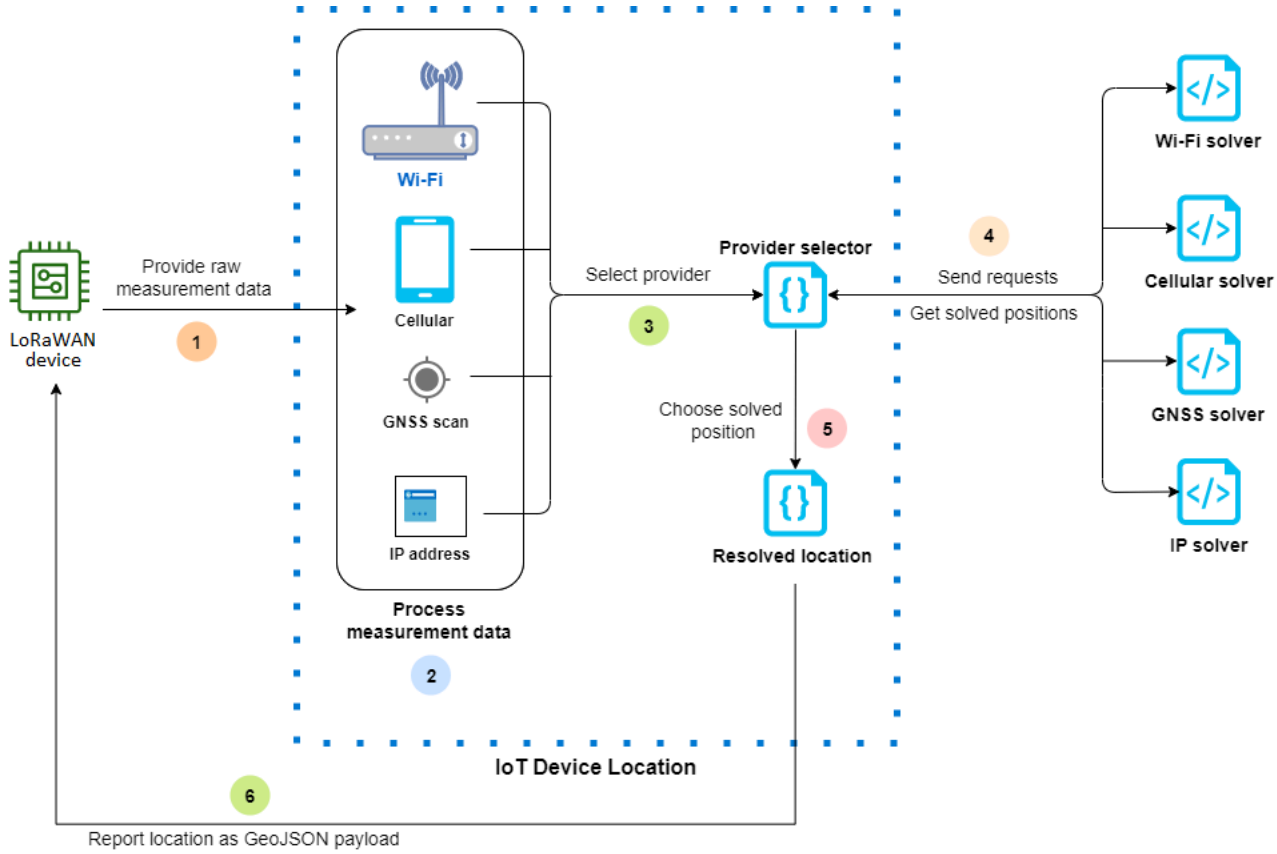
Messungstypen und Solver

| Messungstyp | Solver von Drittanbietern | Unterstützte Geräte |
|---|---|---|
| WLAN-Zugangspunkte | WLAN-basierter Solver | Allgemeine IoT-Geräte und Sidewalk-Geräte LoRa WAN |
| Mobilfunkmasten:GSM,LTE,CDMA, SCDMAWCMDA, und TD-Daten SCDMA | Solver auf Mobilfunkbasis | Allgemeine IoT-Geräte und Sidewalk-Geräte LoRa WAN |
| IP-Adresse | IP-Reverse-Lookup-Solver | Allgemeine IoT-Geräte und Sidewalk-Geräte |
| GNSSDaten (NAVNachrichten) scannen | GNSSSolver | Allgemeine IoT-Geräte und Gerätegeräte LoRa WAN |

Weitere Informationen zu den Location Solvern und Beispiele, welche die Gerätenutzlast für die verschiedenen Messungstypen zeigen, finden Sie unter Location Solver und Geräte-Payload.

# So funktioniert der AWS IoT Core Gerätestandort

Das folgende Diagramm zeigt, wie AWS IoT Core Device Location Messdaten sammelt und die Standortinformationen Ihrer Geräte auflöst.




Die folgenden Schritte zeigen, wie der AWS IoT Core Gerätestandort funktioniert.

1. Empfangen von Messungsdaten

   Die Rohmessungsdaten, die sich auf Ihren Gerätestandort beziehen, werden zuerst vom Gerät gesendet. Die Messdaten werden als JSON Nutzdaten angegeben.

2. Prozessmessungsdaten

   Die Messdaten werden verarbeitet, und der AWS IoT Core Gerätestandort wählt die zu verwendenden Messdaten aus. Dabei kann es sich um WLAN-, Mobilfunk-, GNSS Scan- oder IP-Adressinformationen handeln.

3. Auswählen des Solver

   Der Solver eines Drittanbieters wird auf der Grundlage der Messungsdaten ausgewählt. Wenn die Messungsdaten beispielsweise WLAN- und IP-Adressinformationen enthalten, werden der WLAN-Solver und der IP-Reverse-Lookup-Solver ausgewählt.

4. Abrufen des gelösten Standorts

   Es wird eine API Anfrage an die Solver-Anbieter gesendet, in der sie aufgefordert werden, den Standort zu ermitteln. AWS IoT Core Der Gerätestandort ruft dann die geschätzten Geolokalisierungsinformationen von den Solvern ab.

5. Auswählen des aufgelösten Standort

   Die aufgelösten Standortinformationen und ihre Genauigkeit werden verglichen, und der AWS IoT Core Gerätestandort wählt die Geolokalisierungsergebnisse mit der höchsten Genauigkeit aus.

6. Ausgabe der Standortinformationen

   Die Geolokalisierungsinformationen werden Ihnen als Geo-Payload gesendet. JSON Die Payload enthält die WGS84 Geokoordinaten, die Genauigkeitsinformationen, die Konfidenzstufen und den Zeitstempel, zu dem der ermittelte Standort abgerufen wurde.

# Wie benutzt man den Gerätestandort AWS IoT Core

Die folgenden Schritte zeigen, wie Sie den AWS IoT Core Gerätestandort verwenden.

1. Bereitstellen von Messungsdaten

   Geben Sie die Rohmessdaten, die sich auf den Standort Ihres Geräts beziehen, als JSON Nutzdaten an. Um die Nutzlast-Messdaten abzurufen, gehen Sie zu Ihren Geräteprotokollen oder verwenden Sie CloudWatch Protokolle und kopieren Sie die Nutzdateninformationen. Die JSON Payload muss eine oder mehrere Arten der Datenmessung enthalten. Beispiele, in denen das Nutzlastformat für verschiedene Solver gezeigt werden, finden Sie unter Location Solver und Geräte-Payload.

2. Auflösen von Standortinformationen

   Verwenden Sie die Seite Gerätestandort in der AWS IoT Konsole oder im GetPositionEstimateAPIVorgang, um die Payload-Messdaten zu übergeben und den Gerätestandort zu ermitteln. AWS IoT Core Der Gerätestandort wählt dann den Solver mit der

höchsten Genauigkeit aus und meldet den Gerätestandort. Weitere Informationen finden Sie unter Auflösen des Standorts von IoT-Geräten.

3. Kopieren von Standortinformationen

   Überprüfen Sie die Geolokalisierungsinformationen, die anhand AWS IoT Core des Gerätestandorts aufgelöst und als Geo-Payload gemeldet wurden. JSON Sie können die Payload kopieren, um sie mit Ihren Anwendungen und anderen zu verwenden. AWS-Service Beispielsweise können Sie Ihre geografischen Standortdaten mithilfe der Ort AWS IoT Regelaktion an Amazon Location Service senden.

In den folgenden Themen wird die Verwendung von AWS IoT Core Device Location und Beispiele für Payloads zum Gerätestandort beschrieben.

- Auflösen des Standorts von IoT-Geräten
- Location Solver und Geräte-Payload

# Auflösen des Standorts von IoT-Geräten

Verwenden Sie den AWS IoT Core Gerätestandort, um die Messdaten Ihrer Geräte zu dekodieren und den Gerätestandort mithilfe von Solvern von Drittanbietern zu ermitteln. Der aufgelöste Standort wird als JSON Geo-Payload mit den Geokoordinaten und Genauigkeitsinformationen generiert. Sie können den Standort Ihres Geräts über die AWS IoT Konsole AWS IoT Wireless API, das oder AWS CLI ermitteln.

Themen

- Auflösen des Gerätestandorts (Konsole)
- Gerätestandort wird aufgelöst () API
- Fehlerbehebung beim Auflösen des Standorts

## Auflösen des Gerätestandorts (Konsole)

So lösen Sie den Gerätestandort auf (Konsole)

1. Rufen Sie in der AWS IoT Konsole die Seite „Gerätestandort“ auf.
2. Rufen Sie die Nutzlast-Messdaten aus Ihren Geräteprotokollen oder aus den CloudWatch Protokollen ab und geben Sie sie im Abschnitt Position über Payload auflösen ein.

Der folgende Code zeigt ein Beispiel JSON für eine Payload. Die Nutzlast enthält Mobilfunk- und WLAN-Messungsdaten. Wenn Ihre Nutzlast zusätzliche Arten von Messungsdaten enthält, wird der Solver mit der besten Genauigkeit verwendet. Weitere Informationen und Beispiele zur Nutzlast finden Sie unter the section called “Location Solver und Geräte-Payload”.

> **Note**
>
> Die JSON Nutzlast muss mindestens einen Typ von Messdaten enthalten.

```
{
    "Timestamp": 1664313161,
    "Ip":{
        "IpAddress": "54.240.198.35"
    },
    "WiFiAccessPoints": [{
        "MacAddress": "A0:EC:F9:1E:32:C1",
        "Rss": -77
    }],
    "CellTowers": {
        "Gsm": [{
            "Mcc": 262,
            "Mnc": 1,
            "Lac": 5126,
            "GeranCid": 16504,
            "GsmLocalId": {
                "Bsic": 6,
                "Bcch": 82
            },
            "GsmTimingAdvance": 1,
            "RxLevel": -110,
            "GsmNmr": [{
                "Bsic": 7,
                "Bcch": 85,
                "RxLevel": -100,
                "GlobalIdentity": {
                    "Lac": 1,
                    "GeranCid": 1
                }
            }]
        }],
```

```
        "Wcdma": [{
            "Mcc": 262,
            "Mnc": 7,
            "Lac": 65535,
            "UtranCid": 14674663,
            "WcdmaNmr": [{
                    "Uarfcndl": 10786,
                    "UtranCid": 14674663,
                    "Psc": 149
                },
                {
                    "Uarfcndl": 10762,
                    "UtranCid": 14674663,
                    "Psc": 211
                }
            ]
        }],
        "Lte": [{
            "Mcc": 262,
            "Mnc": 2,
            "EutranCid": 2898945,
            "Rsrp": -50,
            "Rsrq": -5,
            "LteNmr": [{
                    "Earfcn": 6300,
                    "Pci": 237,
                    "Rsrp": -60,
                    "Rsrq": -6,
                    "EutranCid": 2898945
                },
                {
                    "Earfcn": 6300,
                    "Pci": 442,
                    "Rsrp": -70,
                    "Rsrq": -7,
                    "EutranCid": 2898945
                }
            ]
        }]
    }
}
```

3. Um die Standortinformationen aufzulösen, wählen Sie Auflösen aus.

Die Standortinformationen sind vom Typ Blob und werden als Payload zurückgegeben, die das JSON Geo-Format verwendet, ein Format, das für die Kodierung geografischer Datenstrukturen verwendet wird. Die Nutzlast enthält Folgendes:

- Die WGS84 Geokoordinaten, die die Breiten- und Längengradinformationen enthalten. Sie kann auch eine Höheninformation enthalten.
- Den Typ der gemeldeten Standortinformationen, z. B. Punkt. Ein Punktpositionstyp stellt die Position als WGS84 Breitengrad und Längengrad dar, kodiert als JSONGeopunkt.
- Die horizontalen und vertikalen Genauigkeitsinformationen, die den Unterschied in Metern zwischen den von den Solvern geschätzten Standortinformationen und dem tatsächlichen Gerätestandort angeben.
- Den Zuverlässigkeitsgrad, der die Unsicherheit in der bereitgestellten Standortschätzung angibt. Der Standardwert ist 0,68, was auf eine Wahrscheinlichkeit von 68 % hinweist, dass der tatsächliche Gerätestandort innerhalb des Unsicherheitsradius des geschätzten Standorts liegt.
- Die Stadt, das Bundesland, das Land und die Postleitzahl, in der sich das Gerät befindet. Diese Informationen werden nur gemeldet, wenn der IP-Reverse-Lookup-Solver verwendet wird.
- Die Informationen zum Zeitstempel, die dem Datum und der Uhrzeit entspricht, an denen der Standort aufgelöst wurde. Es wird das UNIX-Zeitstempelformat verwendet.

Der folgende Code zeigt ein Beispiel für eine JSON Geo-Payload, die bei der Auflösung des Standorts zurückgegeben wurde.

> **Note**
>
> Wenn AWS IoT Core Device Location beim Versuch, den Standort zu ermitteln, Fehler meldet, können Sie die Fehler und den Standort beheben. Weitere Informationen finden Sie unter Fehlerbehebung beim Auflösen des Standorts.

```
{
    "coordinates": [
        13.376076698303223,
        52.51823043823242
    ],
```

```
    "type": "Point",
    "properties": {
        "verticalAccuracy": 45,
        "verticalConfidenceLevel": 0.68,
        "horizontalAccuracy": 303,
        "horizontalConfidenceLevel": 0.68,
        "country": "USA",
        "state": "CA",
        "city": "Sunnyvalue",
        "postalCode": "91234",
        "timestamp": "2022-11-18T12:23:58.189Z"
    }
}
```

4. Gehen Sie zum Abschnitt Ressourcenstandort und überprüfen Sie die vom AWS IoT Core Gerätestandort gemeldeten Geolokalisierungsinformationen. Sie können die Payload kopieren, um sie mit anderen Anwendungen und Apps zu verwenden. AWS-Service Beispielsweise können Sie Ihre geografischen Standortdaten mithilfe der Ort-Regelaktion an Amazon Location Service senden.

## Gerätestandort wird aufgelöst () API

Um den Gerätestandort mithilfe von zu ermitteln AWS IoT Wireless API, verwenden Sie den GetPositionEstimateAPIVorgang oder den get-position-estimateCLIBefehl. Geben Sie die Nutzlast-Messdaten als Eingabe an und führen Sie den API Vorgang aus, um den Gerätestandort zu ermitteln.

> **Note**
>
> Der `GetPositionEstimate` API Vorgang speichert keine Geräte- oder Statusinformationen und kann nicht zum Abrufen historischer Standortdaten verwendet werden. Er führt eine einmalige Operation durch, bei der die Messungsdaten aufgelöst und der geschätzte Standort erstellt werden. Um die Standortinformationen abzurufen, müssen Sie die Nutzlastinformationen jedes Mal angeben, wenn Sie diesen API Vorgang ausführen.

Der folgende Befehl zeigt ein Beispiel dafür, wie der Standort mithilfe dieses API Vorgangs aufgelöst werden kann.

> **Note**
>
> Wenn Sie den `get-position-estimate` CLI Befehl ausführen, müssen Sie die JSON Ausgabedatei als erste Eingabe angeben. In dieser JSON Datei werden die geschätzten Standortinformationen gespeichert, die als Antwort vom CLI im JSON Geo-Format abgerufen wurden. Der folgende Befehl speichert die Standortinformationen beispielsweise im *`locationout.json`* file.

```
aws iotwireless get-position-estimate locationout.json \
    --ip IpAddress=""54.240.198.35"" \
    --wi-fi-access-points \
        MacAddress="A0:EC:F9:1E:32:C1",Rss=-75 \
        MacAddress="A0:EC:F9:15:72:5E",Rss=-67
```

Dieses Beispiel umfasst sowohl Wi-Fi-Zugangspunkte als auch IP-Adressen als Messtypen. AWS IoT Core Der Gerätestandort wählt zwischen dem Wi-Fi-Solver und dem IP-Reverse-Lookup-Solver und wählt den Solver mit der höheren Genauigkeit aus.

Der aufgelöste Standort wird als Payload zurückgegeben, der das JSON Geo-Format verwendet, ein Format, das für die Kodierung geografischer Datenstrukturen verwendet wird. Es wird dann gespeichert im *`locationout.json`* file. Die Nutzdaten enthalten die WGS84 Breiten- und Längengradkoordinaten, Informationen zur Genauigkeit und zum Konfidenzniveau, den Standortdatentyp und den Zeitstempel, zu dem der Standort ermittelt wurde.

```
{
    "coordinates": [
        13.37704086303711,
        52.51865005493164
    ],
    "type": "Point",
    "properties": {
        "verticalAccuracy": 707,
        "verticalConfidenceLevel": 0.68,
        "horizontalAccuracy": 389,
        "horizontalConfidenceLevel": 0.68,
        "country": "USA",
        "state": "CA",
        "city": "Sunnyvalue",
        "postalCode": "91234",
```

```
        "timestamp": "2022-11-18T14:03:57.391Z"
    }
}
```

## Fehlerbehebung beim Auflösen des Standorts

Wenn Sie versuchen, den Standort zu ermitteln, wird möglicherweise einer der folgenden Fehlercodes angezeigt. AWS IoT Core Der Gerätestandort kann bei der Verwendung des `GetPositionEstimate` API Vorgangs zu einem Fehler führen, oder es wird auf die Zeilennummer verwiesen, die dem Fehler in der AWS IoT Konsole entspricht.

- 400-Fehler

  Dieser Fehler weist darauf hin, dass das Format der Geräte-Payload nicht anhand des AWS IoT Core Gerätestandorts überprüft werden JSON kann. Der Fehler kann aus folgenden Gründen auftreten:

  - Die JSON Messdaten sind falsch formatiert.
  - Die Nutzlast enthält nur die Informationen zum Zeitstempel.
  - Die Messungsdatenparameter, wie z. B. die IP-Adresse, sind ungültig.

  Um diesen Fehler zu beheben, überprüfen Sie, ob Ihre JSON Datei korrekt formatiert ist und Daten von einem oder mehreren Messarten als Eingabe enthält. Wenn die IP-Adresse ungültig ist, finden Sie Informationen darüber, wie Sie eine gültige IP-Adresse zur Behebung des Fehlers angeben können, unter IP-Reverse-Lookup-Solver.
- 403-Fehler

  Dieser Fehler weist darauf hin, dass Sie nicht berechtigt sind, den API Vorgang auszuführen oder die AWS IoT Konsole zum Abrufen des Gerätestandorts zu verwenden. Um diesen Fehler zu beheben, stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen, um diese Aktion auszuführen. Dieser Fehler kann auftreten, wenn Ihre AWS Management Console Sitzung oder Ihr AWS CLI Sitzungstoken abgelaufen sind. Um diesen Fehler zu beheben, aktualisieren Sie das Sitzungstoken, um das zu verwenden AWS CLI, oder melden Sie sich ab AWS Management Console und melden Sie sich dann mit Ihren Anmeldeinformationen an.
- 404-Fehler

  Dieser Fehler weist darauf hin, dass keine Standortinformationen gefunden oder anhand AWS IoT Core des Gerätestandorts behoben wurden. Der Fehler kann beispielsweise aufgrund unzureichender Daten in der Eingabe von Messungsdaten auftreten. Beispielsweise:

- Die MAC Adress- oder Mobilfunkmastinformationen sind nicht ausreichend.
- Die IP-Adresse ist nicht verfügbar, um den Standort zu suchen und abzurufen.
- Die GNSS Nutzlast ist nicht ausreichend.

  Um den Fehler in solchen Fällen zu beheben, überprüfen Sie, ob Ihre Messungsdaten ausreichende Informationen enthalten, um den Gerätestandort zu ermitteln.
- 500-Fehler

  Dieser Fehler weist darauf hin, dass eine interne Serverausnahme aufgetreten ist, als AWS IoT Core  Device Location versucht hat, den Standort aufzulösen. Um diesen Fehler zu beheben, aktualisieren Sie die Sitzung und versuchen Sie erneut, die zu lösenden Messungsdaten zu senden.

# Auflösen des Gerätestandorts mithilfe von Themen AWS IoT Core zum Gerätestandort MQTT

Mithilfe der Funktion „ AWS IoT Core Gerätestandort“ können Sie reservierte MQTT Themen verwenden, um die neuesten Standortinformationen für Ihre Geräte abzurufen.

## Format der MQTT Themen zum Gerätestandort

Für Themen, die für den AWS IoT Core Gerätestandort reserviert sind, wird das folgende Präfix verwendet:

`$aws/device_location/{customer_device_id}/`

Um ein vollständiges Thema zu erstellen, ersetzen Sie zunächst *`customer_device_id`* durch Ihre eindeutige ID, mit der Sie Ihr Gerät identifizieren. Wir empfehlen, dass Sie das angeben`WirelessDeviceId`, z. B. für LoRa WAN und für Sidewalk-Geräte, und*`thingName`*, ob Ihr Gerät als Objekt registriert ist AWS IoT . Anschließend fügen Sie das Thema mit dem Themenbereich hinzu, z. B. `get_position_estimate` oder `get_position_estimate/accepted`, wie im folgenden Abschnitt gezeigt.

> **Note**
>
> *`{customer_device_id}`* darf nur Buchstaben, Zahlen und Bindestriche enthalten. Wenn Sie Themen zum Gerätestandort abonnieren, können Sie nur das Pluszeichen

(+) als Platzhalterzeichen verwenden. Sie können beispielsweise den Platzhalter + für *{customer_device_id}* verwenden, um die Standortinformationen für Ihre Geräte abzurufen. Wenn Sie das Thema `$aws/device_location/+/get_position_estimate/accepted` abonnieren, wird eine Nachricht mit den Standortinformationen für Geräte veröffentlicht, die mit einer beliebigen Geräte-ID übereinstimmen, sofern das Problem erfolgreich gelöst wurde.

Im Folgenden finden Sie die reservierten Themen, die für die Interaktion mit AWS IoT Core Device Location verwendet werden.

MQTTThemen zum Gerätestandort

| Thema | Zulässige Operationen | Beschreibung |
|---|---|---|
| $aws/device_location/*customer_device_id* /get_position_estimate | Veröffentlichen | Ein Gerät veröffentlicht zu diesem Thema, um die gescannten Rohmessdaten nach Gerätestandort aufzulösen. AWS IoT Core |
| $aws/device_location/*customer_device_id* /get_position_estimate/accepted | Abonnieren | AWS IoT Core Der Gerätestandort veröffentlicht die Standortinformationen zu diesem Thema, wenn der Gerätestandort erfolgreich ermittelt wurde. |
| $aws/device_location/*customer_device_id* /get_position_estimate/rejected | Abonnieren | AWS IoT Core Device Location veröffentlicht die Fehlerinformationen zu diesem Thema, wenn der Gerätestandort nicht behoben werden kann. |

## Richtlinien für MQTT Themen zum Gerätestandort

Um Nachrichten zu Themen zum Gerätestandort zu erhalten, muss Ihr Gerät eine Richtlinie verwenden, die es ermöglicht, eine Verbindung zum AWS IoT Gerätegateway herzustellen und die MQTT Themen zu abonnieren.

Im Folgenden finden Sie ein Beispiel für die Richtlinie, die für den Empfang von Nachrichten zu verschiedenen Themen erforderlich ist.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/device_location/customer_device_id/
get_position_estimate"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/device_location/customer_device_id/
get_position_estimate/accepted",
        "arn:aws:iot:region:account:topic/$aws/device_location/customer_device_id/
get_position_estimate/rejected"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topicfilter/$aws/
device_location/customer_device_id/get_position_estimate/accepted",
        "arn:aws:iot:region:account:topicfilter/$aws/
device_location/customer_device_id/get_position_estimate/rejected"
      ]
    }
  ]
}
```

# Themen zum Gerätestandort und Nutzlast

Im Folgenden werden die Themen AWS IoT Core zum Gerätestandort, das Format ihrer Nutzdaten für Nachrichten und eine Beispielrichtlinie für jedes Thema beschrieben.

Themen

- /get_position_estimate
- /get_position_estimate/accepted
- /get_position_estimate/rejected

## /get_position_estimate

Veröffentlichen Sie eine Nachricht zu diesem Thema, um die Rohmessdaten des Geräts abzurufen und nach AWS IoT Core Gerätestandort aufzulösen.

```
$aws/device_location/customer_device_id/get_position_estimate
```

AWS IoT Core Device Location antwortet mit der Veröffentlichung entweder auf /get_position_estimate/accepted oder/get_position_estimate/rejected.

> **Note**
>
> Bei der zu diesem Thema veröffentlichten Nachricht muss es sich um eine gültige JSON Payload handeln. Wenn die Eingabenachricht kein gültiges JSON Format hat, erhalten Sie keine Antwort. Weitere Informationen finden Sie unter Nachrichtennutzlast.

Nachrichten-Payload

Das Format der Nachrichtennutzdaten folgt einer ähnlichen Struktur wie der Hauptteil der AWS IoT Wireless API Vorgangsanforderung. `GetPositionEstimate` Sie enthält Folgendes:

- Eine optionale `Timestamp`-Zeichenfolge, die dem Datum und der Uhrzeit entspricht, an denen der Standort aufgelöst wurde. Die `Timestamp`-Zeichenfolge kann eine Mindestlänge von 1 und eine Maximallänge von 10 haben.
- Eine optionale `MessageId`-Zeichenfolge, die verwendet werden kann, um die Anforderung der Antwort zuzuordnen. Wenn Sie diese Zeichenfolge angeben, enthält die Nachricht, die in den Themen `get_position_estimate/accepted` oder `get_position_estimate/rejected`

veröffentlicht wird, diese `MessageId`. Die `MessageID`-Zeichenfolge kann eine Mindestlänge von 1 und eine Maximallänge von 256 haben.

- Die Messungsdaten des Geräts, das mindestens einen der folgenden Messungstypen enthält:
  - `WiFiAccessPoint`
  - `CellTowers`
  - `IpAddress`
  - `Gnss`

Im Folgenden finden Sie ein Beispiel für eine Nachrichtennutzlast.

```
{
    "Timestamp": "1664313161",
    "MessageId": "ABCD1",
    "WiFiAccessPoints":  [
        {
            "MacAddress": "A0:EC:F9:1E:32:C1",
            "Rss": -66
        }
    ],
    "Ip":{
        "IpAddress": "54.192.168.0"
    },
    "Gnss":{
      "Payload":"8295A614A2029517F4F77C0A7823B161A6FC57E25183D96535E3689783F6CA48",
      "CaptureTime":1354393948
    }
}
```

Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

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

```
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/device_location/customer_device_id/
get_position_estimate"
      ]
    }
  ]
}
```

### /get_position_estimate/accepted

AWS IoT Core Device Location veröffentlicht eine Antwort zu diesem Thema, wenn die aufgelösten Standortinformationen für Ihr Gerät zurückgesendet werden. Die Standortinformationen werden im JSONGeoformat zurückgegeben.

```
$aws/device_location/customer_device_id/get_position_estimate/accepted
```

Im Folgenden werden die Nachrichtennutzlast und ein Beispiel für eine Richtlinie dargestellt.

#### Nachrichten-Payload

Im Folgenden finden Sie ein Beispiel für die Nachrichtennutzlast im JSON Geo-Format. Wenn Sie `MessageId` in Ihren Rohmessdaten a angegeben haben und der AWS IoT Core Gerätestandort die Standortinformationen erfolgreich aufgelöst hat, gibt die Nachrichtennutzlast dieselben `MessageId` Informationen zurück.

```
{
    "coordinates": [
        13.37704086303711,
        52.51865005493164
    ],
    "type": "Point",
    "properties": {
        "verticalAccuracy": 707,
        "verticalConfidenceLevel": 0.68,
        "horizontalAccuracy": 389,
        "horizontalConfidenceLevel": 0.68,
        "country": "USA",
        "state": "CA",
        "city": "Sunnyvalue",
        "postalCode": "91234",
        "timestamp": "2022-11-18T14:03:57.391Z",
        "messageId": "ABCD1"
```

```
    }
}
```

Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topicfilter/$aws/
device_location/customer_device_id/get_position_estimate/accepted"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/device_location/customer_device_id/
get_position_estimate/accepted"
      ]
    }
  ]
}
```

## /get_position_estimate/rejected

AWS IoT Core Device Location veröffentlicht eine Fehlermeldung zu diesem Thema, wenn der Gerätestandort nicht aufgelöst werden kann.

```
$aws/device_location/customer_device_id/get_position_estimate/rejected
```

Im Folgenden sehen Sie die Nachrichtennutzlast und ein Beispiel für die Richtlinie. Weitere Informationen zu den Fehlern finden Sie unter Fehlerbehebung beim Auflösen des Standorts.

### Nachrichtennutzlast

Im Folgenden finden Sie ein Beispiel für die Nachrichten-Payload, die den Fehlercode und die Meldung enthält, aus der hervorgeht, warum AWS IoT Core Device Location die Standortinformationen nicht auflösen konnte. Wenn Sie `MessageId` bei der Bereitstellung Ihrer Rohmessdaten ein angegeben haben und der AWS IoT Core Gerätestandort die Standortinformationen nicht auflösen konnte, werden dieselben `MessageId` Informationen in der Nachrichtennutzlast zurückgegeben.

```
{
    "errorCode": 500,
    "errorMessage":"Internal server error",
    "messageId": "ABCD1"
}
```

### Beispielrichtline

Im Folgenden finden Sie ein Beispiel für die erforderliche Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Subscribe"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topicfilter/$aws/
device_location/customer_device_id/get_position_estimate/rejected"
      ]
    },
    {
      "Action": [
        "iot:Receive"
      ],
      "Resource": [
        "arn:aws:iot:region:account:topic/$aws/device_location/customer_device_id/
get_position_estimate/rejected"
      ]
    }
  ]
```

```
}
```

# Location Solver und Geräte-Payload

Location Solver sind Algorithmen, mit denen der Standort Ihrer IoT-Geräte ermittelt werden kann. AWS IoT Core Device Location unterstützt die folgenden Location Solver. Sie sehen Beispiele für das JSON Payload-Format für diese Messtypen, die vom Solver unterstützten Geräte und die Art und Weise, wie der Standort ermittelt wird.

Um den Gerätestandort zu ermitteln, geben Sie mindestens einen dieser Messungsdatentypen an. Für alle Messungsdaten zusammen wird ein einziger, aufgelöster Standort zurückgegeben.

Themen


- WLAN-basierter Solver
- Solver auf Mobilfunkbasis
- IP-Reverse-Lookup-Solver
- GNSSSolver


## WLAN-basierter Solver

Verwenden Sie den WLAN-basierten Solver, um den Standort anhand der Scaninformationen von WLAN-Zugangspunkten zu ermitteln. Der Solver unterstützt die WLAN Technologie und kann zur Berechnung des Gerätestandorts für allgemeine IoT-Geräte und LoRa WAN drahtlose Geräte verwendet werden.

Die LoRa WAN Geräte müssen über den LoRa Edge-Chipsatz verfügen, der die eingehenden Wi-Fi-Scaninformationen dekodieren kann. LoRa Edge ist eine Plattform mit extrem geringem Stromverbrauch, die einen LoRa Transceiver mit großer Reichweite, einen Scanner mit mehreren Konstellationen und einen passiven GNSS Wi-Fi-Scanner für Geolokalisierungsanwendungen integriert. MAC Wenn eine Uplink-Nachricht vom Gerät empfangen wird, werden die Wi-Fi-Scandaten an den Gerätestandort gesendet, und der Standort wird auf AWS IoT Core der Grundlage der Wi-Fi-Scanergebnisse geschätzt. Die dekodierten Informationen werden dann an den WLAN-basierten Solver weitergeleitet, um die Standortinformationen abzurufen.

Beispiel für die Nutzlast eines WLAN-basierten Solvers

Der folgende Code zeigt ein Beispiel für die JSON Nutzdaten des Geräts, die die Messdaten enthalten. Wenn AWS IoT Core Device Location diese Daten als Eingabe empfängt, sendet es

eine HTTP Anfrage an den Solver-Anbieter, um die Standortinformationen aufzulösen. Um die Informationen abzurufen, geben Sie Werte für die MAC Adresse und RSS (empfangene Signalstärke) an. Geben Sie dazu entweder die JSON Nutzdaten in diesem Format an oder verwenden Sie den WiFiAccessPointsObjektparameter der GetPositionEstimateAPIOperation.

```
{
    "Timestamp": 1664313161,    // optional
    "WiFiAccessPoints": [
        {
            "MacAddress": "A0:EC:F9:1E:32:C1",  // required
            "Rss": -75                          // required
        }
    ]
}
```

## Solver auf Mobilfunkbasis

Sie können den Solver auf Mobilfunkbasis verwenden, um den Standort anhand von Messungsdaten von Mobilfunkmasten aufzulösen. Der Solver unterstützt die folgenden Technologien. Es wird eine einzige aufgelöste Standortinformation abgerufen, auch wenn Sie Messungsdaten aus einer oder allen dieser Technologien einbeziehen.

- GSM
- CDMA
- WCDMA
- TD- SCDMA
- LTE

### Beispiele für Solver-Nutzlasten auf Mobilfunkbasis

Der folgende Code zeigt Beispiele für die JSON Nutzlast des Geräts, das Mobilfunkmessdaten enthält. Wenn AWS IoT Core Device Location diese Daten als Eingabe empfängt, sendet es eine HTTP Anfrage an den Solver-Anbieter, um die Standortinformationen aufzulösen. Um die Informationen abzurufen, geben Sie entweder die JSON Payload in diesem Format in der Konsole an oder geben Werte für den CellTowersParameter des GetPositionEstimateAPIVorgangs an. Sie können die Messungsdaten bereitstellen, indem Sie Werte für Parameter angeben, die eine oder alle dieser Mobilfunktechnologien verwenden.

LTE(Langfristige Entwicklung)

Wenn Sie diese Messungsdaten verwenden, müssen Sie Informationen wie das Netzwerk und die Landesvorwahl des Mobilfunknetzes sowie optionale zusätzliche Parameter, einschließlich Informationen zur lokalen ID, angeben. Der nachfolgende Code zeigt ein Beispiel für das Nutzlastformat. Weitere Informationen zu diesen Parametern finden Sie unter LTEObjekt.

```
{
    "Timestamp": 1664313161,           // optional
    "CellTowers": {
        "Lte": [
        {
          "Mcc": int,                   // required
          "Mnc": int,                   // required
          "EutranCid": int,             // required. Make sure that you use int for
 EutranCid.
          "Tac": int,                   // optional
          "LteLocalId": {               // optional
              "Pci": int,               // required
              "Earfcn": int,            // required
          },
          "LteTimingAdvance": int,      // optional
          "Rsrp": int,                  // optional
          "Rsrq": float,                // optional
          "NrCapable": boolean,         // optional
          "LteNmr": [                   // optional
                {
                    "Pci": int,         // required
                    "Earfcn": int,      // required
                    "EutranCid": int,   // required
                    "Rsrp": int,        // optional
                    "Rsrq": float       // optional
                }
            ]
         }
      ]
   }
}
```

GSM(Globales System für Mobilkommunikation)

Wenn Sie diese Messungsdaten verwenden, müssen Sie Informationen wie das Netzwerk und die Landesvorwahl des Mobilfunknetzes, Informationen zur Basisstation und optionale weitere Parameter

angeben. Der nachfolgende Code zeigt ein Beispiel für das Nutzlastformat. Weitere Informationen zu diesen Parametern finden Sie unter GSMObjekt.

```
{
    "Timestamp": 1664313161,           // optional
    "CellTowers": {
        "Gsm": [
        {
          "Mcc": int,                   // required
          "Mnc": int,                   // required
          "Lac": int,                   // required
          "GeranCid": int,              // required
          "GsmLocalId": {               // optional
              "Bsic": int,              // required
              "Bcch": int,              // required
          },
          "GsmTimingAdvance": int,      // optional
          "RxLevel": int,               // optional
          "GsmNmr": [                   // optional
            {
                "Bsic": int,            // required
                "Bcch": int,            // required
                "RxLevel": int,         // optional
                "GlobalIdentity": {
                    "Lac": int,         // required
                    "GeranCid": int     // required
                }
             }
          ]
       }
    ]
}
```

CDMA(Mehrfachzugriff nach Code-Division)

Wenn Sie diese Messungsdaten verwenden, müssen Sie Informationen wie die Signalleistung und Identifikationsinformationen, Informationen zur Basisstation und optionale weitere Parameter angeben. Der nachfolgende Code zeigt ein Beispiel für das Nutzlastformat. Weitere Informationen zu diesen Parametern finden Sie unter CDMA Objekt.

```
{
    "Timestamp": 1664313161,              // optional
```

```
    "CellTowers": {
        "Cdma": [
        {
            "SystemId": int,                // required
            "NetworkId": int,               // required
            "BaseStationId": int,           // required
            "RegistrationZone": int,        // optional
            "CdmaLocalId": {                // optional
              "PnOffset": int,              // required
              "CdmaChannel": int,           // required
            },
            "PilotPower": int,              // optional
            "BaseLat": float,               // optional
            "BaseLng": float,               // optional
            "CdmaNmr": [                    // optional
                {
                    "PnOffset": int,        // required
                    "CdmaChannel": int,     // required
                    "PilotPower": int,      // optional
                    "BaseStationId": int    // optional
                }
             ]
          }
       ]
    }
}
```

WCDMA(Breitband-Mehrfachzugriff mit Codedivision)

Wenn Sie diese Messungsdaten verwenden, müssen Sie Informationen wie das Netzwerk und die Landesvorwahl, die Signalleistung und Identifikationsinformationen, Informationen zur Basisstation und optionale weitere Parameter angeben. Der nachfolgende Code zeigt ein Beispiel für das Nutzlastformat. Weitere Informationen zu diesen Parametern finden Sie unter Objekt. CDMA

```
{
    "Timestamp": 1664313161,           // optional
    "CellTowers": {
        "Wcdma": [
        {
          "Mcc": int,                   // required
          "Mnc": int,                   // required
          "UtranCid": int,              // required
          "Lac": int,                   // optional
```

```
          "WcdmaLocalId": {             // optional
              "Uarfcndl": int,          // required
              "Psc": int,               // required
          },
          "Rscp": int,                  // optional
          "Pathloss": int,              // optional
          "WcdmaNmr": [                 // optional
                {
                  "Uarfcndl": int,      // required
                  "Psc": int,           // required
                  "UtranCid": int,      // required
                  "Rscp": int,          // optional
                  "Pathloss": int,      // optional
                }
             ]
          }
       ]
    }
}
```

TD- SCDMA (Zeitteilung, synchrone Codeteilung, Mehrfachzugriff)

Wenn Sie diese Messungsdaten verwenden, müssen Sie Informationen wie das Netzwerk und die Landesvorwahl, die Signalleistung und Identifikationsinformationen, Informationen zur Basisstation und optionale weitere Parameter angeben. Der nachfolgende Code zeigt ein Beispiel für das Nutzlastformat. Weitere Informationen zu diesen Parametern finden Sie unter Objekt. CDMA

```
{
    "Timestamp": 1664313161,           // optional
    "CellTowers": {
        "Tdscdma": [
        {
          "Mcc": int,                   // required
          "Mnc": int,                   // required
          "UtranCid": int,              // required
          "Lac": int,                   // optional
          "TdscdmaLocalId": {           // optional
              "Uarfcn": int,            // required
              "CellParams": int,        // required
          },
          "TdscdmaTimingAdvance": int,  // optional
          "Rscp": int,                  // optional
          "Pathloss": int,              // optional
```

```
          "TdscdmaNmr": [               // optional
                {
                  "Uarfcn": int,        // required
                  "CellParams": int,    // required
                  "UtranCid": int,      // optional
                  "Rscp": int,          // optional
                  "Pathloss": int,      // optional
                }
             ]
          }
       ]
    }
}
```

## IP-Reverse-Lookup-Solver

Sie können den IP-Reverse-Lookup-Solver verwenden, um den Standort mithilfe der IP-Adresse als Eingabe aufzulösen. Der Solver kann die Standortinformationen von Geräten abrufen, für die die Geräte bereitgestellt wurden. AWS IoT Geben Sie die IP-Adressinformationen in einem Format an, das entweder dem IPv6 Standardmuster IPv4 oder dem IPv6 Hex-komprimierten Muster entspricht. Anschließend erhalten Sie die aufgelöste Standortschätzung, einschließlich zusätzlicher Informationen wie Stadt und Land, in denen sich das Gerät befindet.

> **Note**
>
> Durch die Verwendung des IP-Reverse-Lookup-Solvers erklären Sie sich damit einverstanden, diesen nicht zum Zweck der Identifizierung oder Ortung eines bestimmten Haushalts oder einer Straßenadresse zu verwenden.

Beispiel für eine Nutzlast des IP-Reverse-Lookup-Solvers

Der folgende Code zeigt ein Beispiel für die JSON Nutzdaten des Geräts, das die Messdaten enthält. Wenn AWS IoT Core Device Location die IP-Adressinformationen in den Messdaten empfängt, sucht es diese Informationen in der Datenbank des Solver-Anbieters, die dann zur Auflösung der Standortinformationen verwendet wird. Um die Informationen abzurufen, geben Sie entweder die JSON Payload in diesem Format an, oder geben Sie Werte für den IP-Parameter des GetPositionEstimateAPIVorgangs an.

> **Note**
>
> Wenn dieser Solver verwendet wird, werden zusätzlich zu den Koordinaten auch die Stadt, das Bundesland, das Land und die Postleitzahl gemeldet, in denen sich das Gerät befindet. Ein Beispiel finden Sie unter Auflösen des Gerätestandorts (Konsole).

```
{
    "Timestamp": 1664313161,
    "Ip":{
        "IpAddress":"54.240.198.35"
      }
}
```

## GNSSSolver

Verwenden Sie den Solver GNSS (Global Navigation Satellite System), um den Gerätestandort anhand der in den Meldungen oder NAV Meldungen der GNSS Scanergebnisse enthaltenen Informationen abzurufen. Sie können optional zusätzliche GNSS Hilfsinformationen angeben, wodurch die Anzahl der Variablen reduziert wird, die der Solver für die Suche nach Signalen verwenden muss. Durch die Bereitstellung dieser unterstützenden Informationen, zu denen Position, Höhe, Erfassungszeit und Genauigkeitsinformationen gehören, kann der Solver die Satelliten im Sichtfeld leicht identifizieren und den Gerätestandort berechnen.

Dieser Solver kann mit LoRa WAN Geräten und anderen Geräten verwendet werden, für die eine Bereitstellung vorgesehen ist. AWS IoT Bei allgemeinen IoT-Geräten gilt: Wenn die Geräte die StandortschätzungunterstützenGNSS, indem die Transceiver die Standortinformationen auflösen, wenn die GNSS Scaninformationen vom Gerät empfangen werden. Bei LoRa WAN Geräten müssen die Geräte über den Edge-Chipsatz verfügen. LoRa Wenn eine Uplink-Nachricht vom Gerät empfangen wird, werden die GNSS Scandaten an das Gerät gesendet AWS IoT Core for LoRaWAN, und der Standort wird anhand der Scanergebnisse der Transceiver geschätzt.

GNSSBeispiel für eine Solver-Payload

Der folgende Code zeigt ein Beispiel für die JSON Nutzdaten des Geräts, das die Messdaten enthält. Wenn AWS IoT Core Device Location die GNSS Scan-Informationen empfängt, die die Nutzdaten in den Messdaten enthalten, verwendet es die Transceiver und alle zusätzlichen enthaltenen Hilfsinformationen, um nach Signalen zu suchen und die Standortinformationen aufzulösen. Um die

Informationen abzurufen, geben Sie entweder die JSON Nutzdaten in diesem Format an oder geben Sie Werte für den Gnss-Parameter der Operation an. GetPositionEstimateAPI

> **Note**
>
> Bevor AWS IoT Core Device Location den Gerätestandort ermitteln kann, müssen Sie das Zielbyte aus der Payload entfernen.

```
{
    "Timestamp": 1664313161,                    // optional
    "Gnss": {
        "AssistAltitude": number,               // optional
        "AssistPosition": [ number ],           // optional
        "CaptureTime": number,                  // optional
        "CaptureTimeAccuracy": number,          // optional
        "Payload": "string",                    // required
        "Use2DSolver": boolean                  // optional
   }
}
```

# Ereignismeldungen

Dieser Abschnitt enthält Informationen zu Nachrichten, die veröffentlicht werden AWS IoT , wenn Dinge oder Jobs aktualisiert oder geändert werden. Informationen zu dem AWS IoT Events Dienst, mit dem Sie Melder einrichten können, mit denen Sie Ihre Geräte auf Ausfälle oder Betriebsänderungen überwachen und bei deren Auftreten Aktionen auslösen können, finden Sie unter AWS IoT Events.

## Generieren von Ereignisnachrichten

AWS IoT veröffentlicht Ereignismeldungen, wenn bestimmte Ereignisse eintreten. Beispielsweise werden Ereignisse von der Registry generiert, wenn Geräte hinzugefügt, aktualisiert oder gelöscht werden. Jedes Ereignis bewirkt, dass eine einzelne Ereignismeldung gesendet wird. Ereignismeldungen werden MQTT zusammen mit einer JSON Payload veröffentlicht. Der Inhalt der Nutzlast hängt von der Art des Ereignisses ab.

> **Note**
>
> Ereignismeldungen werden garantiert einmal veröffentlicht. Es ist möglich, dass sie mehr als einmal veröffentlicht werden. Die Reihenfolge von Ereignismeldungen ist nicht garantiert.

### Richtlinie für den Empfang von Ereignisnachrichten

Um Ereignisnachrichten zu empfangen, muss Ihr Gerät eine entsprechende Richtlinie verwenden, die es ermöglicht, eine Verbindung zum AWS IoT Gerätegateway herzustellen und MQTT Veranstaltungsthemen zu abonnieren. Sie müssen auch die entsprechenden Themenfilter abonnieren.

Es folgt ein Beispiel der für den Empfang von Ereignissen zum Lebenszyklus erforderlichen Richtlinie:

```
{
    "Version":"2012-10-17",
    "Statement":[{
        "Effect":"Allow",
        "Action":[
            "iot:Subscribe",
            "iot:Receive"
```

```
        ],
        "Resource":[
            "arn:aws:iot:region:account:/$aws/events/*"
        ]
    }]
}
```

# Ereignisse aktivieren für AWS IoT

Bevor Abonnenten der reservierten Themen Nachrichten empfangen können, müssen Sie mithilfe von AWS Management Console Oder die Option API oder aktivierenCLI. Informationen zu den Ereignisnachrichten, die mit den verschiedenen Optionen verwaltet werden, finden Sie in der Tabelle mit den Einstellungen für die AWS IoT Ereigniskonfiguration.

- Um Ereignismeldungen zu aktivieren, wechseln Sie in der AWS IoT Konsole zur Registerkarte Einstellungen und wählen Sie dann im Abschnitt Ereignisbasierte Nachrichten die Option Ereignisse verwalten aus. Sie können die Ereignisse angeben, die Sie verwalten möchten.
- Um mithilfe des Befehls API oder zu steuern, welche Ereignistypen veröffentlicht werdenCLI, rufen Sie den update-event-configurations CLI Befehl UpdateEventConfigurationsAPIoder auf. Beispielsweise:

```
aws iot update-event-configurations --event-configurations "{\"THING\":{\"Enabled\":
 true}}"
```

> **Note**
>
> Alle Anführungszeichen („“) werden durch Backslashes (\) umgangen.

Sie können die aktuelle Ereigniskonfiguration abrufen, indem Sie DescribeEventConfigurationsAPIoder mit dem describe-event-configurations CLI Befehl aufrufen. Zum Beispiel:.

```
aws iot describe-event-configurations
```

Tabelle der Einstellungen für die AWS IoT -Ereigniskonfiguration

| Ereigniskategorie<br><br>(AWS IoT Konsole: Einstellungen: Ereignisbasierte Nachrichten) | **`eventConfigurations`** - Schlüsselwert<br><br>(AWS CLI/API) | Topic der Ereignismeldung |
|---|---|---|
| (Kann nur mit dem AWS CLI/APIkonfiguriert werden) | `CA_CERTIFICATE` | `$aws/events/certificates/registered/` *`caCertificateId`* |
| (Kann nur mit dem AWS CLI/konfiguriert werdenAPI) | `CERTIFICATE` | `$aws/events/presence/connected/` *`clientId`* |
| (Kann nur mit dem AWS CLI/konfiguriert werdenAPI) | `CERTIFICATE` | `$aws/events/presence/disconnected/` *`clientId`* |
| (Kann nur mit dem AWS CLI/konfiguriert werdenAPI) | `CERTIFICATE` | `$aws/events/subscriptions/subscribed/` *`clientId`* |
| (Kann nur mit dem AWS CLI/konfiguriert werdenAPI) | `CERTIFICATE` | `$aws/events/subscriptions/unsubscribed/` *`clientId`* |
| Auftrag abgeschlossen, storniert | `JOB` | `$aws/events/job/`*`jobID`*`/canceled` |
| Auftrag abgeschlossen, storniert | `JOB` | `$aws/events/job/`*`jobID`*`/cancellation_in_progress` |
| Auftrag abgeschlossen, storniert | `JOB` | `$aws/events/job/`*`jobID`*`/completed` |
| Auftrag abgeschlossen, storniert | `JOB` | `$aws/events/job/`*`jobID`*`/deleted` |

| Ereigniskategorie<br><br>(AWS IoT Konsole: Einstellungen: Ereignisbasierte Nachrichten) | **`eventConfigurations`** - Schlüsselwert<br><br>(AWS CLI/API) | Topic der Ereignismeldung |
|---|---|---|
| Auftrag abgeschlossen, storniert | `JOB` | `$aws/events/job/`*`jobID`*`/deletion_in_progress` |
| Auftragsausführung: erfolgreich, abgelehnt, storniert, entfernt | `JOB_EXECUTION` | `$aws/events/jobExecution/ `*`jobID`*`/canceled` |
| Auftragsausführung: erfolgreich, abgelehnt, storniert, entfernt | `JOB_EXECUTION` | `$aws/events/jobExecution/ `*`jobID`*`/deleted` |
| Auftragsausführung: erfolgreich, abgelehnt, storniert, entfernt | `JOB_EXECUTION` | `$aws/events/jobExecution/ `*`jobID`*`/failed` |
| Auftragsausführung: erfolgreich, abgelehnt, storniert, entfernt | `JOB_EXECUTION` | `$aws/events/jobExecution/ `*`jobID`*`/rejected` |
| Auftragsausführung: erfolgreich, abgelehnt, storniert, entfernt | `JOB_EXECUTION` | `$aws/events/jobExecution/ `*`jobID`*`/removed` |
| Auftragsausführung: erfolgreich, abgelehnt, storniert, entfernt | `JOB_EXECUTION` | `$aws/events/jobExecution/ `*`jobID`*`/succeeded` |
| Auftragsausführung: erfolgreich, abgelehnt, storniert, entfernt | `JOB_EXECUTION` | `$aws/events/jobExecution/ `*`jobID`*`/timed_out` |

| Ereigniskategorie<br><br>(AWS IoT Konsole: Einstellungen: Ereignisbasierte Nachrichten) | **`eventConfigurations`** - Schlüsselwert<br><br>(AWS CLI/API) | Topic der Ereignismeldung |
|---|---|---|
| Objekt: erstellt, aktualisiert, gelöscht | `THING` | `$aws/events/thing/` *`thingName`* `/created` |
| Objekt: erstellt, aktualisiert, gelöscht | `THING` | `$aws/events/thing/` *`thingName`* `/updated` |
| Objekt: erstellt, aktualisiert, gelöscht | `THING` | `$aws/events/thing/` *`thingName`* `/deleted` |
| Objektgruppe: hinzugefügt, entfernt | `THING_GROUP` | `$aws/events/thingGroup/` *`thingGroupName`* `/created` |
| Objektgruppe: hinzugefügt, entfernt | `THING_GROUP` | `$aws/events/thingGroup/` *`thingGroupName`* `/updated` |
| Objektgruppe: hinzugefügt, entfernt | `THING_GROUP` | `$aws/events/thingGroup/` *`thingGroupName`* `/deleted` |
| Objektgruppenhierarchie: hinzugefügt, entfernt | `THING_GROUP_HIERARCHY` | `$aws/events/thingGroupHierarchy/thingGroup/` *`parentThingGroupName`* `/childThingGroup/` *`childThingGroupName`* `/added` |

| Ereigniskategorie<br><br>(AWS IoT Konsole: Einstellungen: Ereignisbasierte Nachrichten) | **`eventConfigurations`** - Schlüsselwert<br><br>(AWS CLI/API) | Topic der Ereignismeldung |
|---|---|---|
| Objektgruppenhierarchie: hinzugefügt, entfernt | `THING_GROUP_HIERARCHY` | `$aws/events/thingGroupHierarchy/thingGroup/` *`parentThingGroupName`* `/childThingGroup/` *`childThingGroupName`* `/removed` |
| Mitgliedschaft in einer Objektgruppe: hinzugefügt, entfernt | `THING_GROUP_MEMBERSHIP` | `$aws/events/thingGroupMembership/thingGroup/` *`thingGroupName`* `/thing/`*`thingName`* `/added` |
| Mitgliedschaft in einer Objektgruppe: hinzugefügt, entfernt | `THING_GROUP_MEMBERSHIP` | `$aws/events/thingGroupMembership/thingGroup/` *`thingGroupName`* `/thing/`*`thingName`* `/removed` |
| Objekttyp: erstellt, aktualisiert, gelöscht | `THING_TYPE` | `$aws/events/thingType/` *`thingTypeName`* `/created` |
| Objekttyp: erstellt, aktualisiert, gelöscht | `THING_TYPE` | `$aws/events/thingType/` *`thingTypeName`* `/updated` |
| Objekttyp: erstellt, aktualisiert, gelöscht | `THING_TYPE` | `$aws/events/thingType/` *`thingTypeName`* `/deleted` |

| Ereigniskategorie<br><br>(AWS IoT Konsole: Einstellungen: Ereignisbasierte Nachrichten) | **`eventConfigurations`** - Schlüsselwert<br><br>(AWS CLI/API) | Topic der Ereignismeldung |
|---|---|---|
| Zuordnung des Objekttyps: hinzugefügt, entfernt | `THING_TYPE_ASSOCIATION` | `$aws/events/thingTypeAssociation/thing/` *`thingName`* `/thingType/` *`thingTypeName`* `/added`<br><br>`$aws/events/thingTypeAssociation/thing/` *`thingName`* `/thingType/` *`thingTypeName`* `/removed` |

# Registry-Ereignisse

Die Registry kann Ereignismeldungen veröffentlichen, wenn Objekte, Objekttypen und Objektgruppen erstellt, aktualisiert oder gelöscht werden. Diese Ereignisse sind jedoch standardmäßig nicht verfügbar. Weitere Informationen darüber, wie Sie diese Ereignisse aktivieren, finden Sie unter Ereignisse aktivieren für AWS IoT.

Die Registry kann die folgenden Ereignistypen bereitstellen:

- Objektereignisse
- Objekttypereignisse
- Objektgruppenereignisse

## Objektereignisse

Sache Created/Updated/Deleted

Die Registry veröffentlicht die folgenden Ereignismeldungen, wenn Objekte erstellt, aktualisiert oder gelöscht werden:

- $aws/events/thing/*thingName*/created
- $aws/events/thing/*thingName*/updated
- $aws/events/thing/*thingName*/deleted

Die Meldungen enthalten die folgende Beispielnutzlast:

```
{
    "eventType" : "THING_EVENT",
    "eventId" : "f5ae9b94-8b8e-4d8e-8c8f-b3266dd89853",
    "timestamp" : 1234567890123,
    "operation" : "CREATED|UPDATED|DELETED",
    "accountId" : "123456789012",
    "thingId" : "b604f69c-aa9a-4d4a-829e-c480e958a0b5",
    "thingName" : "MyThing",
    "versionNumber" : 1,
    "thingTypeName" : null,
    "attributes": {
                "attribute3": "value3",
                "attribute1": "value1",
                "attribute2": "value2"
    }
}
```

Die Nutzlasten enthalten die folgenden Attribute:

eventType

Auf "THING_EVENT“ setzen.

eventId

Eine eindeutige Ereignis-ID (Zeichenfolge).

Zeitstempel

Der UNIX Zeitstempel, zu dem das Ereignis eingetreten ist.

operation

Die Operation, die das Ereignis ausgelöst hat. Gültige Werte für sind:

- CREATED
- UPDATED

- DELETED

accountId

Ihr AWS-Konto Ausweis.

thingId

Die ID des gerade erstellten, aktualisierten oder gelöschten Objekts.

thingName

Der Name des gerade erstellten, aktualisierten oder gelöschten Objekts.

versionNumber

Die Version des gerade erstellten, aktualisierten oder gelöschten Objekts. Dieser Wert wird bei der Erstellung eines Objekts auf 1 festgelegt. Er wird bei jeder Aktualisierung des Objekts um 1 erhöht.

thingTypeName

Der mit dem Objekt verknüpfte Objekttyp, sofern vorhanden. Andernfalls `null`.

Attribute

Eine Reihe von mit dem Objekt verknüpften Name-Wert-Paaren.

## Objekttypereignisse

Ereignisse im Zusammenhang mit dem Objekttyp:

- Art der Sache Created/Updated/Deprecated/Undeprecated/Deleted
- Objekttyp einem Objekt zugeordnet/nicht zugeordnet

### Art der Sache Created/Updated/Deprecated/Undeprecated/Deleted

Die Registrierung veröffentlicht die folgenden Ereignismeldungen, wenn Dingtypen erstellt, aktualisiert, veraltet, nicht mehr unterstützt oder gelöscht werden:

- `$aws/events/thingType/`*`thingTypeName`*`/created`
- `$aws/events/thingType/`*`thingTypeName`*`/updated`
- `$aws/events/thingType/`*`thingTypeName`*`/deleted`

Die Nachricht enthält die folgende Beispielnutzlast:

```
{
    "eventType" : "THING_TYPE_EVENT",
    "eventId" : "8827376c-4b05-49a3-9b3b-733729df7ed5",
    "timestamp" : 1234567890123,
    "operation" : "CREATED|UPDATED|DELETED",
    "accountId" : "123456789012",
    "thingTypeId" : "c530ae83-32aa-4592-94d3-da29879d1aac",
    "thingTypeName" : "MyThingType",
    "isDeprecated" : false|true,
    "deprecationDate" : null,
    "searchableAttributes" : [ "attribute1", "attribute2", "attribute3" ],
    "propagatingAttributes": [
        {
     "userPropertyKey": "key",
     "thingAttribute": "model"
        },
        {
     "userPropertyKey": "key",
     "connectionAttribute": "iot:ClientId"
        }
    ],
    "description" : "My thing type"
}
```

Die Nutzlasten enthalten die folgenden Attribute:

eventType

Auf "THING_ _“ gesetzt. TYPE EVENT

eventId

Eine eindeutige Ereignis-ID (Zeichenfolge).

Zeitstempel

Der UNIX Zeitstempel, zu dem das Ereignis eingetreten ist.

operation

Die Operation, die das Ereignis ausgelöst hat. Gültige Werte für sind:

- CREATED

- UPDATED
- DELETED

accountId

Ihr AWS-Konto Ausweis.

thingTypeId

Die ID des Dingtyps, der erstellt, aktualisiert, veraltet oder gelöscht wird.

thingTypeName

Der Name des Dingtyps, der erstellt, aktualisiert, veraltet oder gelöscht wird.

isDeprecated

`true`, wenn der Objekttyp veraltet ist. Andernfalls `false`.

deprecationDate

Der UNIX Zeitstempel, zu dem der Dingtyp veraltet war.

searchableAttributes

Eine Reihe von mit dem Objekttyp verknüpften Name-Wert-Paaren, die für Suchen verwendet werden können.

propagatingAttributes

Eine Liste von Attributen, die sich verbreiten. Ein propagierendes Attribut kann ein Dingattribut, ein Verbindungsattribut und einen Benutzereigenschaftsschlüssel enthalten. Weitere Informationen finden Sie unter Hinzufügen von propagierenden Attributen zur Nachrichtenanreicherung.

description

Eine Beschreibung des Objekttyps.

## Objekttyp einem Objekt zugeordnet/nicht zugeordnet

Die Registry veröffentlicht die folgenden Ereignismeldungen, wenn ein Objekttyp einem Objekt zugeordnet wird oder die Zuordnung entfernt wird.

- `$aws/events/thingTypeAssociation/thing/`*`thingName`*`/thingType/`*`typeName`*`/added`

- `$aws/events/thingTypeAssociation/thing/thingName/thingType/typeName/removed`

Im Folgenden sehen Sie ein Beispiel für eine `added`-Nutzlast. Die Nutzlasten für `removed`-Nachrichten sind ähnlich.

```
{
    "eventId" : "87f8e095-531c-47b3-aab5-5171364d138d",
    "eventType" : "THING_TYPE_ASSOCIATION_EVENT",
    "operation" : "ADDED",
    "thingId" : "b604f69c-aa9a-4d4a-829e-c480e958a0b5",
    "thingName": "myThing",
    "thingTypeName" : "MyThingType",
    "timestamp" : 1234567890123,
}
```

Die Nutzlasten enthalten die folgenden Attribute:

eventId

Eine eindeutige Ereignis-ID (Zeichenfolge).

eventType

Auf "THING_ _ TYPE ASSOCIATION _EVENT“ setzen.

operation

Die Operation, die das Ereignis ausgelöst hat. Gültige Werte für sind:

- ADDED
- REMOVED

thingId

Die ID des Objekts, dessen Zuordnung geändert wurde.

thingName

Der Name des Objekts, dessen Zuordnung geändert wurde.

thingTypeName

Der Objekttyp, der dem Objekt zugeordnet oder nicht mehr zugeordnet ist.

Zeitstempel

Der UNIX Zeitstempel, zu dem das Ereignis eingetreten ist.

## Objektgruppenereignisse

Ereignisse im Zusammenhang mit Objektgruppen:

- Dinggruppe Created/Updated/Deleted
- Objekt, das einer Objektgruppe hinzugefügt/aus dieser entfernt wird
- Objektgruppe, die einer Objektgruppe hinzugefügt/aus dieser gelöscht wird

### Dinggruppe Created/Updated/Deleted

Die Registry veröffentlicht die folgenden Ereignismeldungen, wenn eine Objektgruppe erstellt, aktualisiert oder gelöscht wird.

- `$aws/events/thingGroup/`*`groupName`*`/created`
- `$aws/events/thingGroup/`*`groupName`*`/updated`
- `$aws/events/thingGroup/`*`groupName`*`/deleted`

Im Folgenden sehen Sie ein Beispiel für eine `updated`-Nutzlast. Die Nutzlasten für `created`- und `deleted`-Nachrichten sind ähnlich.

```
{
  "eventType": "THING_GROUP_EVENT",
  "eventId": "8b9ea8626aeaa1e42100f3f32b975899",
  "timestamp": 1603995417409,
  "operation": "UPDATED",
  "accountId": "571EXAMPLE833",
  "thingGroupId": "8757eec8-bb37-4cca-a6fa-403b003d139f",
  "thingGroupName": "Tg_level5",
  "versionNumber": 3,
  "parentGroupName": "Tg_level4",
  "parentGroupId": "5fce366a-7875-4c0e-870b-79d8d1dce119",
  "description": "New description for Tg_level5",
  "rootToParentThingGroups": [
    {
      "groupArn": "arn:aws:iot:us-west-2:571EXAMPLE833:thinggroup/TgTopLevel",
```

```
      "groupId": "36aa0482-f80d-4e13-9bff-1c0a75c055f6"
    },
    {
      "groupArn": "arn:aws:iot:us-west-2:571EXAMPLE833:thinggroup/Tg_level1",
      "groupId": "bc1643e1-5a85-4eac-b45a-92509cbe2a77"
    },
    {
      "groupArn": "arn:aws:iot:us-west-2:571EXAMPLE833:thinggroup/Tg_level2",
      "groupId": "0476f3d2-9beb-48bb-ae2c-ea8bd6458158"
    },
    {
      "groupArn": "arn:aws:iot:us-west-2:571EXAMPLE833:thinggroup/Tg_level3",
      "groupId": "1d9d4ffe-a6b0-48d6-9de6-2e54d1eae78f"
    },
    {
      "groupArn": "arn:aws:iot:us-west-2:571EXAMPLE833:thinggroup/Tg_level4",
      "groupId": "5fce366a-7875-4c0e-870b-79d8d1dce119"
    }
  ],
  "attributes": {
    "attribute1": "value1",
    "attribute3": "value3",
    "attribute2": "value2"
  },
  "dynamicGroupMappingId": null
}
```

Die Nutzlasten enthalten die folgenden Attribute:

eventType

Auf "THING_ GROUP _EVENT“ setzen.

eventId

Eine eindeutige Ereignis-ID (Zeichenfolge).

Zeitstempel

Der UNIX Zeitstempel, zu dem das Ereignis eingetreten ist.

operation

Die Operation, die das Ereignis ausgelöst hat. Gültige Werte für sind:

- CREATED

- UPDATED
- DELETED

accountId

Ihr AWS-Konto Ausweis.

thingGroupId

Die ID der gerade erstellten, aktualisierten oder gelöschten Objektgruppe.

thingGroupName

Der Name der gerade erstellten, aktualisierten oder gelöschten Objektgruppe.

versionNumber

Die Version der Objektgruppe. Dieser Wert wird bei der Erstellung einer Objektgruppe auf 1 festgelegt. Er wird bei jeder Aktualisierung der Objektgruppe um 1 erhöht.

parentGroupName

Der Name der übergeordneten Objektgruppe (sofern vorhanden).

parentGroupId

Die ID der übergeordneten Objektgruppe (sofern vorhanden).

description

Eine Beschreibung der Objektgruppe.

rootToParentThingGroups

Ein Array mit Informationen zur übergeordneten Objektgruppe. Es gibt ein Element für jede übergeordnete Objektgruppe. Der erste Eintrag bezieht sich auf die Stamm-Objektgruppe und dies wird fortgesetzt, bis die übergeordnete Objektgruppe erreicht wurde. Jeder Eintrag enthält die Werte `groupArn` und `groupId` der Objektgruppe.

Attribute

Eine Reihe von mit der Objektgruppe verknüpften Name-Wert-Paaren.

## Objekt, das einer Objektgruppe hinzugefügt/aus dieser entfernt wird

Die Registry veröffentlicht die folgenden Ereignismeldungen, wenn ein Objekt einer Objektgruppe hinzugefügt oder aus dieser entfernt wird.

- `$aws/events/thingGroupMembership/thingGroup/thingGroupName/thing/thingName/added`
- `$aws/events/thingGroupMembership/thingGroup/thingGroupName/thing/thingName/removed`

Die Meldungen enthalten die folgende Beispielnutzlast:

```
{
    "eventType" : "THING_GROUP_MEMBERSHIP_EVENT",
    "eventId" : "d684bd5f-6f6e-48e1-950c-766ac7f02fd1",
    "timestamp" : 1234567890123,
    "operation" : "ADDED|REMOVED",
    "accountId" : "123456789012",
    "groupArn" : "arn:aws:iot:ap-northeast-2:123456789012:thinggroup/
MyChildThingGroup",
    "groupId" : "06838589-373f-4312-b1f2-53f2192291c4",
    "thingArn" : "arn:aws:iot:ap-northeast-2:123456789012:thing/MyThing",
    "thingId" : "b604f69c-aa9a-4d4a-829e-c480e958a0b5",
    "membershipId" : "8505ebf8-4d32-4286-80e9-c23a4a16bbd8"
}
```

Die Nutzlasten enthalten die folgenden Attribute:

eventType

Auf "THING_ _ GROUP MEMBERSHIP _EVENT“ setzen.

eventId

Die Ereignis-ID.

Zeitstempel

Der UNIX Zeitstempel für den Zeitpunkt, zu dem das Ereignis eingetreten ist.

operation

`ADDED`, wenn ein Objekt zu einer Objektgruppe hinzugefügt wird, `REMOVED`, wenn ein Objekt aus einer Objektgruppe entfernt wird.

accountId

Deine AWS-Konto ID.

groupArn

Der ARN der Dinggruppe.

groupId

Die ID der Gruppe.

thingArn

Das ARN Ding, das der Dinggruppe hinzugefügt oder daraus entfernt wurde.

thingId

Die ID des Objekts, das der Objektgruppe hinzugefügt bzw. daraus entfernt wurde.

membershipId

Eine ID, die die Beziehung zwischen dem Objekt und der Objektgruppe angibt. Dieser Wert wird generiert, wenn Sie ein Objekt zu einer Objektgruppe hinzufügen.

## Objektgruppe, die einer Objektgruppe hinzugefügt/aus dieser gelöscht wird

Die Registry veröffentlicht die folgenden Ereignismeldungen, wenn eine Objektgruppe einer anderen Objektgruppe hinzugefügt oder aus dieser entfernt wird.

- `$aws/events/thingGroupHierarchy/thingGroup/`*`parentThingGroupName`*`/childThingGroup/`*`childThingGroupName`*`/added`
- `$aws/events/thingGroupHierarchy/thingGroup/`*`parentThingGroupName`*`/childThingGroup/`*`childThingGroupName`*`/removed`

Die Nachricht enthält die folgende Beispielnutzlast:

```
{
    "eventType" : "THING_GROUP_HIERARCHY_EVENT",
    "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"
```

```
}
```

Die Nutzlasten enthalten die folgenden Attribute:

eventType

Auf "THING_ _ GROUP HIERARCHY _EVENT“ gesetzt.

eventId

Die Ereignis-ID.

Zeitstempel

Der UNIX Zeitstempel für den Zeitpunkt, zu dem das Ereignis eingetreten ist.

operation

`ADDED`, wenn ein Objekt zu einer Objektgruppe hinzugefügt wird, `REMOVED`, wenn ein Objekt aus einer Objektgruppe entfernt wird.

accountId

Deine AWS-Konto ID.

thingGroupId

Die ID der übergeordneten Objektgruppe.

thingGroupName

Der Name der übergeordneten Objektgruppe.

childGroupId

Die ID der untergeordneten Objektgruppe.

childGroupName

Der Name der untergeordneten Objektgruppe.

# Auftragsereignisse

Der AWS IoT Jobs-Dienst veröffentlicht zu bestimmten Themen im MQTT Protokoll, wenn Jobs ausstehen, abgeschlossen oder storniert sind und wenn ein Gerät bei der Ausführung eines Jobs

Erfolg oder Misserfolg meldet. Geräte oder Management- und Überwachungsanwendungen können den Status der Aufträge nachverfolgen, indem sie diese Topics abonnieren.

Aktivieren von Ereignisbenachrichtigungen

Antwortnachrichten des AWS IoT Jobs-Dienstes werden nicht über den Message Broker weitergeleitet und können auch nicht von anderen Clients oder Regeln abonniert werden. Verwenden Sie die Topics `notify` and `notify-next`, um Nachrichten zu Auftragsaktivitäten zu abonnieren. Weitere Informationen über auftragsbezogene Topics finden Sie unter Auftragsthemen.

Um über Job-Updates informiert zu werden, aktivieren Sie diese Job-Ereignisse mithilfe von oder mithilfe von API oderCLI. AWS Management Console Weitere Informationen finden Sie unter Ereignisse aktivieren für AWS IoT.

Funktionsweise von Auftragsereignissen

Da das Abbrechen oder Löschen eines Auftrags einige Zeit in Anspruch nehmen kann, werden zwei Nachrichten gesendet, um den Start und das Ende einer Anfrage anzuzeigen. Wenn zum Beispiel eine Abbruchanfrage gestartet wird, wird eine Nachricht an das `$aws/events/job/jobID/cancellation_in_progress`-Thema gesendet. Wenn die Abbruchanfrage abgeschlossen ist, wird eine Nachricht an das `$aws/events/job/jobID/canceled`-Thema gesendet.

Ein ähnlicher Prozess findet bei einer Anfrage zur Löschung eines Auftrags statt. Management- und Überwachungsanwendungen können diese Themen abonnieren, um den Status von Aufträgen nachzuverfolgen. Weitere Informationen zum Veröffentlichen und Abonnieren von MQTT Themen finden Sie unterthe section called “Gerätekommunikationsprotokolle”.

Auftragsereignistypen

Im Folgenden werden die verschiedenen Arten von Auftragsereignissen dargestellt:

Job Completed/Canceled/Deleted

Der AWS IoT Jobs-Dienst veröffentlicht eine Nachricht zu einem MQTT Thema, wenn ein Job abgeschlossen, storniert oder gelöscht wird oder wenn gerade ein Auftrag storniert oder gelöscht wird:

- `$aws/events/job/`*`jobID`*`/completed`
- `$aws/events/job/`*`jobID`*`/canceled`
- `$aws/events/job/`*`jobID`*`/deleted`

- `$aws/events/job/jobID/cancellation_in_progress`
- `$aws/events/job/jobID/deletion_in_progress`

Die `completed`-Nachricht enthält die folgende Beispielnutzlast:

```
{
  "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/2fc4c0a4-6e45-4525-
a238-0fe8d3dd21bb"
  ],
  "description": "My Job Description",
  "completedAt": 1234567890123,
  "createdAt": 1234567890123,
  "lastUpdatedAt": 1234567890123,
  "jobProcessDetails": {
    "numberOfCanceledThings": 0,
    "numberOfRejectedThings": 0,
    "numberOfFailedThings": 0,
    "numberOfRemovedThings": 0,
    "numberOfSucceededThings": 3
  }
}
```

Die `canceled`-Nachricht enthält die folgende Beispielnutzlast.

```
{
  "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
}
```

Die `deleted`-Nachricht enthält die folgende Beispielnutzlast.

```
{
      "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"
    }
```

Die `cancellation_in_progress`-Nachricht enthält die folgende Beispielnutzlast:

```
{
      "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"
    }
```

Die `deletion_in_progress`-Nachricht enthält die folgende Beispielnutzlast:

```
{
      "eventType": "JOB",
      "eventId": "568d2ade-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"
    }
```

### Endstatus der Auftragsausführung

Der AWS IoT Jobs-Dienst veröffentlicht eine Meldung, wenn ein Gerät eine Auftragsausführung auf den Terminalstatus aktualisiert:

- `$aws/events/jobExecution/`*`jobID`*`/succeeded`
- `$aws/events/jobExecution/`*`jobID`*`/failed`
- `$aws/events/jobExecution/`*`jobID`*`/rejected`
- `$aws/events/jobExecution/`*`jobID`*`/canceled`

- `$aws/events/jobExecution/jobID/timed_out`
- `$aws/events/jobExecution/jobID/removed`
- `$aws/events/jobExecution/jobID/deleted`

Die Nachricht enthält die folgende Beispielnutzlast:

```
{
  "eventType": "JOB_EXECUTION",
  "eventId": "cca89fa5-8a7f-4ced-8c20-5e653afb3572",
  "timestamp": 1234567890,
  "operation": "succeeded|failed|rejected|canceled|removed|timed_out",
  "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|TIMED_OUT",
  "statusDetails": {
    "key": "value"
  }
}
```

# Ereignisse im Lebenszyklus

AWS IoT kann Lebenszyklusereignisse zu den MQTT Themen veröffentlichen. Diese Ereignisse stehen standardmäßig zur Verfügung und können nicht deaktiviert werden.

> **Note**
>
> Nachrichten zum Lebenszyklus können ohne feste Reihenfolge gesendet werden. Unter Umständen erhalten Sie einzelne Nachrichten auch mehrfach.
> `thingName`wird nur berücksichtigt, wenn der Client über die Funktion „Exklusive Dinge“ eine Verbindung herstellt.

In diesem Thema:


- „Verbinden/Verbindung trennen“-Ereignisse
- Ereignis mit fehlgeschlagenem Verbindungsversuch
- „Abonnieren/Abonnement beenden“-Ereignisse

# „Verbinden/Verbindung trennen“-Ereignisse

> **Note**
>
> Mit der AWS IoT Device Management-Flottenindizierung können Sie nach Dingen suchen, aggregierte Abfragen ausführen und dynamische Gruppen auf der Grundlage von Connect/Disconnect-Ereignissen für Dinge erstellen. Weitere Informationen finden Sie unter Flottenindizierung.

AWS IoT veröffentlicht eine Nachricht zu den folgenden MQTT Themen, wenn ein Client eine Verbindung herstellt oder trennt:

- `$aws/events/presence/connected/clientId`: Ein Client, der mit dem Message Broker verbunden ist.
- `$aws/events/presence/disconnected/clientId`: Ein Client, dessen Verbindung mit dem Message Broker getrennt wurde

Im Folgenden finden Sie eine Liste der JSON Elemente, die in den zu diesem Thema veröffentlichten Verbindungs-/Trennungsmeldungen enthalten sind. `$aws/events/presence/connected/clientId`

clientId

Die Client-ID des Clients, der eine Verbindung herstellt oder trennt

> **Note**
>
> ClientsIDs, die # oder + enthalten, empfangen keine Lebenszyklusereignisse.

thingName

Der Name deiner IoT-Sache. `thingName`wird nur aufgenommen, wenn der Client über die exklusive Ding-Funktion eine Verbindung herstellt.

clientInitiatedDisconnect

„True“, wenn der Client die Verbindungstrennung initiiert hat. Ansonsten „false”. Nur in Trennungsnachrichten.

disconnectReason

Der Grund, warum der Client die Verbindung trennt. Nur in Trennungsnachrichten. Die folgende Tabelle enthält gültige Werte und gibt an, ob der Broker beim Verbindungsabbruch Nachrichten in Form von Last Will und Testament (LWT) sendet.

| Grund für das Trennen der Verbindung | Beschreibung | Der Broker sendet die Nachrichten LWT |
|---|---|---|
| `AUTH_ERROR` | Der Client konnte sich nicht authentifizieren, oder die Autorisierung ist fehlgeschlagen. | Ja. Wenn das Gerät vor dem Empfang dieses Fehlers über eine aktive Verbindung verfügt. |
| `CLIENT_INITIATED_DISCONNECT` | Der Client gibt an, dass die Verbindung getrennt wird. Der Client kann dies tun, indem er entweder ein MQTT `DISCONNECT` Steuerpaket sendet oder `Close frame` ob der Client eine WebSocket Verbindung verwendet. | Nein. |
| `CLIENT_ERROR` | Der Client hat etwas falsch gemacht, das dazu führt, dass die Verbindung getrennt wird. Beispielsweise wird die Verbindung zu einem Client unterbrochen, wenn er mehr als ein MQTT `CONNECT` Paket über dieselbe Verbindung sendet oder wenn der Client versucht, mit einer Payload zu veröffentlichen, die das Payload-Limit überschreitet. | Ja. |
| `CONNECTION_LOST` | Die Client-Server-Verbindung wird unterbrochen. Dies kann während eines Zeitraums mit hoher Netzwerklatenz geschehen, oder wenn die Internetverbindung unterbrochen wird. | Ja. |

| Grund für das Trennen der Verbindung | Beschreibung | Der Broker sendet die Nachrichten LWT |
|---|---|---|
| DUPLICATE_CLIENTID | Der Client verwendet eine Client-ID, die bereits verwendet wird. In diesem Fall wird der Client, der bereits verbunden ist, mit diesem Trenngrund getrennt. | Ja. |
| FORBIDDEN_ACCESS | Der Client darf keine Verbindung herstellen. So kann ein Client beispielsweise mit einer abgelehnten IP-Adresse keine Verbindung herstellen. | Ja. Wenn das Gerät vor dem Empfang dieses Fehlers über eine aktive Verbindung verfügt. |
| MQTT_KEEP_ALIVE_TIMEOUT | Wenn es für das 1,5-fache der Keepalive-Zeit des Clients keine Client-Server-Kommunikation gibt, wird der Client getrennt. | Ja. |
| SERVER_ERROR | Trennung der Verbindung aufgrund unerwarteter Serverprobleme. | Ja. |
| SERVER_INITIATED_DISCONNECT | Der Server trennt einen Client aus betrieblichen Gründen absichtlich. | Ja. |
| THROTTLED | Der Client wird getrennt, weil er ein Drosselungslimit überschritten hat. | Ja. |
| WEBSOCKET_TTL_EXPIRATION | Die Verbindung mit dem Client wird unterbrochen, weil die Verbindung mit a WebSocket länger dauert als der angegebene Wert. time-to-live | Ja. |
| CUSTOMAUTH_TTL_EXPIRATION | Die Verbindung zum Client wurde unterbrochen, weil die Verbindung länger dauert als der time-to-live Wert seines benutzerdefinierten Autorisierers. | Ja. |

eventType

Der Ereignistyp. Gültige Werte sind `connected` oder `disconnected`.

ipAddress

Die IP-Adresse des verbindenden Clients. Dies kann im Oder-Format IPv4 sein. IPv6 Nur in Verbindungsnachrichten.

principalIdentifier

Die zur Anmeldung verwendeten Anmeldeinformationen. Bei Zertifikaten zur TLS gegenseitigen Authentifizierung ist dies die Zertifikat-ID. Für andere Verbindungsarten sind dies die IAM-Anmeldeinformationen.

sessionIdentifier

Ein global eindeutiger Bezeichner AWS IoT , der für die Dauer der Sitzung existiert.

Zeitstempel

Eine ungefähre Schätzung, wann das Ereignis eingetreten ist.

versionNumber

Die Versionsnummer für das Lebenszyklusereignis. Dies ist ein monoton ansteigender langer Ganzzahlwert für jede Client-ID-Verbindung. Die Versionsnummer kann von einem Abonnenten verwendet werden, um die Reihenfolge der Lebenszyklusereignisse festzustellen.

> **Note**
>
> Die Verbindungs- und Trennungsnachrichten für eine Client-Verbindung haben dieselbe Versionsnummer.
> Die Versionsnummer kann Werte überspringen und wird nicht zwingend konsistent für jedes Ereignis um 1 erhöht.
> Wenn ein Client etwa eine Stunde lang nicht verbunden ist, wird die Versionsnummer auf 0 zurückgesetzt. Bei persistenten Sitzungen wird die Versionsnummer auf 0 zurückgesetzt, nachdem die Verbindung zu einem Client länger unterbrochen wurde als für die persistente Sitzung konfiguriert time-to-live (TTL).

Eine Verbindungsnachricht hat die folgende Struktur.

```
{
```

```
    "clientId": "186b5",
    "thingName": "exampleThing",
    "timestamp": 1573002230757,
    "eventType": "connected",
    "sessionIdentifier": "00000000-0000-0000-0000-000000000000",
    "principalIdentifier": "12345678901234567890123456789012",
    "ipAddress": "192.0.2.0",
    "versionNumber": 0
}
```

Eine Trennungsnachricht hat die folgende Struktur.

```
{
    "clientId": "186b5",
    "thingName": "exampleThing",
    "timestamp": 1573002340451,
    "eventType": "disconnected",
    "sessionIdentifier": "00000000-0000-0000-0000-000000000000",
    "principalIdentifier": "12345678901234567890123456789012",
    "clientInitiatedDisconnect": true,
    "disconnectReason": "CLIENT_INITIATED_DISCONNECT",
    "versionNumber": 0
}
```

### Umgang mit Client-Verbindungstrennungen

Es hat sich bewährt, für Lebenszyklusereignisse, einschließlich Nachrichten aus dem letzten Testament und Testament (LWT), immer einen Wartestatus zu implementieren. Wenn eine getrennte Verbindung signalisiert wird, sollte Ihr Code eine gewisse Zeit warten und überprüfen, ob ein Gerät noch offline ist, bevor Maßnahmen ergriffen werden. Eine Möglichkeit, dies zu tun, ist die Verwendung von SQSDelay Queues. Wenn ein Client ein LWT oder ein Lebenszyklusereignis empfängt, können Sie eine Nachricht in die Warteschlange stellen (z. B. für 5 Sekunden). Wenn die Nachricht verfügbar ist und verarbeitet wird (durch Lambda oder einen anderen Service), können Sie zunächst überprüfen, ob das Gerät immer noch offline ist, bevor Sie zu weiteren Maßnahmen greifen.

## Ereignis mit fehlgeschlagenem Verbindungsversuch

AWS IoT veröffentlicht eine Nachricht zum folgenden MQTT Thema, wenn ein Kunde nicht autorisiert ist, eine Verbindung herzustellen, oder wenn ein Testament konfiguriert ist und der Kunde nicht berechtigt ist, zu diesem letzten Testamentsthema zu veröffentlichen.

```
$aws/events/presence/connect_failed/clientId
```

Im Folgenden finden Sie eine Liste der JSON Elemente, die in den Nachrichten zur Verbindungsautorisierung enthalten sind, die zu `$aws/events/presence/connect_failed/clientId` diesem Thema veröffentlicht wurden.

clientId

Die Client-ID des Clients, der versucht hat, eine Verbindung herzustellen, aber fehlgeschlagen ist.

> **Note**
>
> ClientsIDs, die # oder + enthalten, empfangen keine Lebenszyklusereignisse.

thingName

Der Name deiner IoT-Sache. `thingName`wird nur aufgenommen, wenn der Client über die exklusive Ding-Funktion eine Verbindung herstellt.

Zeitstempel

Eine ungefähre Schätzung, wann das Ereignis eingetreten ist.

eventType

Der Ereignistyp. Gültiger Wert ist`connect_failed`.

connectFailureReason

Der Grund, warum die Verbindung fehlschlägt. Gültiger Wert ist`AUTHORIZATION_FAILED`.

principalIdentifier

Die zur Anmeldung verwendeten Anmeldeinformationen. Bei Zertifikaten zur TLS gegenseitigen Authentifizierung ist dies die Zertifikat-ID. Für andere Verbindungsarten sind dies die IAM-Anmeldeinformationen.

sessionIdentifier

Ein global eindeutiger Bezeichner AWS IoT , der für die Dauer der Sitzung existiert.

ipAddress

Die IP-Adresse des verbindenden Clients. Dies kann in unserem IPv4 IPv6 Format sein. Nur in Verbindungsnachrichten.

Eine Meldung über einen Verbindungsfehler hat die folgende Struktur.

```
{
    "clientId": "186b5",
    "thingName": "exampleThing",
    "timestamp": 1460065214626,
    "eventType": "connect_failed",
    "connectFailureReason": "AUTHORIZATION_FAILED",
    "principalIdentifier": "12345678901234567890123456789012",
    "sessionIdentifier": "00000000-0000-0000-0000-000000000000",
    "ipAddress" : "192.0.2.0"
}
```

## „Abonnieren/Abonnement beenden“-Ereignisse

AWS IoT veröffentlicht eine Nachricht zum folgenden MQTT Thema, wenn ein Client ein Thema abonniert oder abbestellt: MQTT

```
$aws/events/subscriptions/subscribed/clientId
```

or

```
$aws/events/subscriptions/unsubscribed/clientId
```

Wo `clientId` ist die MQTT Client-ID, die eine Verbindung zum Message Broker herstellt? AWS IoT

Die im Topic veröffentlichte Nachricht weist die folgende Struktur auf:

```
{
    "clientId": "186b5",
    "thingName": "exampleThing",
    "timestamp": 1460065214626,
    "eventType": "subscribed" | "unsubscribed",
    "sessionIdentifier": "00000000-0000-0000-0000-000000000000",
    "principalIdentifier": "12345678901234567890123456789012",
    "topics" : ["foo/bar","device/data","dog/cat"]
}
```

Im Folgenden finden Sie eine Liste der JSON Elemente, die in den abonnierten und abgemeldeten Nachrichten enthalten sind, die in den Themen und Themen veröffentlicht wurden. `$aws/`

`events/subscriptions/subscribed/`*`clientId`* `$aws/events/subscriptions/unsubscribed/`*`clientId`*

clientId

Die Client-ID des Clients, der ein Topic abonniert oder das Abonnement abbestellt.

> **Note**
>
> ClientsIDs, die # oder + enthalten, empfangen keine Lebenszyklusereignisse.

thingName

Der Name deiner IoT-Sache. `thingName`wird nur aufgenommen, wenn der Client über die exklusive Ding-Funktion eine Verbindung herstellt.

eventType

Der Ereignistyp. Gültige Werte sind `subscribed` oder `unsubscribed`.

principalIdentifier

Die zur Anmeldung verwendeten Anmeldeinformationen. Bei Zertifikaten zur TLS gegenseitigen Authentifizierung ist dies die Zertifikat-ID. Für andere Verbindungsarten sind dies die IAM-Anmeldeinformationen.

sessionIdentifier

Ein global eindeutiger Bezeichner AWS IoT , der für die Dauer der Sitzung existiert.

Zeitstempel

Eine ungefähre Schätzung, wann das Ereignis eingetreten ist.

topics

Eine Reihe von MQTT Themen, die der Kunde abonniert hat.

> **Note**
>
> Nachrichten zum Lebenszyklus können ohne feste Reihenfolge gesendet werden. Unter Umständen erhalten Sie einzelne Nachrichten auch mehrfach.

# Problembehebung AWS IoT

Helfen Sie uns, dieses Thema zu verbessern

Lassen Sie uns wissen, was dazu beitragen würde, es besser zu machen

Die folgenden Informationen helfen Ihnen möglicherweise bei der Lösung häufiger Probleme in AWS IoT.

Aufgaben

- AWS IoT Core Anleitung zur Fehlerbehebung
- AWS IoT Device Management Leitfaden zur Fehlerbehebung
- AWS IoT Leitfaden zur Fehlerbehebung in Device Advisor
- AWS IoT Fehler

# AWS IoT Core Anleitung zur Fehlerbehebung

Helfen Sie uns, dieses Thema zu verbessern

Lassen Sie uns wissen, was dazu beitragen würde, es besser zu machen

Dies ist der Abschnitt zur Fehlerbehebung für AWS IoT Core.

Themen

- Diagnostizieren von Verbindungsproblemen
- Fehler bei der Regeldiagnose
- Diagnostizieren von Problemen mit Schatten
- Problemdiagnose bei Input-Stream-Aktionen für die Salesforce IoT
- Diagnostizieren von Stream-Limits
- Behebung von Verbindungsabbrüchen bei Geräteflotten

# Diagnostizieren von Verbindungsproblemen

Helfen Sie uns, dieses Thema zu verbessern

Lassen Sie uns wissen, was dazu beitragen würde, es besser zu machen

Eine erfolgreiche Verbindung zu AWS IoT erfordert:

- Eine gültige Verbindung
- Ein gültiges und aktives Zertifikat
- Eine Richtlinie, die die gewünschte Verbindung und den gewünschten Vorgang ermöglicht

## Verbindung

Wie finde ich den richtigen Endpunkt?

- die von `aws iot describe-endpoint --endpoint-type iot:Data-ATS` zurückgegebene `endpointAddress`

  or

- den von `aws iot describe-domain-configuration --domain-configuration-name "domain_configuration_name"` zurückgegebenen `domainName`

Wie finde ich den richtigen Wert für Server Name Indication (SNI)?

Der richtige SNI-Wert ist `endpointAddress`, der vom describe-endpoint-Befehl zurückgegeben wird, oder `domainName`, der vom describe-domain-configuration-Befehl zurückgegeben wird. Es ist dieselbe Adresse wie der Endpunkt im vorherigen Schritt. Beim Verbinden von Geräten mit können Clients die Server Name Indication (SNI) -Erweiterung senden. Dies ist nicht erforderlich, wird aber dringend empfohlen. AWS IoT Core Um Funktionen wie die Registrierung mehrerer Konten, benutzerdefinierte Domänen und VPC-Endpunkte zu verwenden, müssen Sie die SNI-Erweiterung verwenden. Weitere Informationen finden Sie unter Transportsicherheit in AWS IoT.

Wie löse ich ein anhaltendes Verbindungsproblem?

Sie können AWS Device Advisor zur Problembehandlung verwenden. Die vorgefertigten Tests von Device Advisor helfen Ihnen dabei, Ihre Gerätesoftware anhand von Best Practices für die Verwendung von TLS, MQTT, AWS IoT Geräteschatten und AWS IoT -Jobs zu validieren.

Hier ist ein Link zu den vorhandenen Device Advisor-Inhalten.

## Authentifizierung

Geräte müssen authentifiziert werden, um eine Verbindung zu AWS IoT Endpunkten herzustellen. Bei Geräten, die X.509-Clientzertifikate zur Authentifizierung verwendet werden, müssen die Zertifikate registriert AWS IoT und aktiv sein.

Wie authentifizieren meine Geräte AWS IoT Endgeräte?

Fügen Sie das AWS IoT CA-Zertifikat dem Trust Store Ihres Kunden hinzu. Lesen Sie die Dokumentation zu Serverauthentifizierung in AWS IoT Core und folgen Sie dann den Links, um das entsprechende CA-Zertifikat herunterzuladen.

Was wird geprüft, wenn ein Gerät eine Verbindung herstellt AWS IoT?

Wenn ein Gerät versucht, eine Verbindung mit AWS IoT herzustellen:

1. AWS IoT prüft, ob ein gültiges Zertifikat und ein gültiger Wert für Server Name Indication (SNI) vorliegen.
2. AWS IoT überprüft, ob das verwendete Zertifikat im AWS IoT Konto registriert und aktiviert wurde.
3. Wenn ein Gerät versucht, eine Aktion auszuführen AWS IoT, z. B. eine Nachricht zu abonnieren oder zu veröffentlichen, wird die Richtlinie, die dem Zertifikat beigefügt ist, mit dem es eine Verbindung hergestellt hat, überprüft, um zu bestätigen, dass das Gerät berechtigt ist, diese Aktion auszuführen.

Wie kann ich ein korrekt konfiguriertes Zertifikat validieren?

Verwenden Sie den OpenSSL `s_client`-Befehl, um die Verbindung zum AWS IoT -Endpunkt zu überprüfen:

```
openssl s_client -connect custom_endpoint.iot.aws-region.amazonaws.com:8443 -
CAfile CA.pem -cert cert.pem -key privateKey.pem
```

Weitere Informationen zur Verwendung von `openssl s_client` finden Sie in der OpenSSL s_client-Dokumentation.

Wie überprüfe ich den Status eines Zertifikats?

- Listen Sie die Zertifikate auf

Wenn Sie die Zertifikat-ID nicht kennen, können Sie den Status all Ihrer Zertifikate mit dem `aws iot list-certificates`-Befehl anzeigen.

- Zertifikatdetails anzeigen

  Wenn Sie die ID des Zertifikats kennen, zeigt Ihnen dieser Befehl detailliertere Informationen zum Zertifikat an.

  ```
  aws iot describe-certificate --certificate-id "certificateId"
  ```

- Überprüfen Sie das Zertifikat in der AWS IoT Konsole

  Wählen Sie in der AWS IoT Konsole im linken Menü die Option Sicher und dann Zertifikate aus.

  Wählen Sie das Zertifikat aus der Liste aus, das Sie für die Verbindung verwenden, um die Detailseite zu öffnen.

  Auf der Detailseite des Zertifikats können Sie seinen aktuellen Status sehen.

  Der Zertifikatstatus kann mit dem Menü Aktionen in der oberen rechten Ecke der Detailseite geändert werden.

## Autorisierung

AWS IoT RessourcenAWS IoT Core Richtlinien, die verwendet werden, um diese Ressourcen zur Ausführung von Aktionen zu autorisieren. Damit eine Aktion autorisiert werden kann, muss den angegebenen AWS IoT Ressourcen ein Richtliniendokument beigefügt sein, das die Genehmigung zur Durchführung dieser Aktion erteilt.

Ich habe die Antwort `PUBNACK` oder `SUBNACK` vom Broker erhalten. Was soll ich tun?

Stellen Sie sicher, dass dem Zertifikat, das Sie für den Anruf verwenden, eine Richtlinie beigefügt ist AWS IoT. Alle Veröffentlichungs-/Anmeldevorgänge werden standardmäßig abgelehnt.

Stellen Sie sicher, dass die beigefügte Richtlinie die Aktionen autorisiert, die Sie ausführen möchten.

Stellen Sie sicher, dass die beigefügte Richtlinie die Ressourcen autorisiert, die versuchen, die autorisierten Aktionen auszuführen.

Ich habe einen AUTHORIZATION_FAILURE-Eintrag in meinen Protokollen.

Stellen Sie sicher, dass dem Zertifikat, das Sie für den Anruf verwenden, eine Richtlinie beigefügt ist AWS IoT. Alle Veröffentlichungs-/Anmeldevorgänge werden standardmäßig abgelehnt.

Stellen Sie sicher, dass die beigefügte Richtlinie die Aktionen autorisiert, die Sie ausführen möchten.

Stellen Sie sicher, dass die beigefügte Richtlinie die Ressourcen autorisiert, die versuchen, die autorisierten Aktionen auszuführen.

Wie überprüfe ich, was die Richtlinie autorisiert?

Wählen Sie in der AWS IoT Konsole im linken Menü Sicherheit und dann Zertifikate aus.

Wählen Sie das Zertifikat aus der Liste aus, das Sie für die Verbindung verwenden, um die Detailseite zu öffnen.

Auf der Detailseite des Zertifikats können Sie seinen aktuellen Status sehen.

Wählen Sie im linken Menü der Detailseite des Zertifikats die Option Richtlinien aus, um die mit dem Zertifikat verknüpften Richtlinien anzuzeigen.

Wählen Sie die gewünschte Richtlinie aus, um ihre Detailseite aufzurufen.

Sehen Sie sich auf der Detailseite der Richtlinie das Richtliniendokument der Richtlinie an, um zu sehen, was damit autorisiert wird.

Wählen Sie Richtliniendokument bearbeiten, um Änderungen am Richtliniendokument vorzunehmen.

## Sicherheits- und Identitätsmethoden

Wenn Sie die Serverzertifikate für die AWS IoT benutzerdefinierte Domänenkonfiguration bereitstellen, haben die Zertifikate maximal vier Domainnamen.

Weitere Informationen finden Sie unter AWS IoT Core -Endpunkte und -Kontingente.

# Fehler bei der Regeldiagnose

> Helfen Sie uns, dieses Thema zu verbessern
>
> Lassen Sie uns wissen, was dazu beitragen würde, es besser zu machen

In diesem Abschnitt werden einige Dinge beschrieben, die Sie überprüfen sollten, wenn Sie auf ein Problem mit einer Regel stoßen.

## Konfiguration von CloudWatch Protokollen für die Problembehandlung

Die beste Methode zum Debuggen von Problemen, die Sie mit Regeln haben, ist die Verwendung von CloudWatch Protokollen. Wenn Sie CloudWatch Logs for aktivieren AWS IoT, können Sie sehen, welche Regeln ausgelöst wurden und ob sie erfolgreich waren oder nicht. Sie werden ebenfalls informiert, ob die Bedingungen der WHERE-Klausel zutreffen. Weitere Informationen finden Sie unter Überwachung AWS IoT mithilfe von Protokollen CloudWatch .

Der häufigsten Probleme in Zusammenhang mit Regeln betreffen die Autorisierung. In den Protokollen wird angezeigt, ob Ihre Rolle nicht autorisiert ist, AssumeRole auf der Ressource zu arbeiten. Hier sehen Sie ein Beispielprotokoll bei einer differenzierten Protokollierung:

```
{
    "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",
        "Table": "trashbin",
        "Operation": "Insert",
        "ItemHashKeyValue": "id",
        "IsPayloadJSON": "true"
    },
    "principalId": "ABCDEFG1234567ABCD890:outis",
```

```
    "details": "User: arn:aws:sts::123456789012:assumed-role/dynamo-
testbin/5aUMInJH is not authorized to perform: dynamodb:PutItem on
 resource: arn:aws:dynamodb:us-east-1:123456789012:table/testbin (Service:
 AmazonDynamoDBv2; Status Code: 400; Error Code: AccessDeniedException; Request ID:
 AKQJ987654321AKQJ123456789AKQJ987654321AKQJ987654321)"
}
```

Hier sehen Sie ein ähnliches Beispielprotokoll bei einer globalen Protokollierung:

```
2017-12-09 22:49:17.954 TRACEID:ff562535-6964-506a-e141-78d40375fc4e
PRINCIPALID:ABCDEFG1234567ABCD890:outis [ERROR] EVENT:DynamoActionFailure
TOPICNAME:test-topic CLIENTID:iotconsole-123456789012-3
MESSAGE:Dynamo Insert record failed. The error received was User:
 arn:aws:sts::123456789012:assumed-role/dynamo-testbin/5aUMInJI is not authorized to
 perform: dynamodb:PutItem on resource: arn:aws:dynamodb:us-east-1:123456789012:table/
testbin
(Service: AmazonDynamoDBv2; Status Code: 400; Error Code: AccessDeniedException;
 Request ID: AKQJ987654321AKQJ987654321AKQJ987654321AKQJ987654321).
Message arrived on: test-topic, Action: dynamo, Table: trashbin, HashKeyField: id,
 HashKeyValue: id, RangeKeyField: None, RangeKeyValue: 123456789012
No newer events found at the moment. Retry.
```

Weitere Informationen finden Sie unter the section called “AWS IoT Protokolle in der CloudWatch Konsole anzeigen”.

## Diagnose externer Services

Externe Services werden vom Endbenutzer reguliert. Stellen Sie vor der Ausführung der Regel sicher, dass die externen Services, die Sie mit Ihrer Regel verknüpft haben, eingerichtet sind und über genügend Durchsatz- und Kapazitätseinheiten für Ihre Anwendung verfügen.

## Diagnose von SQL-Problemen

Wenn Ihre SQL-Abfrage nicht die erwarteten Daten zurückgibt:

- Überprüfen Sie die Protokolle auf Fehlermeldungen.
- Vergewissern Sie sich, dass Ihre SQL-Syntax mit dem JSON-Dokument in der Nachricht übereinstimmt.

Vergleichen Sie die in der Abfrage verwendeten Objekt- und Eigenschaftsnamen mit denen, die im JSON-Dokument der Nachrichtennutzlast des Themas verwendet wurden. Weitere Informationen über die JSON-Formatierung in SQL-Abfragen finden Sie unter JSON-Erweiterungen.

- Prüfen Sie, ob die JSON-Objekt- oder Eigenschaftsnamen reservierte oder numerische Zeichen enthalten.

  Weitere Hinweise zu reservierten Zeichen in JSON-Objektreferenzen in SQL-Abfragen finden Sie unter JSON-Erweiterungen.

## Diagnostizieren von Problemen mit Schatten

Helfen Sie uns, dieses Thema zu verbessern

Lassen Sie uns wissen, was dazu beitragen würde, es besser zu machen

Diagnostizieren von Schatten

| Problem | Richtlinien für die Fehlerbehebung |
| --- | --- |
| Das Schatten-Dokument eines Geräts wird mit `Invalid JSON document` abgelehnt. | Wenn Sie sich mit JSON nicht auskennen, passen Sie die hier aufgeführten Beispiele nach Ihrem Bedarf an. Weitere Informationen finden Sie unter Beispiele für Schatten-Dokumente. |
| Ich habe ein korrektes JSON-Dokument eingereicht, aber nichts oder nur Teile davon sind im Geräteschattendokument gespeichert. | Stellen Sie sicher, dass Sie die JSON-Form atierungsrichtlinien einhalten. Nur JSON-Feld er in den Abschnitten `desired` und `reported` werden gespeichert. JSON-Inhalte außerhalb dieser Abschnitte werden ignoriert (auch wenn sie formal korrekt sind). |
| Ich habe eine Fehlermeldung erhalten, dass mein Geräteschatten die zulässige Größe überschreitet. | Der Geräteschatten unterstützt nur 8 KB Daten. Versuchen Sie, Feldnamen in Ihrem JSON-Dokument zu kürzen, oder erstellen Sie einfach mehrere Schatten, indem Sie mehrere Objekte erstellen. Einem Gerät kann eine unbegrenz |

| Problem | Richtlinien für die Fehlerbehebung |
| --- | --- |
| | te Anzahl von Objekten/Schatten zugeordnet werden. Voraussetzung ist lediglich, dass der Name des Objekts in Ihrem Konto nur einmal verwendet werden darf. |
| Wenn ich einen Geräteschatten erhalte, ist er größer als 8 KB. Wie kann das sein? | Nach Erhalt fügt der AWS IoT Dienst dem Schatten des Geräts Metadaten hinzu. Der Service fügt diese Daten bei der Antwort hinzu, aber sie sind nicht in der Obergrenze von 8 KB enthalten. Nur die Daten für den Status `desired` und den Status `reported` des Statusdokuments, die an den Geräteschatten gesandt werden, werden für den Grenzwert berücksichtigt. |
| Meine Anfrage wurde aufgrund einer inkorrekten Version abgelehnt. Was soll ich tun? | Führen Sie einen GET-Vorgang durch, um auf die letzte Dokumentenversion zu synchronisieren. Wenn Sie MQTT verwenden, melden Sie sich beim Thema ./update/accepted an, um über Statusänderungen informiert zu werden und die neueste Version des JSON-Dokuments zu erhalten. |
| Der Zeitstempel ist um einige Sekunden ungenau. | Der Zeitstempel für einzelne Felder und das gesamte JSON-Dokument wird aktualisiert, wenn das Dokument beim AWS IoT Dienst eingeht oder wenn das Statusdokument auf dem veröffentlicht wird. /update/accepted and ./update/deltaNachricht. Nachrichten können im Netzwerk verspätet sein, sodass der Zeitstempel um einige Sekunden abweicht. |

| Problem | Richtlinien für die Fehlerbehebung |
| --- | --- |
| Ich kann mein Gerät in den entsprechenden Schattenthemen veröffentlichen und anmelden, aber wenn ich versuche, das Schattend okument über die HTTP-REST-API zu aktualisi eren, erhalte ich den Fehler HTTP 403. | Stellen Sie sicher, dass Sie in IAM Richtlini en erstellt haben, um den Zugriff auf diese Themen und auf die entsprechende Aktion (UPDATE/GET/DELETE) für die von Ihnen verwendeten Anmeldeinformationen zu ermöglichen. IAM-Richtlinien und Zertifika tsrichtlinien sind unabhängig. |
| Sonstige Probleme | Der Device Shadow-Dienst protokolliert Fehler in CloudWatch Logs. Um Geräte- und Konfigurationsprobleme zu identifizieren, aktivieren Sie CloudWatch Protokolle und sehen Sie sich die Protokolle mit Debug-Inf ormationen an. |

## Problemdiagnose bei Input-Stream-Aktionen für die Salesforce IoT

Helfen Sie uns, dieses Thema zu verbessern

Lassen Sie uns wissen, was dazu beitragen würde, es besser zu machen

### Ausführungsprotokoll

Wie kann ich das Ausführungsprotokoll einer Salesforce-Aktion anzeigen?

Siehe Abschnitt Überwachung AWS IoT mithilfe von Protokollen CloudWatch . Nachdem Sie die Protokolle aktiviert haben, können Sie die Ausführung der Salesforce-Aktion nachverfolgen.

## Erfolgreiche und fehlgeschlagene Aktionen

Wie kann ich prüfen, ob Nachrichten an einen Salesforce IoT-Eingabe-Stream gesendet werden konnten?

Sehen Sie sich die Protokolle an, die durch die Ausführung der Salesforce-Aktion generiert wurden, unter CloudWatch Protokolle. Wenn Sie das sehen`Action executed successfully`, bedeutet das, dass die AWS IoT Regel-Engine vom Salesforce IoT die Bestätigung erhalten hat, dass die Nachricht erfolgreich an den Zieleingabestream gesendet wurde.

Bei Problemen mit der Salesforce IoT-Plattform wenden Sie sich an den Salesforce IoT-Support.

Was kann ich tun, wenn Nachrichten nicht an einen Salesforce IoT-Eingabe-Stream gesendet werden konnten?

Sehen Sie sich die durch die Ausführung der Salesforce-Aktion generierten Protokolle unter CloudWatch Protokolle an. Je nach Protokolleintrag können Sie die folgenden Aktionen ausprobieren:

`Failed to locate the host`

Prüfen Sie, ob der Parameter `url` der Aktion korrekt angegeben wurde und der Salesforce IoT-Eingabe-Stream vorhanden ist.

`Received Internal Server Error from Salesforce`

Erneut versuchen. Wenn das Problem weiterhin besteht, wenden Sie sich an den Salesforce IoT-Support.

`Received Bad Request Exception from Salesforce`

Prüfen Sie die gesendete Nutzlast auf Fehler.

`Received Unsupported Media Type Exception from Salesforce`

Salesforce IoT unterstützt zurzeit keine binäre Nutzlast. Achten Sie darauf, nur JSON-Nutzlasten zu versenden.

`Received Unauthorized Exception from Salesforce`

Prüfen Sie, ob der Parameter `token` der Aktion korrekt angegeben wurde und das Token weiterhin gültig ist.

`Received Not Found Exception from Salesforce`

Prüfen Sie, ob der Parameter `url` der Aktion korrekt angegeben wurde und der Salesforce IoT-Eingabe-Stream vorhanden ist.

Wenn Sie einen Fehler erhalten, der hier nicht aufgeführt ist, wenden Sie sich an den AWS IoT Support.

## Diagnostizieren von Stream-Limits

Fehlerbehebung von „Stream-Begrenzung für Ihr AWS -Konto überschritten“

Wenn `"Error: You have exceeded the limit for the number of streams in your AWS account."` angezeigt wird, können Sie die nicht verwendeten Streams in Ihrem Konto bereinigen, anstatt eine Limiterhöhung anzufordern.

So bereinigen Sie einen ungenutzten Stream, den Sie mit dem SDK AWS CLI oder erstellt haben:

```
aws iot delete-stream –stream-id value
```

Weitere Informationen finden Sie unter delete-stream.

> **Note**
>
> Sie können den `list-streams` Befehl verwenden, um den Stream zu finden IDs.

## Behebung von Verbindungsabbrüchen bei Geräteflotten

> **Helfen Sie uns, dieses Thema zu verbessern**
>
> Lassen Sie uns wissen, was dazu beitragen würde, es besser zu machen

AWS IoT Verbindungsabbrüche bei Geräteflotten können aus verschiedenen Gründen auftreten. In diesem Artikel wird erklärt, wie Sie einen Grund für eine Unterbrechung diagnostizieren und wie Sie mit Verbindungsabbrüchen umgehen können, die durch regelmäßige Wartungsarbeiten oder ein AWS IoT Drosselungslimit verursacht werden.

Um den Grund für die Unterbrechung zu diagnostizieren

Sie können die AWSIotLogsV2-Protokollgruppe einchecken, CloudWatchum den Grund für die Unterbrechung im `disconnectReason` Feld des Protokolleintrags zu ermitteln.

Sie können auch die Funktion für AWS IoTLebenszyklusereignisse verwenden, um den Grund für die Unterbrechung der Verbindung zu ermitteln. Wenn Sie das Verbindungsabbruchereignis (`$aws/events/presence/disconnected/clientId`) von Lifecycle abonniert haben, erhalten Sie eine Benachrichtigung, AWS IoT sobald die Verbindung unterbrochen wird. Sie können den Grund für die Unterbrechung der Verbindung im `disconnectReason`-Feld der Benachrichtigung identifizieren.

Weitere Informationen finden Sie unter CloudWatch AWS IoT Protokolleinträge und Lifecycle-Ereignisse.

Zur Behebung von Verbindungsabbrüchen aufgrund von AWS IoT Wartungsarbeiten

Verbindungsunterbrechungen, die durch AWS IoT Wartungsarbeiten verursacht werden, werden als `SERVER_INITIATED_DISCONNECT` Lebenszyklusereignis und protokolliert. AWS IoT CloudWatch Um diese Verbindungsabbrüche zu beheben, passen Sie Ihre clientseitige Konfiguration so an, dass Ihre Geräte automatisch wieder mit der Plattform verbunden werden können. AWS IoT

Zur Behebung von Verbindungsabbrüchen aufgrund einer Drosselungsgrenze

Verbindungsabbrüche, die durch ein Drosselungslimit verursacht werden, werden als Lifecycle-Ereignis und protokolliert. `THROTTLED` AWS IoT CloudWatch Um diese Verbindungsabbrüche zu bewältigen, können Sie beantragen, dass das Message-Broker-Limit erhöht wird, wenn die Anzahl der Geräte zunimmt.

Weitere Informationen finden Sie unter AWS IoT Core Message Broker.

# AWS IoT Device Management Leitfaden zur Fehlerbehebung

> Helfen Sie uns, dieses Thema zu verbessern
>
> Lassen Sie uns wissen, was dazu beitragen würde, es besser zu machen

Dies ist der Abschnitt zur Fehlerbehebung für AWS IoT Device Management.

Themen


- AWS IoT Problembehebung bei Jobs
- Fehlerbehebung bei der Flottenindizierung
- AWS IoT Fehlerbehebung im Geräteverwaltungs-Softwarepaketkatalog


# AWS IoT Problembehebung bei Jobs

Dies ist der Abschnitt zur Fehlerbehebung für AWS IoT Jobs.

## Wie finde ich einen AWS IoT Jobs-Endpunkt?

Wie finde ich den Endpunkt der AWS IoT Jobs-Kontrollebene?

AWS IoT Jobs unterstützt API-Operationen auf Kontrollebene mithilfe des HTTPS-Protokolls. Stellen Sie sicher, dass Sie über das HTTPS-Protokoll eine Verbindung zum richtigen Endpunkt der Steuerebene hergestellt haben.

Eine Liste der AWS regionsspezifischen Endpunkte finden Sie unter AWS IoT Core — Endpoints der Steuerungsebene.

Eine Liste der FIPS-kompatiblen Endpunkte der AWS IoT -Auftragssteuerebene finden Sie unter FIPS-Endpunkte nach Dienst

> **Note**
>
> AWS IoT Jobs und AWS IoT Core teilen sich dieselben regionsspezifischen Endpunkte. AWS

Wie finde ich den Endpunkt der AWS IoT Jobs-Datenebene?

AWS IoT Jobs unterstützt API-Operationen auf Datenebene mithilfe der Protokolle HTTPS und MQTT. Stellen Sie sicher, dass Sie über das HTTPS- oder MQTT-Protokoll eine Verbindung zum richtigen Endpunkt der Datenebene hergestellt haben.

- Protokoll: HTTPS
  - Verwenden Sie den folgenden describe-endpoint-CLI-Befehl, der unten gezeigt wird, oder die `DescribeEndpoint`-REST-API. Verwenden Sie `iot:Jobs` für den Endpunkttyp.

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

- MQTT-Protokoll
  - Verwenden Sie den folgenden describe-endpoint-CLI-Befehl, der unten gezeigt wird, oder die `DescribeEndpoint`-REST-API. Verwenden Sie `iot:Data-ATS` für den Endpunkttyp.

    ```
    aws iot describe-endpoint --endpoint-type iot:Data-ATS
    ```

  Eine Liste der FIPS-kompatiblen AWS IoT Auftrags-Datenebenen-Endpunkte finden Sie unter FIPS-Endpunkte nach Dienst

## Wie überwache ich die AWS IoT Jobs-Aktivitäten und stelle Messwerte bereit?

Die Überwachung AWS IoT der Auftragsaktivitäten mithilfe von Amazon CloudWatch bietet Echtzeiteinblicke in den laufenden AWS IoT Auftragsbetrieb und hilft, die Kosten mithilfe von CloudWatch Alarmen mithilfe von AWS IoT Regeln zu kontrollieren. Sie müssen die Protokollierung konfigurieren, bevor Sie die AWS IoT Job-Aktivitäten überwachen und CloudWatch Alarme einrichten können. Weitere Informationen zum Einrichten der Protokollierung finden Sie unter Konfigurieren Sie die AWS IoT Protokollierung.

Weitere Informationen zu Amazon CloudWatch und zur Einrichtung von Berechtigungen über eine IAM-Benutzerrolle zur Nutzung von CloudWatch Ressourcen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon CloudWatch.

Wie richte ich AWS IoT Job-Metriken und Monitoring mit Amazon ein CloudWatch?

Um die AWS IoT Protokollierung einzurichten, folgen Sie den unter AWS IoT Protokollierung konfigurieren beschriebenen Schritten. AWS IoT Die Einrichtung der Protokollierung kann in der AWS Management Console AWS CLI, oder API erfolgen. AWS IoT Die Protokollierung, die für bestimmte Dinggruppen eingerichtet wurde, darf nur in der API AWS CLI oder erfolgen.

Der Abschnitt AWS IoT Job-Metriken enthält die AWS IoT Job-Metriken, die zur Überwachung der AWS IoT Jobs-Aktivität verwendet werden. Darin wird erklärt, wie die Metriken in den Feldern AWS Management Console und angezeigt AWS CLI werden.

Darüber hinaus können Sie CloudWatch Alarme einrichten, um Sie auf bestimmte Kennzahlen aufmerksam zu machen, die Sie genau überwachen möchten. Anleitungen zur Alarmeinrichtung finden Sie unter CloudWatch Amazon-Alarme verwenden.

## Problembehebung bei Geräteflotten und einzelnen Geräten

### Bei der Ausführung eines Auftrags wird der Status von **QUEUED** auf unbestimmte Zeit beibehalten

Wenn eine Auftragsausführung mit einem Status von `QUEUED` nicht zum nächsten logischen Status übergeht, z. B. `IN_PROGRESS`, `FAILED` oder `TIMED_OUT`, kann eines der folgenden Szenarien die Ursache sein:

- Überprüfen Sie Ihre Geräteaktivitäten in den CloudWatch Protokollen in der CloudWatch Konsole. Weitere Informationen finden Sie unter Überwachung AWS IoT mithilfe von CloudWatch Protokollen.
- Die IAM-Rolle, die dem Job und der nachfolgenden Auftragsausführung zugeordnet ist, verfügt möglicherweise nicht über die richtigen Berechtigungen, die in einer der Richtlinienerklärungen der IAM-Richtlinie aufgeführt sind, die dieser IAM-Rolle zugeordnet ist. Verwenden Sie die `describe-job`-API, um die IAM-Rolle zu identifizieren, die mit diesem Auftrag und der nachfolgenden Auftragsausführung verknüpft ist, und überprüfen Sie die IAM-Richtlinie auf die richtigen Berechtigungen. Sobald die Richtlinienberechtigungserklärungen aktualisiert wurden, sollten Sie in der Lage sein, den `AssumeRole`-API-Befehl für die Ressource auszuführen.

### Für mein Objekt oder meine Objektgruppe wurde keine Auftragsausführung erstellt

Wenn der Status eines Auftrags auf `IN_PROGRESS` aktualisiert wird, beginnt der Rollout des Auftragsdokuments auf allen Geräten in Ihrer Zielgruppe. Durch diese Statusaktualisierung wird für jedes Zielgerät eine Auftragsausführung erstellt. Wenn für eines der Zielgeräte keine Auftragsausführung erstellt wurde, lesen Sie die folgenden Anleitungen:

- Wirkt sich der Auftrag direkt auf `thing` aus, hat der Auftrag den Status `IN_PROGRESS`, und läuft der Auftrag gleichzeitig? Wenn alle drei Bedingungen erfüllt sind, sendet der Auftrag immer noch Auftragsausführungen an alle Geräte in Ihrer Zielgruppe, und für dieses spezielle Gerät `thing` wurde der Auftrag noch nicht ausgeführt.
  - Überprüfen Sie die Geräte in Ihrer Zielgruppe für den Job und den Status des Jobs in der AWS Management Console oder verwenden Sie den `describe-job`API-Befehl.
  - Verwenden Sie den `describe-job`-API-Befehl, um zu überprüfen, ob die `IsConcurrent`-Eigenschaft für den Auftrag auf „Wahr“ oder „Falsch“ festgelegt ist. Weitere Informationen finden Sie unter Auftragslimits.
- Der Auftrag zielt nicht direkt auf `thing` ab.
  - Wenn `Thing` zu einem `ThingGroup` hinzugefügt wurde und der Auftrag auf `ThingGroup` abzielte, überprüfen Sie, ob `Thing` Teil von `ThingGroup` ist.

- Handelt es sich bei dem Auftrag um einen Snapshot-Auftrag mit dem Status `IN_PROGRESS` der gleichzeitig läuft, sendet der Auftrag weiterhin Auftragsausführungen an alle Geräte in Ihrer Zielgruppe, und dieser spezifische `Thing` hat seine Auftragsausführung noch nicht erhalten.
- Wenn es sich bei dem Auftrag um einen kontinuierlichen gleichzeitigen Auftrag mit dem Status `IN_PROGRESS` handelt, sendet der Auftrag immer noch Auftragsausführungen an alle Geräte in Ihrer Zielgruppe, und dieser spezifische `Thing` hat seine Auftragsausführung noch nicht erhalten. Nur für fortlaufende Aufträge können Sie den `Thing` aus dem `ThingGroup` entfernen und dann den `Thing` wieder dem `ThingGroup` hinzufügen.
- Handelt es sich bei dem Job um einen Snapshot-Job mit dem Statusstatus `IN_PROGRESS` und ist er nicht gleichzeitig, dann ist es wahrscheinlich, dass die `Thing` oder die `ThingGroup` Mitgliedschaftsbeziehung von AWS IoT Jobs nicht bestätigt wurde. Es wird empfohlen, nach Ihrem `AddThingToThingGroup` Anruf mehrere Sekunden Wartezeit einzuplanen, bevor Sie Ihren Anruf erstellen. `Job` Alternativ können Sie die Zielauswahl auf ändern`Continuous`, sodass der Dienst das verzögerte Ereignis `Thing` und die `ThingGroup` Mitgliedschaft automatisch auffüllt.

Ein neuer Auftrag schlägt aufgrund eines **`LimitedExceededException`**-Fehlers fehl

Wenn Ihre Auftragserstellung mit der Fehlerantwort von `LimitedExceededException` fehlschlägt, rufen Sie die `list-jobs`-API auf und überprüfen Sie alle Aufträge mit `isConcurrent=true`, um festzustellen, ob Sie das Limit für die gleichzeitige Ausführung von Aufträgen erreicht haben. Weitere Informationen zu gleichzeitigen Aufträgen finden Sie unter Auftragslimits. Um Ihre Limits für die gleichzeitige Ausführung von Aufträgen zu sehen und eine Erhöhung des Limits zu beantragen, gehen Sie zu AWS IoT Device Management Auftragslimits und -kontingente.

Begrenzung der Dokumentgröße

Die Größe des Auftragsdokuments ist durch die Größe der MQTT-Payload begrenzt. Wenn Sie ein Auftragsdokument benötigen, das größer als 32 kB (Kilobyte), 32.000 B (Byte) ist, erstellen und speichern Sie das Auftragsdokument in Amazon S3 und fügen Sie eine Amazon S3-Objekt-URL in das `documentSource`-Feld für die `CreateJob`-API ein oder verwenden Sie AWS CLI. Fügen Sie für die AWS Management Console eine Amazon S3 S3-Objekt-URL in das Textfeld Amazon S3 S3-URL ein, wenn Sie einen Job erstellen.

- AWS Management Console Job-Dokumentation erstellen: Erstellen und verwalten Sie Jobs mithilfe der AWS Management Console
- AWS CLI Jobdokumentation erstellen: Erstellen und verwalten Sie Jobs mit dem AWS CLI
- `CreateJob`API-Dokumentation: CreateJob

### Geräteseitige MQTT-Nachrichtenanfragen - Drosselungsgrenzwerte

Wenn Sie den Fehlercode 400 `ThrottlingException` erhalten, ist die geräteseitige MQTT-Nachricht fehlgeschlagen, da das Limit für gleichzeitige geräteseitige Anfragen erreicht wurde. Unter AWS IoT Device Management -Limits und Kontingente für Aufträge finden Sie weitere Informationen zu den Limits für Aufträge und darüber, ob diese einstellbar sind.

### Verbindungstimeoutfehler

Ein Fehlercode 400 `RequestExpired` weist auf einen Verbindungsfehler hin, der auf eine hohe Latenz oder niedrige clientseitige Timeout-Werte zurückzuführen ist.

- Informationen zum Testen der Verbindung zwischen der Client- und der Serverseite finden Sie unter Testen der Konnektivität mit Ihrem Gerätedatenendpunkt.

### Ungültiger API-Befehl

Vergewissern Sie sich, dass der richtige API-Befehl eingegeben wurde, um zu vermeiden, dass die Fehlermeldung angezeigt wird, dass der API-Befehl ungültig ist. In der AWS IoT API-Referenz finden Sie eine umfassende Liste aller AWS IoT -API-Befehle.

### Verbindungsfehler auf der Serviceseite

Ein Fehlercode 503 `ServiceUnavailable` gibt an, dass der Fehler auf der Serverseite auftrat.

- Den aktuellen Status aller AWS Dienste finden Sie unter AWS Health Dashboard (alle AWS Dienste).
- Unter AWS Health Dashboard (persönlich AWS-Konto) finden Sie den aktuellen Status Ihrer persönlichen Daten AWS-Konto.

# Fehlerbehebung bei der Flottenindizierung

## Fehlerbehebung bei Aggregationsabfragen für den Flottenindizierungsservice

Wenn bei Ihnen nicht übereinstimmende Typen auftreten, können Sie CloudWatch Logs verwenden, um das Problem zu beheben. CloudWatch Logs müssen aktiviert werden, bevor Logs vom Fleet Indexing Service geschrieben werden können. Weitere Informationen finden Sie unter Überwachung AWS IoT mithilfe von Protokollen CloudWatch .

Zur Durchführung von Aggregationsabfragen für nicht verwaltete Felder müssen Sie ein Feld angeben, das Sie in dem `customFields`-Argument definiert haben, das an `UpdateIndexingConfiguration` oder update-indexing-configuration übergeben wurde. Wenn der Feldwert nicht mit dem konfigurierten Felddatentyp übereinstimmt, wird dieser Wert beim Ausführen einer Aggregationsabfrage ignoriert.

Wenn ein Feld aufgrund eines nicht übereinstimmenden Typs nicht indexiert werden kann, sendet der Fleet Indexing Service ein Fehlerprotokoll an Logs. CloudWatch Das Fehlerprotokoll enthält den Feldnamen, den Wert, der nicht konvertiert werden konnte, und den Namen des Elements für das Gerät. Nachfolgend sehen Sie ein Beispiel für ein Fehlerprotokoll:

```
{
  "timestamp": "2017-02-20 20:31:22.932",
  "logLevel": "ERROR",
  "traceId": "79738924-1025-3a00-a669-7bec69f7f07a",
  "accountId": "000000000000",
  "status": "SucceededWithIssues",
  "eventType": "IndexingCustomFieldFailed",
  "thingName": "thing0",
  "failedCustomFields": [
    {
      "Name": "attributeName1",
      "Value": "apple",
      "ExpectedType": "String"
    },
    {
      "Name": "attributeName2",
      "Value": "2",
      "ExpectedType": "Boolean"
    }
  ]
}
```

Wenn ein Gerät etwa eine Stunde lang getrennt war, fehlt möglicherweise der `timestamp`-Wert des Konnektivitätsstatus. Bei persistenten Sitzungen fehlt der Wert möglicherweise, wenn die Verbindung zu einem Client länger als die für die persistente Sitzung konfigurierte Zeit time-to-live (TTL) unterbrochen wurde. Die Konnektivitätsstatusdaten werden nur für Verbindungen indiziert, bei denen die Client-ID einen übereinstimmenden Objektnamen hat. (Die Client-ID ist der Wert, mit dem ein Gerät verbunden wird.) AWS IoT Core

## Fehlerbehebung bei der Konfiguration der Flottenindizierung

Die Konfiguration der Flottenindizierung kann nicht herabgestuft werden

Das Herabstufen der Konfiguration für die Flottenindizierung wird nicht unterstützt, wenn Sie die Datenquellen entfernen möchten, die mit einer Flottenkennzahl oder einer dynamischen Gruppe verknüpft sind.

Wenn Ihre Indizierungskonfiguration beispielsweise Registrierungsdaten, Schattendaten und Konnektivitätsdaten enthält und die Flottenmetrik existiert mit der Abfrage `thingName:TempSensor* AND shadow.desired.temperature>80`, führt die Aktualisierung der Indizierungskonfiguration, sodass sie nur die Registrierungsdaten enthält, zu einem Fehler.

Das Ändern von benutzerdefinierten Feldern, die von vorhandenen Flottenkennzahlen verwendet werden, wird nicht unterstützt.

Ihre Indexkonfiguration kann aufgrund inkompatibler Flottenkennzahlen oder dynamischer Gruppen nicht aktualisiert werden

Wenn Sie Ihre Indexkonfiguration aufgrund inkompatibler Flottenkennzahlen oder dynamischer Gruppen nicht aktualisieren können, löschen Sie die inkompatiblen Flottenkennzahlen oder dynamischen Gruppen, bevor Sie die Indexkonfiguration aktualisieren.

## Problembehebung bei der Standortindizierung und bei Geoabfragen

Um Fehler mit nicht übereinstimmenden Typen bei der Standortindizierung und bei Geoabfragen zu beheben, können Sie Protokolle aktivieren. CloudWatch Weitere Informationen zur Überwachung der AWS IoT Nutzung finden Sie in der CloudWatch Anleitung. step-by-step

Wenn Sie Standortdaten mithilfe von Geoabfragen indizieren, müssen die Standortfelder, die Sie in `geoLocations` angeben, mit den Standortfeldern übereinstimmen, die Sie an `UpdateIndexingConfiguration` übergeben. Liegt eine Nichtübereinstimmung vor, sendet die Flottenindizierung einen Fehler mit nicht übereinstimmendem Typ an. CloudWatch Das

Fehlerprotokoll enthält den Feldnamen, den Wert, der nicht konvertiert werden konnte, und den Namen des Elements für das Gerät.

Nachfolgend sehen Sie ein Beispiel für ein Fehlerprotokoll:

```
{
"timestamp": "2023-11-09 01:39:43.466",
    "logLevel": "ERROR",
    "traceId": "79738924-1025-3a00-a669-7bec69f7f07a",
    "accountId": "123456789012",
    "status": "Failure",
    "eventType": "IndexingGeoLocationFieldFailed",
    "thingName": "thing0",
    "failedGeolocationFields": [
        {
"Name": "attributeName1",
            "Value": "apple",
            "ExpectedType": "Geopoint"
        }
    ],
    "reason": "failed to index the field because it could not be converted to one of
 the expected geoLocation formats."
}
```

Weitere Informationen finden Sie unter Indexierung von Standortdaten.

## Fehlerbehebung bei Flottenmetriken

### Ich kann keine Datenpunkte sehen in CloudWatch

Wenn Sie in der Lage sind, eine Flottenmetrik zu erstellen, aber keine Datenpunkte darin sehen können CloudWatch, ist es wahrscheinlich, dass Sie nichts haben, das die Kriterien der Abfragezeichenfolge erfüllt.

Sehen Sie sich diesen Beispielbefehl an, um eine Flottenmetrik zu erstellen:

```
aws iot create-fleet-metric --metric-name "example_FM" --query-string
 "thingName:TempSensor* AND attributes.temperature>80" --period 60 --aggregation-field
 "attributes.temperature" --aggregation-type name=Statistics,values=count
```

Wenn Sie nichts haben, das die Kriterien für die Abfragezeichenfolge `--query-string "thingName:TempSensor* AND attributes.temperature>80"` erfüllt:

- Mit werden Sie in der Lage sein`values=count`, eine Flottenmetrik zu erstellen, und es werden Datenpunkte angezeigt, die angezeigt werden können CloudWatch. Die Datenpunkte des Werts `count` sind immer 0.
- Mit „`values`other than`count`“ können Sie zwar eine Flottenkennzahl erstellen, aber die Flottenkennzahl wird nicht angezeigt CloudWatch und es werden keine Datenpunkte angezeigt CloudWatch.

# AWS IoT Fehlerbehebung im Geräteverwaltungs-Softwarepaketkatalog

Dies ist der Abschnitt zur Fehlerbehebung für den AWS IoT Geräteverwaltungs-Softwarepaketkatalog.

## Allgemeine Fehlermeldungen zur Fehlerbehebung

In diesem Abschnitt werden die häufigsten Fehler aufgeführt, die während des gesamten Lebenszyklus der Softwarepaketversionen auftreten.

**`HeadBucket`**-Fehler

Die folgenden Fehlermeldungen werden angezeigt, wenn Sie den `HeadBucket`API-Vorgang oder den `head-bucket`CLI-Befehl aufrufen, um den Amazon S3 S3-Bucket zu validieren, der für den Datei-Upload während einer Jobbereitstellung verwendet wurde.

Weitere Informationen zur Verwendung eines Amazon S3 S3-Buckets zum Hochladen von Dateien während einer Auftragsbereitstellung finden Sie unterVorsignierte URL für den Datei-Upload.

```
InvalidRoleException
    "Permission denied when attempting to use role %s to access bucket %s."
```

```
InvalidRequestException
    "Cross region S3 bucket is not supported for presigned url upload placeholder"
```

```
InvalidRequestException
    "S3 bucket in job document presigned url upload placeholder not found"
```

```
InvalidRequestException
    "Given S3 bucket name is invalid."
```

```
InvalidRequestException
    "Provided S3 bucket is not valid: %s. Error: %s"
```

Amazon S3 GetObject

Die folgende Fehlermeldung tritt auf, wenn ein ungültiges Argument angegeben wird, was dazu führt, dass der Amazon S3 `GetObject` S3-API-Vorgang fehlschlägt.

```
InvalidRequestException
    "Provided argument for presigned url is invalid"
```

Support Amazon S3 S3-Versions-ID

Wenn Sie mithilfe der Versionskontrolle Zugriff auf einen Amazon S3 S3-Bucket anfordern, stellen Sie sicher, dass Sie Ihren Namen angeben, `versionId` da sonst der folgende Fehler angezeigt werden kann.

Weitere Informationen zu Amazon S3 S3-Buckets, die Versionskontrolle verwenden, finden Sie unter Verwenden der Versionierung in Amazon S3 S3-Buckets

```
InvalidRequestException
    "VersionId not found when attempting to access s3 url"
```

Platzhalter innerhalb einer vorsignierten URL für den Datei-Upload

Die folgenden Fehlermeldungen werden angezeigt, wenn während einer Auftragsbereitstellung Probleme mit einem Platzhalter innerhalb einer vorsignierten URL auftreten, die zum Hochladen von Dateien in einen Amazon S3 S3-Ziel-Bucket verwendet wird. Weitere Informationen zur Verwendung eines Amazon S3 S3-Buckets zum Hochladen von Dateien während einer Auftragsbereitstellung und darüber, was ein lokaler Platzhalter ist, finden Sie unter. Vorsignierte URL für den Datei-Upload

Die folgende Fehlermeldung wird angezeigt, wenn der lokale Platzhalter nicht erkannt wird.

```
InvalidJobDocumentException
    "Undefined placeholder, ${...}, inside of presign url upload parameter"
```

Die folgende Fehlermeldung wird angezeigt, wenn versucht wird, den lokalen Platzhalter in einer vorsignierten URL zu verwenden, die nicht für das Hochladen von Dateien vorgesehen ist.

```
InvalidJobDocumentException
```

```
    "Local placeholder, ${...}, is only valid inside of presign url upload"
```

Amazon S3 S3-URL falsch verschachtelt

Die folgende Fehlermeldung wird angezeigt, wenn die Amazon S3 S3-URL falsch in einem anderen Platzhalter verschachtelt ist.

```
InvalidJobDocumentException
    "${aws:%s[...]} should not be the second layer pattern."
```

Paketversion Artifact Nesting

Die folgende Fehlermeldung wird angezeigt, wenn die vorsignierte URL des Artefakts der Paketversion fälschlicherweise in einem anderen Platzhalter verschachtelt ist.

```
InvalidJobDocumentException
    "${aws:iot:package:[...]:artifact:s3-presigned-url} cannot be nested inside another
 placeholder."
```

Artifact der fehlenden Paketversion

Die folgende Fehlermeldung wird angezeigt, wenn das Artefakt der Paketversion, auf das verwiesen wird, nicht gefunden wird.

```
InvalidJobDocumentException
    "Package %s version %s does not have an associated artifact to generate an S3
 presigned url."
```

Platzhalter für Softwarepakete und Paketversionen

Die folgende Fehlermeldung wird angezeigt, wenn der Platzhalter für das Jobdokument für das Softwarepaket und die Paketversion nicht in die gewünschten gültigen Werte für die Auftragsbereitstellung aufgelöst werden kann, da auf mehrere Softwarepakete und Paketversionen verwiesen wird, auf die im `destinationPackageVersions` Parameter oder auf der Registerkarte Versions-ARN auf der Seite mit den Paketversionsdetails verwiesen wird.

```
InvalidJobDocumentException
    "Cannot resolve empty package name and version name given multiple elements in
 destination package versions."
```

Leeres Softwarepaket und Paketversion verwenden

Die folgende Fehlermeldung wird angezeigt, wenn Sie versuchen, ein leeres Paket oder eine leere Paketversion ohne die andere Version in einem Jobdokument zu verwenden.

```
InvalidJobDocumentException
    "Empty package name and version name have to be used in pair."
```

Null-Verwendung im Jobdokument

Die folgende Fehlermeldung wird angezeigt, wenn Sie versuchen, eine Paketversion im Jobdokument anzugeben`$null`. `$null`kann nur innerhalb des `destinationPackageVersions` Parameters verwendet werden, wenn die `CreateJob` API-Operation verwendet wird.

```
InvalidJobDocumentException
    "$null is not allowed to be referenced as a package version in job documents."
```

Alle Attribute in einer Paketversion

Die folgende Fehlermeldung wird angezeigt, wenn Sie versuchen, alle Attribute in einer Paketversion zu verwenden und diese mit zusätzlichem Text oder Platzhaltern zu umgeben.

Weitere Informationen zur Verwendung aller Attribute in einer Softwarepaketversion finden Sie unter Ersetzungsparameter für Jobs AWS IoT

```
InvalidJobDocumentException
    "The package version attribute placeholder for all attributes has to be a
 json value by itself and not appended with other strings or nested with other
 placeholders."
```

Lokales Platzhalterlimit in der vorsignierten URL für den Datei-Upload

Die folgende Fehlermeldung wird angezeigt, wenn Sie das Limit für die Anzahl der lokalen Platzhalter überschreiten, die in einer vorsignierten URL für das Hochladen von Dateien während einer Auftragsbereitstellung verwendet werden.

Weitere Informationen zur Verwendung einer vorsignierten URL für das Hochladen von Dateien während einer Stellenbereitstellung finden Sie unter Vorsignierte URL für den Datei-Upload

```
InvalidJobDocumentException
    "The occurrence of local placeholder %s within S3 presigned url upload placeholder
 exceeds limit of %d."
```

Lokale Platzhalter in einem Amazon S3 S3-Bucket

Die folgende Fehlermeldung wird angezeigt, wenn Sie versuchen, eine lokale Platzhalter-URL im Amazon S3 S3-Bucket-Namen für einen vorsignierten URL-Platzhalter zu platzieren, der für den Datei-Upload während einer Jobbereitstellung verwendet wird.

Weitere Informationen zur Verwendung einer vorsignierten URL für den Datei-Upload während einer Jobbereitstellung finden Sie unter Vorsignierte URL für den Datei-Upload

```
InvalidJobDocumentException
    "S3 bucket name in presigned url upload is not allowed to contain any placeholders"
```

Klammern öffnen und schließen

Die folgende Fehlermeldung wird angezeigt, wenn Sie einem Jobdokument einen Parameter oder Platzhalter ohne schließende Klammer „}“ hinzufügen.

```
InvalidJobDocumentException
    "One or more parameters or placeholders are not terminated."
```

IAM-Rolle mit vorsignierter Amazon S3 S3-URL

Die folgende Fehlermeldung wird angezeigt, wenn Sie versuchen, eine vorsignierte Amazon S3 S3-URL in einem Jobdokument ohne IAM-Rolle zu verwenden.

Weitere Informationen zu Amazon S3 Presigned URLs finden Sie unter Working with URLs presigned.

```
InvalidRequestException
    "presignedUrlConfig role ARN is required to generate an S3 presigned url in job
 document."
```

IAM-Rolle mit vorsignierter Amazon S3 S3-URL für Package Version Artifact

Die folgende Fehlermeldung wird angezeigt, wenn Sie versuchen, eine vorsignierte Amazon S3 S3-URL zu verwenden, die ein Paketversionsartefakt in einem Auftragsdokument ohne IAM-Rolle darstellt.

```
InvalidRequestException
    "presignedUrlConfig role ARN is required to generate an S3 presigned url in job
 document for package %s version %s artifact."
```

## Fehlermeldungen zur Stückliste der Software

In diesem Abschnitt werden häufig auftretende Fehler im Zusammenhang mit einer Softwareliste (SBOM) aufgeführt, die mit einer Paketversion verknüpft ist.

Eingabevalidierung für die SBOM-Zuordnungsanfrage

Die folgende Fehlermeldung wird angezeigt, wenn der `AssociateSbomWithPackageVersion` API-Vorgang verwendet wird und der `s3Location` Parameter Null ist.

```
InvalidRequestException "Associate request needs to include SBOM reference"
```

Weitere Informationen zum `AssociateSbomWithPackageVersion` API-Vorgang finden Sie unter AssociateSbomWithPackageVersion.

Fehler bei der SBOM-Validierung

In diesem Abschnitt werden die häufigsten Fehler aufgeführt, die bei der ersten Validierung der Softwareliste (SBOM) aufgetreten sind, wenn sie mit einer Softwarepaketversion verknüpft ist.

Die folgende Fehlermeldung wird angezeigt, wenn der `AssociateSbomWithPackageVersion` API-Vorgang verwendet wird und der Parameter `bucket` Null ists`3Location`.

```
InvalidRequestException "S3 bucket name for SBOM cannot be null"
```

Die folgende Fehlermeldung wird angezeigt, wenn die Zeichenfolge `bucket` im `s3Location` Parameter für den `AssociateSbomWithPackageVersion` API-Vorgang zu lang ist.

```
InvalidRequestException "S3 bucket name for SBOM is illegal. String length exceeds
 limit"
```

Die folgende Fehlermeldung wird angezeigt, wenn der `key` Parameter Null ist.

```
InvalidRequestException "S3 key name for SBOM cannot be null"
```

Die folgende Fehlermeldung wird angezeigt, wenn die Zeichenfolge `key` im `s3Location` Parameter für den `AssociateSbomWithPackageVersion` API-Vorgang zu lang ist.

```
InvalidRequestException "S3 key name for SBOM is illegal. String length exceeds limit"
```

Die folgende Fehlermeldung wird angezeigt, wenn die Zeichenfolge `version` im `s3Location` Parameter für den `AssociateSbomWithPackageVersion` API-Vorgang Null ist.

```
InvalidRequestException "S3 object version for SBOM cannot be null"
```

Die folgende Fehlermeldung wird angezeigt, wenn die Zeichenfolge `version` im `s3Location` Parameter für den `AssociateSbomWithPackageVersion` API-Vorgang zu lang ist.

```
InvalidRequestException "S3 object version for SBOM is illegal. String length exceeds
 limit"
```

Die folgende Fehlermeldung wird angezeigt, wenn die Größe der im Amazon S3-Bucket gespeicherten SBOM-Zip-Archivdatei zu groß ist.

```
InvalidRequestException "S3 object file size exceeds limit"
```

Die folgende Fehlermeldung wird angezeigt, wenn Sie den `AssociateSbomWithPackageVersion` API-Vorgang verwenden und die aktuelle Anzahl der laufenden SBOM-Validierungen bereits den Höchstwert erreicht hat.

```
LimitExceededException "Too many ongoing SBOM validation workflows. Please wait and
 retry"
```

Zugriffsprobleme mit der SBOM-Datei im Amazon S3 S3-Bucket

Die folgende Fehlermeldung wird angezeigt, wenn eine andere Entität nicht auf den Amazon S3 S3-Bucket zugreifen kann, weil der Amazon S3 S3-Bucket nicht existiert oder die richtigen Berechtigungen für den Zugriff auf den Amazon S3 S3-Bucket nicht erteilt wurden.

Weitere Informationen zu den erforderlichen Berechtigungsrichtlinien für den Zugriff auf den Amazon S3 S3-Bucket finden Sie unterAufbewahrung von Softwarelisten.

```
InvalidRequestException "SBOM not accessible by the service. Please make sure the
 bucket exists and S3 permission is granted."
```

Die folgende Fehlermeldung wird angezeigt, wenn eine andere Entität nicht auf die SBOM-Zip-Archivdatei im `key` Parameter zugreifen kann, weil der Amazon S3 S3-Bucket nicht existiert oder die richtigen Berechtigungen für den Zugriff auf im Amazon S3 S3-Bucket gespeicherte Inhalte nicht erteilt wurden.

```
InvalidRequestException "SBOM not accessible by the service. Please make sure the key
 exists and S3 permission is granted."
```

Die folgende Fehlermeldung wird angezeigt, wenn eine andere Entität nicht auf den Amazon S3 S3-Bucket zugreifen kann, weil der Bucket, der Schlüssel und die Versions-ID nicht existieren oder die richtigen Berechtigungen für den Zugriff auf den Amazon S3 S3-Bucket nicht erteilt wurden. Darüber hinaus kann diese Fehlermeldung angezeigt werden, wenn die erteilten Berechtigungen nicht ausreichen, um auf die SBOM-Zip-Archivdatei im Amazon S3-Bucket zuzugreifen.

```
InvalidRequestException "SBOM not accessible by the service. Please make sure the
 bucket/key/version exists and S3 permission is granted."
```

Die folgende Fehlermeldung wird angezeigt, wenn eine andere Entität nicht auf den Amazon S3 S3-Bucket zugreifen kann, weil sich der Bucket in einer anderen Region befindet.

```
InvalidRequestException "Cross-region S3 bucket for %s is not supported."
```

Die folgende Fehlermeldung wird angezeigt, wenn eine andere Entität nicht auf den Amazon S3 S3-Bucket zugreifen kann`bucket`, weil die `version` Parameter`key`, oder bei der Verwendung des `AssociateSbomWithPackageVersion` API-Vorgangs falsch geschrieben wurden.

```
InvalidRequestException "Please make sure SBOM S3 bucket name/key length/version is
 valid"
```

# AWS IoT Leitfaden zur Fehlerbehebung in Device Advisor

> Helfen Sie uns, dieses Thema zu verbessern
>
> Lassen Sie uns wissen, was dazu beitragen würde, es besser zu machen

Allgemeines

F: Kann ich mehrere Testsuiten parallel ausführen?

A: Ja. Device Advisor unterstützt jetzt die Ausführung mehrerer Testsuiten auf verschiedenen Geräten mithilfe eines Endpunkts auf Geräteebene. Wenn Sie den Endpunkt auf Kontoebene

verwenden, können Sie jeweils eine Suite ausführen, da pro Konto ein Device Advisor-Endpunkt verfügbar ist. Weitere Informationen finden Sie unter Konfigurieren Ihres Geräts.

F: Ich habe von meinem Gerät aus gesehen, dass die TLS-Verbindung von Device Advisor verweigert wurde. Ist das normal?

A: Ja. Device Advisor verweigert die TLS-Verbindung vor und nach jedem Testlauf. Wir empfehlen Benutzern, einen Mechanismus zur Gerätewiederholung zu implementieren, um ein vollautomatisches Testerlebnis mit Device Advisor zu gewährleisten. Wenn Sie eine Testsuite mit mehr als einem Testfall ausführen, zum Beispiel TLS Connect, MQTT Connect und MQTT Publish, dann empfehlen wir, dass Sie einen Mechanismus für Ihr Gerät entwickeln lassen. Der Mechanismus kann versuchen, alle 5 Sekunden für ein bis zwei Minuten eine Verbindung zu unserem Testendpunkt herzustellen. Auf diese Weise können Sie mehrere Testfälle nacheinander automatisiert ausführen.

Kann ich für Sicherheitsanalysen und zu Fehlerbehebungszwecken einen Verlauf der API-Aufrufe abrufen, die von der Device Advisor API in meinem Konto gesendet wurden?

A: Ja. Um einen Verlauf der Device Advisor-API-Aufrufe zu erhalten, die für Ihr Konto getätigt wurden, schalten Sie die Option einfach CloudTrail in der AWS IoT Management Console ein und filtern Sie die Ereignisquelle nach`iotdeviceadvisor.amazonaws.com`.

F: Wie kann ich mir die Device Advisor-Anmeldungen ansehen CloudWatch?

A: Protokolle, die während einer Testsuite-Ausführung generiert wurden, werden hochgeladen, CloudWatch wenn Sie die erforderliche Richtlinie (z. B. CloudWatchFullAccess) zu Ihrer Servicerolle hinzufügen (sieheEinrichtung). Wenn die Testsuite mindestens einen Testfall enthält, wird eine Protokollgruppe "aws/iot/deviceadvisor/$testSuiteId" mit zwei Protokollströmen erstellt. Ein Stream ist „$testRunId“ und enthält Protokolle von Aktionen, die vor und nach der Ausführung der Testfälle in Ihrer Testsuite ausgeführt wurden, z. B. Einrichtungs- und Bereinigungsschritte. Der andere Protokollstream ist „$ suiteRunId _$“testRunId, der spezifisch für die Ausführung einer Testsuite ist. Ereignisse, die von Geräten gesendet AWS IoT Core werden und in diesem Protokollstream protokolliert werden.

F: Was ist der Zweck der Geräteberechtigungsrolle?

A: Device Advisor steht zwischen Ihrem Testgerät und dient AWS IoT Core zur Simulation von Testszenarien. Er akzeptiert Verbindungen und Nachrichten von Ihren Testgeräten und leitet sie weiter an AWS IoT Core , indem er Ihre Geräteberechtigungsrolle übernimmt und in Ihrem Namen eine Verbindung initiiert. Es ist wichtig, sicherzustellen, dass die Berechtigungen für die Geräterolle mit denen auf dem Zertifikat übereinstimmen, das Sie für die Ausführung

von Tests verwenden. AWS IoT Zertifikatsrichtlinien werden nicht durchgesetzt, wenn Device Advisor in AWS IoT Core Ihrem Namen mithilfe der Geräteberechtigungsrolle eine Verbindung zu initiiert. Die Berechtigungen der von Ihnen festgelegten Geräteberechtigungsrolle werden jedoch durchgesetzt.

F: In welchen Regionen wird Device Advisor unterstützt?

A: Device Advisor wird in den Regionen us-east-1, us-west-2, ap-northeast-1 und eu-west-1 unterstützt.

F: Warum sehe ich inkonsistente Ergebnisse?

A: Eine der Hauptursachen für inkonsistente Ergebnisse ist die Einstellung von `EXECUTION_TIMEOUT` eines Tests auf einen zu niedrigen Wert. Weitere Informationen zu empfohlenen und standardmäßigen `EXECUTION_TIMEOUT`-Werten finden Sie unter Device Advisor-Testfälle.

F: Welches MQTT-Protokoll unterstützt Device Advisor?

A: Device Advisor unterstützt MQTT Version 3.1.1 mit X509-Client-Zertifikaten.

F: Was ist, wenn mein Testfall mit einer Meldung über das Ausführungszeitlimit fehlschlägt, obwohl ich versucht habe, mein Gerät mit dem Testendpunkt zu verbinden?

A: Überprüfen Sie alle Schritte unter Erstellen Sie eine IAM-Rolle, die als Ihre Geräterolle verwendet werden soll. Wenn der Test immer noch fehlschlägt, sendet das Gerät möglicherweise nicht die richtige SNI-Erweiterung (Server Name Indication), die erforderlich ist, damit Device Advisor funktioniert. Der richtige SNI-Wert ist die Endpunktadresse, die zurückgegeben wird, wenn Sie dem Abschnitt Gerät konfigurieren folgen. AWS IoT erfordert außerdem, dass Geräte die Server Name Indication (SNI) -Erweiterung an das Transport Layer Security (TLS) -Protokoll senden. Weitere Informationen finden Sie unter Transportsicherheit in AWS IoT.

F: Meine MQTT-Verbindung schlägt mit dem Fehler "libaws-c-mqtt: AWS_ERROR _MQTT_UNEXPECTED_HANGUP“ fehl (oder) die MQTT-Verbindung meines Geräts wird automatisch vom Device Advisor-Endpunkt getrennt. Wie kann dieser Fehler behoben werden?

A: Dieser spezielle Fehlercode und unerwartete Verbindungsabbrüche können viele verschiedene Ursachen haben, hängen aber höchstwahrscheinlich mit der dem Gerät zugewiesenen Geräterolle zusammen. Die folgenden Prüfpunkte (in der Reihenfolge ihrer Priorität) lösen dieses Problem.

- Die dem Gerät zugeordnete Geräterolle muss über die IAM-Mindestrechte verfügen, die für die Ausführung der Tests erforderlich sind. Device Advisor verwendet die angefügte

Geräterolle, um AWS IoT -MQTT-Aktionen im Namen des Testgeräts durchzuführen. Wenn die erforderlichen Berechtigungen nicht vorhanden sind, wird der Fehler `AWS_ERROR_MQTT_UNEXPECTED_HANGUP` angezeigt oder es kommt zu unerwarteten Verbindungsabbrüchen, während das Gerät versucht, eine Verbindung zum Device Advisor-Endpunkt herzustellen. Wenn Sie sich beispielsweise dafür entschieden haben, den Testfall MQTT Publish auszuführen, müssen die Aktionen Connect und Publish in der Rolle mit dem entsprechenden ClientId Thema enthalten sein (Sie können mehrere Werte angeben, indem Sie die Werte durch Kommas trennen, und Sie können Präfixwerte mit einem Platzhalterzeichen (*) angeben. Beispiel: Um Berechtigungen zur Veröffentlichung für ein beliebiges Thema zu erteilen, das mit `TestTopic` beginnt, können Sie „`TestTopic*`“ als Ressourcenwert angeben. Hier sind einige Beispiele für Richtlinien.

- Nichtübereinstimmung zwischen den in der Geräterolle für Ihre Ressourcentypen definierten Werten und den tatsächlich im Code verwendeten Werten. Zum Beispiel: Eine Diskrepanz zwischen der ClientId Definition in der Rolle und der tatsächlich ClientId verwendeten Rolle in Ihrem Gerätecode. Werte wie ClientId, Thema und TopicFilter müssen in der Geräterolle und im Code identisch sein.
- Das an Ihr Gerät angehängte Gerätezertifikat muss aktiv sein und mit einer Richtlinie versehen sein, die die erforderlichen Aktionsberechtigungen für Ressourcen enthält. Beachten Sie, dass die Richtlinie für Gerätezertifikate den Zugriff auf AWS IoT Ressourcen und AWS IoT Core Datenebenenoperationen gewährt oder verweigert. Device Advisor setzt voraus, dass Sie ein aktives Gerätezertifikat an Ihr Gerät angeschlossen haben, das die während eines Testfalls verwendeten Aktionsberechtigungen gewährt.

# AWS IoT Fehler

> Helfen Sie uns, dieses Thema zu verbessern
>
> Lassen Sie uns wissen, was dazu beitragen würde, es besser zu machen

In diesem Abschnitt sind die Fehlercodes aufgeführt, die von gesendet wurden AWS IoT.

Fehlercodes für Message Broker

| Fehlercode | Fehlerbeschreibung |
| --- | --- |
| 400 | Inkorrekte Anfrage |

| Fehlercode | Fehlerbeschreibung |
| --- | --- |
| 401 | Nicht autorisiert |
| 403 | Verboten. |
| 426 | Upgrade erforderlich. |
| 503 | Service nicht verfügbar |

### Identitäts- und Sicherheitsfehlercodes

| Fehlercode | Fehlerbeschreibung |
| --- | --- |
| 401 | Nicht autorisiert |

### Geräteschatten-Fehlercodes

| Fehlercode | Fehlerbeschreibung |
| --- | --- |
| 400 | Inkorrekte Anfrage |
| 401 | Nicht autorisiert |
| 403 | Verboten. |
| 404 | Nicht gefunden |
| 409 | Konflikt |
| 413 | Anfrage zu lang |
| 422 | Anfrage konnte nicht verarbeitet werden |
| 429 | Zu viele Anfragen |
| 500 | Interner Fehler |
| 503 | Service nicht verfügbar |

# AWS IoT Geräte SDKs - SDKs, Mobil- und AWS IoT Geräteclient

Diese Seite fasst AWS IoT Geräte SDKs, Open-Source-Bibliotheken, Entwicklerhandbücher, Beispiel-Apps und Portierungsleitfäden zusammen, um Sie bei der Entwicklung innovativer IoT-Lösungen mit Hardwareplattformen AWS IoT und Ihrer Wahl zu unterstützen.

Diese SDKs sind für die Verwendung auf Ihrem IoT-Gerät vorgesehen. Wenn Sie eine IoT-App für die Verwendung auf einem Mobilgerät entwickeln, finden Sie weitere Informationen unter AWS Mobil SDKs. Wenn Sie eine IoT-App oder ein serverseitiges Programm entwickeln, finden Sie weitere Informationen unter AWS SDKs.

## AWS IoT Gerät SDKs

Das AWS IoT Gerät SDKs umfasst Open-Source-Bibliotheken, Entwicklerhandbücher mit Beispielen und Portierungsleitfäden, sodass Sie innovative IoT-Produkte oder -Lösungen auf den Hardwareplattformen Ihrer Wahl entwickeln können.

> **Note**
>
> The AWS IoT Device SDKs hat einen MQTT 5-Client veröffentlicht. Das AWS IoT Gerät unterstützt die Verwendung von TLS 1.3 auf macOS SDKs nicht.

Diese SDKs helfen Ihnen dabei, Ihre IoT-Geräte AWS IoT mit den Protokollen MQTT und WSS zu verbinden.

C++

AWS IoT C++-Geräte-SDK

Das AWS IoT C++-Geräte-SDK ermöglicht es Entwicklern, verbundene Anwendungen mithilfe von AWS und zu erstellen AWS IoT APIs. Dieses SDK wurde speziell für Geräte entwickelt, die nicht ressourcenbeschränkt sind und die erweiterte Funktionen benötigen, wie beispielsweise Nachrichtenwarteschlangen, Multithreading-Support und die aktuellen Sprachfunktionen. Weitere Informationen finden Sie hier:

- AWS IoT Geräte-SDK C++ v2 aktiviert GitHub

- AWS IoT Readme für das Geräte-SDK C++ v2
- AWS IoT C++ v2-Beispiele für das Geräte-SDK
- AWS IoT C++ v2-API-Dokumentation für das Geräte-SDK

Python

AWS IoT Geräte-SDK für Python

Das AWS IoT Device SDK für Python ermöglicht es Entwicklern, Python-Skripte zu schreiben, um ihre Geräte für den Zugriff auf die AWS IoT Plattform über MQTT oder MQTT über das WebSocket Protokoll zu verwenden. Durch die Verbindung ihrer Geräte mit können Benutzer sicher mit dem Message Broker, den Regeln und Schatten arbeiten, die von AWS IoT und mit anderen AWS Diensten wie AWS Lambda Kinesis und Amazon S3 und mehr bereitgestellt werden. AWS IoT

- AWS IoT Geräte-SDK für Python v2 auf GitHub
- AWS IoT Readme zum Geräte-SDK für Python v2
- AWS IoT Geräte-SDK für Python v2-Beispiele
- AWS IoT API-Dokumentation zum Geräte-SDK für Python v2

JavaScript

AWS IoT Geräte-SDK für JavaScript

Das aws-iot-device-sdk .js-Paket ermöglicht es Entwicklern, JavaScript Anwendungen zu schreiben, die AWS IoT mithilfe von MQTT oder MQTT über das WebSocket Protokoll darauf zugreifen. Das Paket kann in Node.js-Umgebungen und Browser-Anwendungen verwendet werden. Weitere Informationen finden Sie hier:

- AWS IoT Geräte-SDK für Version 2 aktiviert JavaScript GitHub
- AWS IoT Readme für das Geräte-SDK JavaScript für Version 2
- AWS IoT Geräte-SDK für JavaScript v2-Beispiele
- AWS IoT Geräte-SDK für JavaScript v2-API-Dokumentation

Java

AWS IoT Geräte-SDK SDK for Java

Das AWS IoT Device SDK for Java ermöglicht es Java-Entwicklern, über MQTT oder MQTT über das Protokoll auf die AWS IoT WebSocket Plattform zuzugreifen. Das SDK wird mit Support für Schattengeräte angelegt. Sie können über die HTTP-Methoden GET, UPDATE und DELETE auf Schattengeräte zugreifen. Das SDK unterstützt auch ein vereinfachtes Zugangsmodell für Schattengeräte, sodass Entwickler mithilfe der Methoden „Getter” und „Setter” Daten mit den Schattengeräten austauschen können, ohne JSON-Dokumente serialisieren oder deserialisieren zu müssen.

> **Note**
>
> Das AWS IoT Device SDK for Java v2 unterstützt jetzt die Android-Entwicklung. Weitere Informationen finden Sie unter AWS IoT Geräte-SDK SDK for Android.

Weitere Informationen finden Sie hier:

- AWS IoT Geräte-SDK SDK for Java v2 auf GitHub
- AWS IoT Readme zum Geräte-SDK für Java v2
- AWS IoT Geräte-SDK SDK for Java v2-Beispiele
- AWS IoT API-Dokumentation zum Geräte-SDK für Java v2

Swift

AWS IoT Geräte-SDK für Swift

Das AWS IoT Device SDK for Swift ermöglicht es Swift-Entwicklern, AWS IoT Anwendungen für Linux und Apple MacOS-, iOS- und tvOS-Plattformen mithilfe des MQTT 5-Protokolls zu erstellen.

Weitere Informationen finden Sie hier:

- AWS IoT Geräte-SDK für Swift aktiviert GitHub
- AWS IoT Geräte-SDK für Swift Readme
- AWS IoT Geräte-SDK für Swift-Beispiele

## AWS IoT Geräte-SDK für Embedded C

> **Note**
>
> Dieses SDK ist für die Verwendung durch erfahrene Entwickler eingebetteter Software vorgesehen.

Das AWS IoT Device SDK for Embedded C (C-SDK) ist eine Sammlung von C-Quelldateien unter der MIT-Open-Source-Lizenz, die in eingebetteten Anwendungen verwendet werden können, um IoT-Geräte sicher zu AWS IoT Core verbinden. Es umfasst einen MQTT-Client, JSON-Parser und AWS IoT Device Shadow, AWS IoT Jobs, AWS IoT Fleet Provisioning und Bibliotheken. AWS IoT Device Defender Dieses SDK wird im Quellformat verteilt und kann zusammen mit dem Anwendungscode, weiteren Bibliotheken und einem Betriebssystem (BS) Ihrer Wahl in die Kunden-Firmware integriert werden.

Das AWS IoT Device SDK for Embedded C richtet sich im Allgemeinen an Geräte mit eingeschränkten Ressourcen, die eine optimierte Laufzeit in C-Sprache benötigen. Sie können das SDK auf jedem Betriebssystem verwenden und es auf jedem Prozessortyp hosten (z. B. MCUs und MPUs).

Weitere Informationen finden Sie hier:

- AWS IoT Geräte-SDK für Embedded C auf GitHub
- AWS IoT Readme-Datei zum Geräte-SDK für Embedded C
- AWS IoT Geräte-SDK für eingebettete C-Beispiele

# AWS Mobil SDKs

The AWS Mobile SDKs bietet Entwicklern mobiler Apps plattformspezifischen Support für die APIs AWS IoT Core Dienste, die IoT-Gerätekommunikation mit MQTT und andere Dienste. APIs AWS

Android

AWS Mobile SDK for Android

Das AWS Mobile SDK for Android enthält eine Bibliothek, Beispiele und Dokumentation, mit denen Entwickler vernetzte mobile Anwendungen erstellen können. AWS Dieses SDK bietet auch

Unterstützung für die MQTT-Gerätekommunikation und das Aufrufen APIs der AWS IoT Core Dienste. Weitere Informationen finden Sie hier:

- AWS Mobile SDK for Android auf GitHub
- AWS Mobile SDK for Android Readme
- AWS Mobile SDK for Android Beispiele
- AWS Mobile SDK for Android API-Referenz
- AWSIoTClient Referenzdokumentation zum Unterricht

iOS

AWS Mobile SDK for iOS

Das AWS Mobile SDK for iOS ist ein Open-Source-Software-Entwicklungskit, das unter einer Apache Open Source-Lizenz vertrieben wird. Das AWS Mobile SDK for iOS bietet eine Bibliothek, Codebeispiele und Dokumentation, mit deren Hilfe Entwickler vernetzte mobile Anwendungen erstellen können. AWS Dieses SDK bietet auch Unterstützung für die MQTT-Gerätekommunikation und das Aufrufen APIs der AWS IoT Core Dienste. Weitere Informationen finden Sie hier:

- AWS Mobile SDK for iOS auf GitHub
- AWS Mobile SDK for iOS Readme
- AWS Mobile SDK for iOS Beispiele
- AWSIoReferenzdokumente der T-Klasse in der AWS Mobile SDK for iOS

# AWS IoT Geräteclient

Der AWS IoT Geräteclient stellt Code bereit, mit dem Ihr Gerät eine Verbindung herstellen AWS IoT, Aufgaben zur Flottenbereitstellung ausführen, Gerätesicherheitsrichtlinien unterstützen, eine Verbindung über sicheres Tunneling herstellen und Aufträge auf Ihrem Gerät verarbeiten kann. Sie können diese Software auf Ihrem Gerät installieren, um diese routinemäßigen Geräteaufgaben zu erledigen, sodass Sie sich auf Ihre spezifische Lösung konzentrieren können.

> **Note**
>
> Der AWS IoT Device Client funktioniert mit mikroprozessorbasierten IoT-Geräten mit x86_64- oder ARM-Prozessoren und gängigen Linux-Betriebssystemen.

C++

AWS IoT Geräteclient

Weitere Informationen zum AWS IoT Geräteclient in C++ finden Sie unter:

- AWS IoT Geräteclient im C++-Quellcode auf GitHub
- AWS IoT Geräteclient in der C++-Readme-Datei

## Frühere AWS IoT Geräteversionen SDKs

Dies sind frühere Versionen von AWS IoT Device SDKs , die durch die oben aufgeführten neueren Versionen ersetzt wurden. Diese SDKs erhalten nur Wartungs- und Sicherheitsupdates. Sie werden nicht aktualisiert, um neue Funktionen aufzunehmen, und sollten nicht für neue Projekte verwendet werden.

- AWS IoT C++-Geräte-SDK aktiviert GitHub
- AWS IoT Readme-Datei zum C++-Geräte-SDK
- AWS IoT Geräte-SDK für Python v1 auf GitHub
- AWS IoT Readme zum Geräte-SDK für Python v1
- AWS IoT Geräte-SDK SDK for Java auf GitHub
- AWS IoT Readme für das Geräte-SDK für Java
- AWS IoT Geräte-SDK für ein JavaScript GitHub
- AWS IoT Geräte-SDK für JavaScript Readme
- Arduino Yún SDK aktiviert GitHub
- SDK für Arduino Yún Readme

# Codebeispiele für die AWS IoT Verwendung AWS SDKs

Die folgenden Codebeispiele zeigen, wie die Verwendung AWS IoT mit einem AWS Software Development Kit (SDK) funktioniert.

Bei Grundlagen handelt es sich um Code-Beispiele, die Ihnen zeigen, wie Sie die wesentlichen Vorgänge innerhalb eines Services ausführen.

Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Während Aktionen Ihnen zeigen, wie Sie einzelne Service-Funktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarios anzeigen.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erste Schritte

## Hallo AWS IoT

Die folgenden Codebeispiele veranschaulichen, wie Sie mit der Verwendung von AWS IoT beginnen.

C++

SDK für C++

Code für die CMake Datei CMake Lists.txt.

```
# Set the minimum required version of CMake for this project.
cmake_minimum_required(VERSION 3.13)

# Set the AWS service components used by this project.
set(SERVICE_COMPONENTS iot)

# Set this project's name.
project("hello_iot")

# Set the C++ standard to use to build this target.
# At least C++ 11 is required for the AWS SDK for C++.
set(CMAKE_CXX_STANDARD 11)
```

```
# Use the MSVC variable to determine if this is a Windows build.
set(WINDOWS_BUILD ${MSVC})

if (WINDOWS_BUILD) # Set the location where CMake can find the installed
 libraries for the AWS SDK.
    string(REPLACE ";" "/aws-cpp-sdk-all;" SYSTEM_MODULE_PATH
 "${CMAKE_SYSTEM_PREFIX_PATH}/aws-cpp-sdk-all")
    list(APPEND CMAKE_PREFIX_PATH ${SYSTEM_MODULE_PATH})
endif ()

# Find the AWS SDK for C++ package.
find_package(AWSSDK REQUIRED COMPONENTS ${SERVICE_COMPONENTS})

if (WINDOWS_BUILD AND AWSSDK_INSTALL_AS_SHARED_LIBS)
    # Copy relevant AWS SDK for C++ libraries into the current binary directory
 for running and debugging.

    # set(BIN_SUB_DIR "/Debug") # If you are building from the command line, you
 may need to uncomment this
    # and set the proper subdirectory to the executables' location.

    AWSSDK_CPY_DYN_LIBS(SERVICE_COMPONENTS ""
 ${CMAKE_CURRENT_BINARY_DIR}${BIN_SUB_DIR})
endif ()

add_executable(${PROJECT_NAME}
        hello_iot.cpp)

target_link_libraries(${PROJECT_NAME}
        ${AWSSDK_LINK_LIBRARIES})
```

Code für die Quelldatei hello_iot.cpp.

```
#include <aws/core/Aws.h>
#include <aws/iot/IoTClient.h>
#include <aws/iot/model/ListThingsRequest.h>
#include <iostream>

/*
 *  A "Hello IoT" starter application which initializes an AWS IoT client and
 *  lists the AWS IoT topics in the current account.
 *
```

```
 *  main function
 *
 *  Usage: 'hello_iot'
 *
 */

int main(int argc, char **argv) {
    Aws::SDKOptions options;
    //  Optional: change the log level for debugging.
    //  options.loggingOptions.logLevel = Aws::Utils::Logging::LogLevel::Debug;
    Aws::InitAPI(options); // Should only be called once.
    {
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

        Aws::IoT::IoTClient iotClient(clientConfig);
        // List the things in the current account.
        Aws::IoT::Model::ListThingsRequest listThingsRequest;

        Aws::String nextToken; // Used for pagination.
        Aws::Vector<Aws::IoT::Model::ThingAttribute> allThings;

        do {
            if (!nextToken.empty()) {
                listThingsRequest.SetNextToken(nextToken);
            }

            Aws::IoT::Model::ListThingsOutcome listThingsOutcome =
 iotClient.ListThings(
                    listThingsRequest);
            if (listThingsOutcome.IsSuccess()) {
                const Aws::Vector<Aws::IoT::Model::ThingAttribute> &things =
 listThingsOutcome.GetResult().GetThings();
                allThings.insert(allThings.end(), things.begin(), things.end());
                nextToken = listThingsOutcome.GetResult().GetNextToken();
            }
            else {
                std::cerr << "List things failed"
                          << listThingsOutcome.GetError().GetMessage() <<
 std::endl;
                break;
            }
        } while (!nextToken.empty());
```

```
        std::cout << allThings.size() << " thing(s) found." << std::endl;
        for (auto const &thing: allThings) {
            std::cout << thing.GetThingName() << std::endl;
        }
    }

    Aws::ShutdownAPI(options); // Should only be called once.
    return 0;
}
```

- Einzelheiten zur API finden Sie unter ListThings in der AWS SDK für C++ API-Referenz.

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iot.IotClient;
import software.amazon.awssdk.services.iot.model.ListThingsRequest;
import software.amazon.awssdk.services.iot.model.ListThingsResponse;
import software.amazon.awssdk.services.iot.model.ThingAttribute;
import software.amazon.awssdk.services.iot.paginators.ListThingsIterable;

import java.util.List;

public class HelloIoT {
    public static void main(String[] args) {
```

```
        System.out.println("Hello AWS IoT. Here is a listing of your AWS IoT
 Things:");
        IotClient iotClient = IotClient.builder()
            .region(Region.US_EAST_1)
            .build();

        listAllThings(iotClient);
    }

    public static void listAllThings(IotClient iotClient) {
        iotClient.listThingsPaginator(ListThingsRequest.builder()
                .maxResults(10)
                .build())
            .stream()
            .flatMap(response -> response.things().stream())
            .forEach(attribute -> {
                System.out.println("Thing name: " + attribute.thingName());
                System.out.println("Thing ARN: " + attribute.thingArn());
            });
    }
}
```

- Einzelheiten zur API finden Sie unter ListThings in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import aws.sdk.kotlin.services.iot.IotClient
import aws.sdk.kotlin.services.iot.model.ListThingsRequest

suspend fun main() {
    println("A listing of your AWS IoT Things:")
    listAllThings()
}
```

```
suspend fun listAllThings() {
    val thingsRequest =
        ListThingsRequest {
            maxResults = 10
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        val response = iotClient.listThings(thingsRequest)
        val thingList = response.things
        if (thingList != null) {
            for (attribute in thingList) {
                println("Thing name ${attribute.thingName}")
                println("Thing ARN: ${attribute.thingArn}")
            }
        }
    }
}
```

- API-Details finden Sie unter ListThings in der AWS API-Referenz zum SDK für Kotlin.

Codebeispiele

- Grundlegende Beispiele für die Verwendung AWS IoTAWS SDKs
  - Hallo AWS IoT
  - Lernen Sie die Grundlagen AWS IoT mit einem AWS SDK kennen
  - Aktionen zur AWS IoT Verwendung AWS SDKs
    - Verwendung AttachThingPrincipal mit einem AWS SDK oder CLI
    - Verwendung CreateKeysAndCertificate mit einem AWS SDK oder CLI
    - Verwendung CreateThing mit einem AWS SDK oder CLI
    - Verwendung CreateTopicRule mit einem AWS SDK oder CLI
    - Verwendung DeleteCertificate mit einem AWS SDK oder CLI
    - Verwendung DeleteThing mit einem AWS SDK oder CLI
    - Verwendung DeleteTopicRule mit einem AWS SDK oder CLI
    - Verwendung DescribeEndpoint mit einem AWS SDK oder CLI
    - Verwendung DescribeThing mit einem AWS SDK oder CLI
    - Verwendung DetachThingPrincipal mit einem AWS SDK oder CLI

- Verwendung ListCertificates mit einem AWS SDK oder CLI
- Verwendung ListThings mit einem AWS SDK oder CLI
- Verwendung SearchIndex mit einem AWS SDK oder CLI
- Verwendung UpdateIndexingConfiguration mit einem AWS SDK oder CLI
- Verwendung UpdateThing mit einem AWS SDK oder CLI

# Grundlegende Beispiele für die Verwendung AWS IoTAWS SDKs

Die folgenden Codebeispiele zeigen, wie die Grundlagen von AWS IoT with verwendet AWS SDKs werden.

Beispiele

- Hallo AWS IoT
- Lernen Sie die Grundlagen AWS IoT mit einem AWS SDK kennen
- Aktionen zur AWS IoT Verwendung AWS SDKs
  - Verwendung AttachThingPrincipal mit einem AWS SDK oder CLI
  - Verwendung CreateKeysAndCertificate mit einem AWS SDK oder CLI
  - Verwendung CreateThing mit einem AWS SDK oder CLI
  - Verwendung CreateTopicRule mit einem AWS SDK oder CLI
  - Verwendung DeleteCertificate mit einem AWS SDK oder CLI
  - Verwendung DeleteThing mit einem AWS SDK oder CLI
  - Verwendung DeleteTopicRule mit einem AWS SDK oder CLI
  - Verwendung DescribeEndpoint mit einem AWS SDK oder CLI
  - Verwendung DescribeThing mit einem AWS SDK oder CLI
  - Verwendung DetachThingPrincipal mit einem AWS SDK oder CLI
  - Verwendung ListCertificates mit einem AWS SDK oder CLI
  - Verwendung ListThings mit einem AWS SDK oder CLI
  - Verwendung SearchIndex mit einem AWS SDK oder CLI
  - Verwendung UpdateIndexingConfiguration mit einem AWS SDK oder CLI
  - Verwendung UpdateThing mit einem AWS SDK oder CLI

# Hallo AWS IoT

Die folgenden Codebeispiele veranschaulichen, wie Sie mit der Verwendung von AWS IoT beginnen.

C++

SDK für C++

Code für die CMake Datei CMake Lists.txt.

```
# Set the minimum required version of CMake for this project.
cmake_minimum_required(VERSION 3.13)

# Set the AWS service components used by this project.
set(SERVICE_COMPONENTS iot)

# Set this project's name.
project("hello_iot")

# Set the C++ standard to use to build this target.
# At least C++ 11 is required for the AWS SDK for C++.
set(CMAKE_CXX_STANDARD 11)

# Use the MSVC variable to determine if this is a Windows build.
set(WINDOWS_BUILD ${MSVC})

if (WINDOWS_BUILD) # Set the location where CMake can find the installed
 libraries for the AWS SDK.
    string(REPLACE ";" "/aws-cpp-sdk-all;" SYSTEM_MODULE_PATH
 "${CMAKE_SYSTEM_PREFIX_PATH}/aws-cpp-sdk-all")
    list(APPEND CMAKE_PREFIX_PATH ${SYSTEM_MODULE_PATH})
endif ()

# Find the AWS SDK for C++ package.
find_package(AWSSDK REQUIRED COMPONENTS ${SERVICE_COMPONENTS})

if (WINDOWS_BUILD AND AWSSDK_INSTALL_AS_SHARED_LIBS)
    # Copy relevant AWS SDK for C++ libraries into the current binary directory
 for running and debugging.

    # set(BIN_SUB_DIR "/Debug") # If you are building from the command line, you
 may need to uncomment this
    # and set the proper subdirectory to the executables' location.
```

```
    AWSSDK_CPY_DYN_LIBS(SERVICE_COMPONENTS ""
 ${CMAKE_CURRENT_BINARY_DIR}${BIN_SUB_DIR})
endif ()

add_executable(${PROJECT_NAME}
        hello_iot.cpp)

target_link_libraries(${PROJECT_NAME}
        ${AWSSDK_LINK_LIBRARIES})
```

Code für die Quelldatei hello_iot.cpp.

```
#include <aws/core/Aws.h>
#include <aws/iot/IoTClient.h>
#include <aws/iot/model/ListThingsRequest.h>
#include <iostream>

/*
 *  A "Hello IoT" starter application which initializes an AWS IoT client and
 *  lists the AWS IoT topics in the current account.
 *
 *  main function
 *
 *  Usage: 'hello_iot'
 *
 */

int main(int argc, char **argv) {
    Aws::SDKOptions options;
    //  Optional: change the log level for debugging.
    //  options.loggingOptions.logLevel = Aws::Utils::Logging::LogLevel::Debug;
    Aws::InitAPI(options); // Should only be called once.
    {
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

        Aws::IoT::IoTClient iotClient(clientConfig);
        // List the things in the current account.
        Aws::IoT::Model::ListThingsRequest listThingsRequest;
```

```
        Aws::String nextToken; // Used for pagination.
        Aws::Vector<Aws::IoT::Model::ThingAttribute> allThings;

        do {
            if (!nextToken.empty()) {
                listThingsRequest.SetNextToken(nextToken);
            }

            Aws::IoT::Model::ListThingsOutcome listThingsOutcome =
 iotClient.ListThings(
                    listThingsRequest);
            if (listThingsOutcome.IsSuccess()) {
                const Aws::Vector<Aws::IoT::Model::ThingAttribute> &things =
 listThingsOutcome.GetResult().GetThings();
                allThings.insert(allThings.end(), things.begin(), things.end());
                nextToken = listThingsOutcome.GetResult().GetNextToken();
            }
            else {
                std::cerr << "List things failed"
                          << listThingsOutcome.GetError().GetMessage() <<
 std::endl;
                break;
            }
        } while (!nextToken.empty());

        std::cout << allThings.size() << " thing(s) found." << std::endl;
        for (auto const &thing: allThings) {
            std::cout << thing.GetThingName() << std::endl;
        }
    }

    Aws::ShutdownAPI(options); // Should only be called once.
    return 0;
}
```

- Einzelheiten zur API finden Sie unter ListThings in der AWS SDK für C++ API-Referenz.

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iot.IotClient;
import software.amazon.awssdk.services.iot.model.ListThingsRequest;
import software.amazon.awssdk.services.iot.model.ListThingsResponse;
import software.amazon.awssdk.services.iot.model.ThingAttribute;
import software.amazon.awssdk.services.iot.paginators.ListThingsIterable;

import java.util.List;

public class HelloIoT {
    public static void main(String[] args) {
        System.out.println("Hello AWS IoT. Here is a listing of your AWS IoT
 Things:");
        IotClient iotClient = IotClient.builder()
            .region(Region.US_EAST_1)
            .build();

        listAllThings(iotClient);
    }

    public static void listAllThings(IotClient iotClient) {
        iotClient.listThingsPaginator(ListThingsRequest.builder()
                .maxResults(10)
                .build())
            .stream()
            .flatMap(response -> response.things().stream())
            .forEach(attribute -> {
                System.out.println("Thing name: " + attribute.thingName());
                System.out.println("Thing ARN: " + attribute.thingArn());
            });
    }
}
```

- Einzelheiten zur API finden Sie unter ListThings in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import aws.sdk.kotlin.services.iot.IotClient
import aws.sdk.kotlin.services.iot.model.ListThingsRequest

suspend fun main() {
    println("A listing of your AWS IoT Things:")
    listAllThings()
}

suspend fun listAllThings() {
    val thingsRequest =
        ListThingsRequest {
            maxResults = 10
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        val response = iotClient.listThings(thingsRequest)
        val thingList = response.things
        if (thingList != null) {
            for (attribute in thingList) {
                println("Thing name ${attribute.thingName}")
                println("Thing ARN: ${attribute.thingArn}")
            }
        }
    }
}
```

- API-Details finden Sie unter ListThings in der AWS API-Referenz zum SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS IoT mit einem SDK AWS Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Lernen Sie die Grundlagen AWS IoT mit einem AWS SDK kennen

Die folgenden Code-Beispiele veranschaulichen Folgendes:

- Erstelle ein AWS IoT Ding.
- Generieren Sie ein Gerätezertifikat.
- Aktualisiere ein AWS IoT Ding mit Attributen.
- Gibt einen eindeutigen Endpunkt zurück.
- Listen Sie Ihre AWS IoT Zertifikate auf.
- Erstelle einen AWS IoT Schatten.
- Schreiben Sie Statusinformationen aus.
- Erstellt eine Regel.
- Listen Sie Ihre Regeln auf.
- Suchen Sie Dinge anhand des Dingnamens.
- Lösche ein AWS IoT Ding.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Erschaffe AWS IoT etwas.

```
    Aws::String thingName = askQuestion("Enter a thing name: ");
```

```
    if (!createThing(thingName, clientConfiguration)) {
        std::cerr << "Exiting because createThing failed." << std::endl;
        cleanup("", "", "", "", "", false, clientConfiguration);
        return false;
    }
```

```
//! Create an AWS IoT thing.
/*!
  \param thingName: The name for the thing.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::createThing(const Aws::String &thingName,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::CreateThingRequest createThingRequest;
    createThingRequest.SetThingName(thingName);

    Aws::IoT::Model::CreateThingOutcome outcome = iotClient.CreateThing(
            createThingRequest);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully created thing " << thingName << std::endl;
    }
    else {
        std::cerr << "Failed to create thing " << thingName << ": " <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

Generieren Sie ein Gerätezertifikat und hängen Sie es an.

```
    Aws::String certificateARN;
    Aws::String certificateID;
    if (askYesNoQuestion("Would you like to create a certificate for your thing?
 (y/n) ")) {
        Aws::String outputFolder;
        if (askYesNoQuestion(
```

```
                "Would you like to save the certificate and keys to file? (y/n)
 ")) {
            outputFolder = std::filesystem::current_path();
            outputFolder += "/device_keys_and_certificates";

            std::filesystem::create_directories(outputFolder);

            std::cout << "The certificate and keys will be saved to the folder: "
                      << outputFolder << std::endl;
        }

        if (!createKeysAndCertificate(outputFolder, certificateARN,
 certificateID,
                                       clientConfiguration)) {
            std::cerr << "Exiting because createKeysAndCertificate failed."
                      << std::endl;
            cleanup(thingName, "", "", "", "", false, clientConfiguration);
            return false;
        }

        std::cout << "\nNext, the certificate will be attached to the thing.\n"
                  << std::endl;
        if (!attachThingPrincipal(certificateARN, thingName,
 clientConfiguration)) {
            std::cerr << "Exiting because attachThingPrincipal failed." <<
 std::endl;
            cleanup(thingName, certificateARN, certificateID, "", "",
                    false,
                    clientConfiguration);
            return false;
        }
    }
```

```
//! Create keys and certificate for an Aws IoT device.
//! This routine will save certificates and keys to an output folder, if
 provided.
/*!
  \param outputFolder: Location for storing output in files, ignored when string
 is empty.
  \param certificateARNResult: A string to receive the ARN of the created
 certificate.
  \param certificateID: A string to receive the ID of the created certificate.
```

```
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::createKeysAndCertificate(const Aws::String &outputFolder,
                                           Aws::String &certificateARNResult,
                                           Aws::String &certificateID,
                                           const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient client(clientConfiguration);
    Aws::IoT::Model::CreateKeysAndCertificateRequest
 createKeysAndCertificateRequest;

    Aws::IoT::Model::CreateKeysAndCertificateOutcome outcome =
            client.CreateKeysAndCertificate(createKeysAndCertificateRequest);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully created a certificate and keys" << std::endl;
        certificateARNResult = outcome.GetResult().GetCertificateArn();
        certificateID = outcome.GetResult().GetCertificateId();
        std::cout << "Certificate ARN: " << certificateARNResult << ",
 certificate ID: "
                  << certificateID << std::endl;

        if (!outputFolder.empty()) {
            std::cout << "Writing certificate and keys to the folder '" <<
 outputFolder
                      << "'." << std::endl;
            std::cout << "Be sure these files are stored securely." << std::endl;

            Aws::String certificateFilePath = outputFolder + "/
certificate.pem.crt";
            std::ofstream certificateFile(certificateFilePath);
            if (!certificateFile.is_open()) {
                std::cerr << "Error opening certificate file, '" <<
 certificateFilePath
                          << "'."
                          << std::endl;
                return false;
            }
            certificateFile << outcome.GetResult().GetCertificatePem();
            certificateFile.close();

            const Aws::IoT::Model::KeyPair &keyPair =
 outcome.GetResult().GetKeyPair();
```

```
            Aws::String privateKeyFilePath = outputFolder + "/private.pem.key";
            std::ofstream privateKeyFile(privateKeyFilePath);
            if (!privateKeyFile.is_open()) {
                std::cerr << "Error opening private key file, '" <<
 privateKeyFilePath
                          << "'."
                          << std::endl;
                return false;
            }
            privateKeyFile << keyPair.GetPrivateKey();
            privateKeyFile.close();

            Aws::String publicKeyFilePath = outputFolder + "/public.pem.key";
            std::ofstream publicKeyFile(publicKeyFilePath);
            if (!publicKeyFile.is_open()) {
                std::cerr << "Error opening public key file, '" <<
 publicKeyFilePath
                          << "'."
                          << std::endl;
                return false;
            }
            publicKeyFile << keyPair.GetPublicKey();
        }
    }
    else {
        std::cerr << "Error creating keys and certificate: "
                  << outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}

//! Attach a principal to an AWS IoT thing.
/*!
  \param principal: A principal to attach.
  \param thingName: The name for the thing.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::attachThingPrincipal(const Aws::String &principal,
                                       const Aws::String &thingName,
                                       const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient client(clientConfiguration);
```

```
    Aws::IoT::Model::AttachThingPrincipalRequest request;
    request.SetPrincipal(principal);
    request.SetThingName(thingName);
    Aws::IoT::Model::AttachThingPrincipalOutcome outcome =
 client.AttachThingPrincipal(
           request);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully attached principal to thing." << std::endl;
    }
    else {
        std::cerr << "Failed to attach principal to thing." <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

Führen Sie verschiedene Operationen an dem AWS IoT Ding durch.

```
    if (!updateThing(thingName, { {"location", "Office"}, {"firmwareVersion",
 "v2.0"} }, clientConfiguration)) {
        std::cerr << "Exiting because updateThing failed." << std::endl;
        cleanup(thingName, certificateARN, certificateID, "", "", false,
                clientConfiguration);
        return false;
    }

    printAsterisksLine();

    std::cout << "Now an endpoint will be retrieved for your account.\n" <<
 std::endl;
    std::cout << "An IoT Endpoint refers to a specific URL or Uniform Resource
 Locator that serves as the entry point\n"
    << "for communication between IoT devices and the AWS IoT service." <<
 std::endl;

    askQuestion("Press Enter to continue:", alwaysTrueTest);

    Aws::String endpoint;
    if (!describeEndpoint(endpoint, clientConfiguration)) {
        std::cerr << "Exiting because getEndpoint failed." << std::endl;
        cleanup(thingName, certificateARN, certificateID, "", "", false,
```

```
                clientConfiguration);
        return false;
    }
    std::cout <<"Your endpoint is " << endpoint << "." << std::endl;
    printAsterisksLine();

    std::cout << "Now the certificates in your account will be listed." <<
 std::endl;
    askQuestion("Press Enter to continue:", alwaysTrueTest);

    if (!listCertificates(clientConfiguration)) {
        std::cerr << "Exiting because listCertificates failed." << std::endl;
        cleanup(thingName, certificateARN, certificateID, "", "", false,
                clientConfiguration);
        return false;
    }

    printAsterisksLine();

    std::cout << "Now the shadow for the thing will be updated.\n" << std::endl;
    std::cout << "A thing shadow refers to a feature that enables you to create a
 virtual representation, or \"shadow,\"\n"
    << "of a physical device or thing. The thing shadow allows you to synchronize
 and control the state of a device between\n"
    << "the cloud and the device itself. and the AWS IoT service. For example,
 you can write and retrieve JSON data from a thing shadow." << std::endl;
    askQuestion("Press Enter to continue:", alwaysTrueTest);

    if (!updateThingShadow(thingName, R"({"state":{"reported":
{"temperature":25,"humidity":50}}})", clientConfiguration)) {
        std::cerr << "Exiting because updateThingShadow failed." << std::endl;
        cleanup(thingName, certificateARN, certificateID, "", "", false,
                clientConfiguration);
        return false;
    }

    printAsterisksLine();

    std::cout << "Now, the state information for the shadow will be retrieved.\n"
 << std::endl;
    askQuestion("Press Enter to continue:", alwaysTrueTest);

    Aws::String shadowState;
    if (!getThingShadow(thingName, shadowState, clientConfiguration)) {
```

```
        std::cerr << "Exiting because getThingShadow failed." << std::endl;
        cleanup(thingName, certificateARN, certificateID, "", "", false,
                clientConfiguration);
        return false;
    }
    std::cout << "The retrieved shadow state is: " << shadowState << std::endl;

    printAsterisksLine();

    std::cout << "A rule with now be added to to the thing.\n" << std::endl;
    std::cout << "Any user who has permission to create rules will be able to
access data processed by the rule." << std::endl;
    std::cout << "In this case, the rule will use an Simple Notification Service
(SNS) topic and an IAM rule." << std::endl;
    std::cout << "These resources will be created using a CloudFormation
template." << std::endl;
    std::cout << "Stack creation may take a few minutes." << std::endl;

    askQuestion("Press Enter to continue: ", alwaysTrueTest);
    Aws::Map<Aws::String, Aws::String> outputs
=createCloudFormationStack(STACK_NAME,clientConfiguration);
    if (outputs.empty()) {
        std::cerr << "Exiting because createCloudFormationStack failed." <<
std::endl;
        cleanup(thingName, certificateARN, certificateID, "", "", false,
                clientConfiguration);
        return false;
    }

    // Retrieve the topic ARN and role ARN from the CloudFormation stack outputs.
    auto topicArnIter = outputs.find(SNS_TOPIC_ARN_OUTPUT);
    auto roleArnIter = outputs.find(ROLE_ARN_OUTPUT);
    if ((topicArnIter == outputs.end()) || (roleArnIter == outputs.end())) {
        std::cerr << "Exiting because output '" << SNS_TOPIC_ARN_OUTPUT <<
        "' or '" << ROLE_ARN_OUTPUT << "'not found in the CloudFormation stack."
<< std::endl;
        cleanup(thingName, certificateARN, certificateID, STACK_NAME, "",
                false,
                clientConfiguration);
        return false;
    }

    Aws::String topicArn = topicArnIter->second;
    Aws::String roleArn = roleArnIter->second;
```

```
    Aws::String sqlStatement = "SELECT * FROM '";
    sqlStatement += MQTT_MESSAGE_TOPIC_FILTER;
    sqlStatement += "'";

    printAsterisksLine();

    std::cout << "Now a rule will be created.\n" << std::endl;
    std::cout << "Rules are an administrator-level action. Any user who has
 permission\n"
                << "to create rules will be able to access data processed by the
 rule." << std::endl;
    std::cout << "In this case, the rule will use an SNS topic" << std::endl;
    std::cout << "and the following SQL statement '" << sqlStatement << "'." <<
 std::endl;
    std::cout << "For more information on IoT SQL, see https://
docs.aws.amazon.com/iot/latest/developerguide/iot-sql-reference.html" <<
 std::endl;
    Aws::String ruleName = askQuestion("Enter a rule name: ");
    if (!createTopicRule(ruleName, topicArn, sqlStatement, roleArn,
 clientConfiguration)) {
        std::cerr << "Exiting because createRule failed." << std::endl;
        cleanup(thingName, certificateARN, certificateID, STACK_NAME, "",
                false,
                clientConfiguration);
        return false;
    }

    printAsterisksLine();

    std::cout << "Now your rules will be listed.\n" << std::endl;
    askQuestion("Press Enter to continue: ", alwaysTrueTest);
    if (!listTopicRules(clientConfiguration)) {
        std::cerr << "Exiting because listRules failed." << std::endl;
        cleanup(thingName, certificateARN, certificateID, STACK_NAME, ruleName,
                false,
                clientConfiguration);
        return false;
    }

    printAsterisksLine();
    Aws::String queryString = "thingName:" + thingName;
    std::cout << "Now the AWS IoT fleet index will be queried with the query\n'"
    << queryString << "'.\n" << std::endl;
```

```
    std::cout << "For query information, see https://docs.aws.amazon.com/iot/
latest/developerguide/query-syntax.html" << std::endl;

    std::cout << "For this query to work, thing indexing must be enabled in your
 account.\n"
    << "This can be done with the awscli command line by calling 'aws iot update-
indexing-configuration'\n"
       << "or it can be done programmatically." << std::endl;
    std::cout << "For more information, see https://docs.aws.amazon.com/iot/
latest/developerguide/managing-index.html" << std::endl;
    if (askYesNoQuestion("Do you want to enable thing indexing in your account?
 (y/n) "))
    {
        Aws::IoT::Model::ThingIndexingConfiguration thingIndexingConfiguration;

 thingIndexingConfiguration.SetThingIndexingMode(Aws::IoT::Model::ThingIndexingMode::REGI

 thingIndexingConfiguration.SetThingConnectivityIndexingMode(Aws::IoT::Model::ThingConnec
        // The ThingGroupIndexingConfiguration object is ignored if not set.
        Aws::IoT::Model::ThingGroupIndexingConfiguration
 thingGroupIndexingConfiguration;
        if (!updateIndexingConfiguration(thingIndexingConfiguration,
 thingGroupIndexingConfiguration, clientConfiguration)) {
            std::cerr << "Exiting because updateIndexingConfiguration failed." <<
 std::endl;
            cleanup(thingName, certificateARN, certificateID, STACK_NAME,
                    ruleName, false,
                    clientConfiguration);
            return false;
        }
    }

    if (!searchIndex(queryString, clientConfiguration)) {

        std::cerr << "Exiting because searchIndex failed." << std::endl;
        cleanup(thingName, certificateARN, certificateID, STACK_NAME, ruleName,
                false,
                clientConfiguration);
        return false;
    }
```

```
//! Update an AWS IoT thing with attributes.
```

```
/*!
  \param thingName: The name for the thing.
  \param attributeMap: A map of key/value attributes/
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::updateThing(const Aws::String &thingName,
                              const std::map<Aws::String, Aws::String>
 &attributeMap,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::UpdateThingRequest request;
    request.SetThingName(thingName);
    Aws::IoT::Model::AttributePayload attributePayload;
    for (const auto &attribute: attributeMap) {
        attributePayload.AddAttributes(attribute.first, attribute.second);
    }
    request.SetAttributePayload(attributePayload);

    Aws::IoT::Model::UpdateThingOutcome outcome = iotClient.UpdateThing(request);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully updated thing " << thingName << std::endl;
    }
    else {
        std::cerr << "Failed to update thing " << thingName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}

//! Describe the endpoint specific to the AWS account making the call.
/*!
  \param endpointResult: String to receive the endpoint result.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::describeEndpoint(Aws::String &endpointResult,
                                   const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::String endpoint;
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::DescribeEndpointRequest describeEndpointRequest;
```

```
    describeEndpointRequest.SetEndpointType(
            "iot:Data-ATS"); // Recommended endpoint type.

    Aws::IoT::Model::DescribeEndpointOutcome outcome =
 iotClient.DescribeEndpoint(
            describeEndpointRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully described endpoint." << std::endl;
        endpointResult = outcome.GetResult().GetEndpointAddress();
    }
    else {
        std::cerr << "Error describing endpoint" <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}

//! List certificates registered in the AWS account making the call.
/*!
   \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::listCertificates(
        const Aws::Client::ClientConfiguration &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::ListCertificatesRequest request;

    Aws::Vector<Aws::IoT::Model::Certificate> allCertificates;
    Aws::String marker; // Used to paginate results.
    do {
        if (!marker.empty()) {
            request.SetMarker(marker);
        }

        Aws::IoT::Model::ListCertificatesOutcome outcome =
 iotClient.ListCertificates(
                request);

        if (outcome.IsSuccess()) {
            const Aws::IoT::Model::ListCertificatesResult &result =
 outcome.GetResult();
```

```
            marker = result.GetNextMarker();
            allCertificates.insert(allCertificates.end(),
                                   result.GetCertificates().begin(),
                                   result.GetCertificates().end());
        }
        else {
            std::cerr << "Error: " << outcome.GetError().GetMessage() <<
 std::endl;
            return false;
        }
    } while (!marker.empty());

    std::cout << allCertificates.size() << " certificate(s) found." << std::endl;

    for (auto &certificate: allCertificates) {
        std::cout << "Certificate ID: " << certificate.GetCertificateId() <<
 std::endl;
        std::cout << "Certificate ARN: " << certificate.GetCertificateArn()
                  << std::endl;
        std::cout << std::endl;
    }

    return true;
}

//! Update the shadow of an AWS IoT thing.
/*!
  \param thingName: The name for the thing.
  \param document: The state information, in JSON format.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::updateThingShadow(const Aws::String &thingName,
                                    const Aws::String &document,
                                    const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoTDataPlane::IoTDataPlaneClient
 iotDataPlaneClient(clientConfiguration);
    Aws::IoTDataPlane::Model::UpdateThingShadowRequest updateThingShadowRequest;
    updateThingShadowRequest.SetThingName(thingName);
    std::shared_ptr<std::stringstream> streamBuf =
 std::make_shared<std::stringstream>(
            document);
    updateThingShadowRequest.SetBody(streamBuf);
```

```
    Aws::IoTDataPlane::Model::UpdateThingShadowOutcome outcome =
 iotDataPlaneClient.UpdateThingShadow(
            updateThingShadowRequest);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully updated thing shadow." << std::endl;
    }
    else {
        std::cerr << "Error while updating thing shadow."
                  << outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}

//! Get the shadow of an AWS IoT thing.
/*!
  \param thingName: The name for the thing.
  \param documentResult: String to receive the state information, in JSON format.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::getThingShadow(const Aws::String &thingName,
                                 Aws::String &documentResult,
                                 const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoTDataPlane::IoTDataPlaneClient iotClient(clientConfiguration);
    Aws::IoTDataPlane::Model::GetThingShadowRequest request;
    request.SetThingName(thingName);
    auto outcome = iotClient.GetThingShadow(request);
    if (outcome.IsSuccess()) {
        std::stringstream ss;
        ss << outcome.GetResult().GetPayload().rdbuf();
        documentResult = ss.str();
    }
    else {
        std::cerr << "Error getting thing shadow: " <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}

//! Create an AWS IoT rule with an SNS topic as the target.
/*!
```

```
  \param ruleName: The name for the rule.
  \param snsTopic: The SNS topic ARN for the action.
  \param sql: The SQL statement used to query the topic.
  \param roleARN: The IAM role ARN for the action.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool
AwsDoc::IoT::createTopicRule(const Aws::String &ruleName,
                             const Aws::String &snsTopicARN, const Aws::String
 &sql,
                             const Aws::String &roleARN,
                             const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);

    Aws::IoT::Model::CreateTopicRuleRequest request;
    request.SetRuleName(ruleName);

    Aws::IoT::Model::SnsAction snsAction;
    snsAction.SetTargetArn(snsTopicARN);
    snsAction.SetRoleArn(roleARN);

    Aws::IoT::Model::Action action;
    action.SetSns(snsAction);

    Aws::IoT::Model::TopicRulePayload topicRulePayload;
    topicRulePayload.SetSql(sql);
    topicRulePayload.SetActions({action});

    request.SetTopicRulePayload(topicRulePayload);
    auto outcome = iotClient.CreateTopicRule(request);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully created topic rule " << ruleName << "." <<
 std::endl;
    }
    else {
        std::cerr << "Error creating topic rule " << ruleName << ": " <<
                  outcome.GetError().GetMessage() << std::endl;
    }
    return outcome.IsSuccess();
}

//! Lists the AWS IoT topic rules.
```

```
/*!
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::listTopicRules(
        const Aws::Client::ClientConfiguration &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::ListTopicRulesRequest request;

    Aws::Vector<Aws::IoT::Model::TopicRuleListItem> allRules;
    Aws::String nextToken; // Used for pagination.
    do {
        if (!nextToken.empty()) {
            request.SetNextToken(nextToken);
        }

        Aws::IoT::Model::ListTopicRulesOutcome outcome =
 iotClient.ListTopicRules(
                request);

        if (outcome.IsSuccess()) {
            const Aws::IoT::Model::ListTopicRulesResult &result =
 outcome.GetResult();
            allRules.insert(allRules.end(),
                            result.GetRules().cbegin(),
                            result.GetRules().cend());

            nextToken = result.GetNextToken();
        }
        else {
            std::cerr << "ListTopicRules error: " <<
                      outcome.GetError().GetMessage() << std::endl;
            return false;
        }

    } while (!nextToken.empty());

    std::cout << "ListTopicRules: " << allRules.size() << " rule(s) found."
              << std::endl;
    for (auto &rule: allRules) {
        std::cout << "  Rule name: " << rule.GetRuleName() << ", rule ARN: "
                  << rule.GetRuleArn() << "." << std::endl;
    }
```

```
    return true;
}

//! Query the AWS IoT fleet index.
//! For query information, see https://docs.aws.amazon.com/iot/latest/
developerguide/query-syntax.html
/*!
  \param: query: The query string.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::searchIndex(const Aws::String &query,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);

    Aws::IoT::Model::SearchIndexRequest request;
    request.SetQueryString(query);

    Aws::Vector<Aws::IoT::Model::ThingDocument> allThingDocuments;
    Aws::String nextToken; // Used for pagination.
    do {
        if (!nextToken.empty()) {
            request.SetNextToken(nextToken);
        }

        Aws::IoT::Model::SearchIndexOutcome outcome =
 iotClient.SearchIndex(request);

        if (outcome.IsSuccess()) {
            const Aws::IoT::Model::SearchIndexResult &result =
 outcome.GetResult();
            allThingDocuments.insert(allThingDocuments.end(),
                                     result.GetThings().cbegin(),
                                     result.GetThings().cend());
            nextToken = result.GetNextToken();

        }
        else {
            std::cerr << "Error in SearchIndex: " <<
 outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
```

```
    } while (!nextToken.empty());

    std::cout << allThingDocuments.size() << " thing document(s) found." <<
 std::endl;
    for (const auto thingDocument: allThingDocuments) {
        std::cout << "  Thing name: " << thingDocument.GetThingName() << "."
                  << std::endl;
    }
    return true;
}
```

Bereinigen von Ressourcen.

```
bool
AwsDoc::IoT::cleanup(const Aws::String &thingName, const Aws::String
 &certificateARN,
                     const Aws::String &certificateID, const Aws::String
 &stackName,
                     const Aws::String &ruleName, bool askForConfirmation,
                     const Aws::Client::ClientConfiguration &clientConfiguration)
 {
    bool result = true;

    if (!ruleName.empty() && (!askForConfirmation ||
                              askYesNoQuestion("Delete the rule '" + ruleName +
                                               "'? (y/n) "))) {
        result &= deleteTopicRule(ruleName, clientConfiguration);
    }

    Aws::CloudFormation::CloudFormationClient
 cloudFormationClient(clientConfiguration);

    if (!stackName.empty() && (!askForConfirmation ||
                               askYesNoQuestion(
                                       "Delete the CloudFormation stack '" +
 stackName +
                                       "'? (y/n) "))) {
        result &= deleteStack(stackName, clientConfiguration);
    }

    if (!certificateARN.empty() && (!askForConfirmation ||
                                    askYesNoQuestion("Delete the certificate '" +
```

```
                                                        certificateARN + "'? (y/n)
 "))) {
        result &= detachThingPrincipal(certificateARN, thingName,
 clientConfiguration);
        result &= deleteCertificate(certificateID, clientConfiguration);
    }

    if (!thingName.empty() && (!askForConfirmation ||
                               askYesNoQuestion("Delete the thing '" + thingName
 +
                                                "'? (y/n) "))) {
        result &= deleteThing(thingName, clientConfiguration);
    }

    return result;
}
```

```
//! Detach a principal from an AWS IoT thing.
/*!
  \param principal: A principal to detach.
  \param thingName: The name for the thing.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::detachThingPrincipal(const Aws::String &principal,
                                       const Aws::String &thingName,
                                       const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);

    Aws::IoT::Model::DetachThingPrincipalRequest detachThingPrincipalRequest;
    detachThingPrincipalRequest.SetThingName(thingName);
    detachThingPrincipalRequest.SetPrincipal(principal);

    Aws::IoT::Model::DetachThingPrincipalOutcome outcome =
 iotClient.DetachThingPrincipal(
            detachThingPrincipalRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully detached principal " << principal << " from
 thing "
                  << thingName << std::endl;
```

```
    }
    else {
        std::cerr << "Failed to detach principal " << principal << " from thing "
                  << thingName << ": "
                  << outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}

//! Delete a certificate.
/*!
  \param certificateID: The ID of a certificate.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::deleteCertificate(const Aws::String &certificateID,
                                    const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);

    Aws::IoT::Model::DeleteCertificateRequest request;
    request.SetCertificateId(certificateID);

    Aws::IoT::Model::DeleteCertificateOutcome outcome =
 iotClient.DeleteCertificate(
            request);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted certificate " << certificateID <<
 std::endl;
    }
    else {
        std::cerr << "Error deleting certificate " << certificateID << ": " <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}

//! Delete an AWS IoT rule.
/*!
  \param ruleName: The name for the rule.
  \param clientConfiguration: AWS client configuration.
```

```
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::deleteTopicRule(const Aws::String &ruleName,
                                  const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::DeleteTopicRuleRequest request;
    request.SetRuleName(ruleName);

    Aws::IoT::Model::DeleteTopicRuleOutcome outcome = iotClient.DeleteTopicRule(
            request);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted rule " << ruleName << std::endl;
    }
    else {
        std::cerr << "Failed to delete rule " << ruleName <<
                  ": " << outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}

//! Delete an AWS IoT thing.
/*!
  \param thingName: The name for the thing.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::deleteThing(const Aws::String &thingName,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::DeleteThingRequest request;
    request.SetThingName(thingName);
    const auto outcome = iotClient.DeleteThing(request);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted thing " << thingName << std::endl;
    }
    else {
        std::cerr << "Error deleting thing " << thingName << ": " <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
```

```
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Führen Sie ein interaktives Szenario durch, in dem AWS IoT Funktionen demonstriert werden.

```
import java.util.Scanner;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This Java example performs these tasks:
 *
 * 1. Creates an AWS IoT Thing.
 * 2. Generate and attach a device certificate.
 * 3. Update an AWS IoT Thing with Attributes.
 * 4. Get an AWS IoT Endpoint.
 * 5. List your certificates.
 * 6. Updates the shadow for the specified thing..
 * 7. Write out the state information, in JSON format
 * 8. Creates a rule
 * 9. List rules
 * 10. Search things
 * 11. Detach amd delete the certificate.
 * 12. Delete Thing.
 */
public class IotScenario {
```

```
   public static final String DASHES = new String(new char[80]).replace("\0",
"-");

   public static void main(String[] args) {
       final String usage =
           """
               Usage:
                   <roleARN> <snsAction>

               Where:
                   roleARN - The ARN of an IAM role that has permission to work
with AWS IOT.
                   snsAction  - An ARN of an SNS topic.
               """;

       if (args.length != 2) {
           System.out.println(usage);
           System.exit(1);
       }

       IotActions iotActions = new IotActions();
       String thingName;
       String ruleName;
       String roleARN = args[0];
       String snsAction = args[1];
       Scanner scanner = new Scanner(System.in);

       System.out.println(DASHES);
       System.out.println("Welcome to the AWS IoT basics scenario.");
       System.out.println("""
           This example program demonstrates various interactions with the AWS
Internet of Things (IoT) Core service. The program guides you through a series
of steps,
           including creating an IoT Thing, generating a device certificate,
updating the Thing with attributes, and so on.
           It utilizes the AWS SDK for Java V2 and incorporates functionality
for creating and managing IoT Things, certificates, rules,
           shadows, and performing searches. The program aims to showcase AWS
IoT capabilities and provides a comprehensive example for
           developers working with AWS IoT in a Java environment.

           Let's get started...

           """);
```

```
        System.out.println(DASHES);

        System.out.println("1. Create an AWS IoT Thing.");
        System.out.println("""
            An AWS IoT Thing represents a virtual entity in the AWS IoT service
that can be associated with
            a physical device.
            """);
        // Prompt the user for input.
        System.out.print("Enter Thing name: ");
        thingName = scanner.nextLine();
        iotActions.createIoTThing(thingName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. Generate a device certificate.");
        System.out.println("""
            A device certificate performs a role in securing the communication
between devices (Things)
            and the AWS IoT platform.
            """);

        System.out.print("Do you want to create a certificate for " +thingName
+"? (y/n)");
        String certAns = scanner.nextLine();
        String certificateArn="" ;
        if (certAns != null && certAns.trim().equalsIgnoreCase("y")) {
            certificateArn = iotActions.createCertificate();
            System.out.println("Attach the certificate to the AWS IoT Thing.");
            iotActions.attachCertificateToThing(thingName, certificateArn);
        } else {
            System.out.println("A device certificate was not created.");
        }
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. Update an AWS IoT Thing with Attributes.");
        System.out.println("""
             IoT Thing attributes, represented as key-value pairs, offer a
pivotal advantage in facilitating efficient data
             management and retrieval within the AWS IoT ecosystem.
            """);
        waitForInputToContinue(scanner);
        iotActions.updateShadowThing(thingName);
```

```
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Return a unique endpoint specific to the Amazon
Web Services account.");
        System.out.println("""
            An IoT Endpoint refers to a specific URL or Uniform Resource Locator
that serves as the entry point for communication between IoT devices and the AWS
IoT service.
           """);
        waitForInputToContinue(scanner);
        String endpointUrl = iotActions.describeEndpoint();
        System.out.println("The endpoint is "+endpointUrl);
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. List your AWS IoT certificates");
        waitForInputToContinue(scanner);
        if (certificateArn.length() > 0) {
            iotActions.listCertificates();
        } else {
            System.out.println("You did not create a certificates. Skipping this
step.");
        }
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Create an IoT shadow that refers to a digital
representation or virtual twin of a physical IoT device");
        System.out.println("""
            A Thing Shadow refers to a feature that enables you to create a
virtual representation, or "shadow,"
            of a physical device or thing. The Thing Shadow allows you to
synchronize and control the state of a device between
            the cloud and the device itself. and the AWS IoT service. For
example, you can write and retrieve JSON data from a Thing Shadow.
           """);
        waitForInputToContinue(scanner);
        iotActions.updateShadowThing(thingName);
        waitForInputToContinue(scanner);
        System.out.println(DASHES);
```

```
        System.out.println(DASHES);
        System.out.println("7. Write out the state information, in JSON
format.");
        waitForInputToContinue(scanner);
        iotActions.getPayload(thingName);
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Creates a rule");
        System.out.println("""
        Creates a rule that is an administrator-level action.
        Any user who has permission to create rules will be able to access data
processed by the rule.
        """);
        System.out.print("Enter Rule name: ");
        ruleName = scanner.nextLine();
        iotActions.createIoTRule(roleARN, ruleName, snsAction);
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. List your rules.");
        waitForInputToContinue(scanner);
        iotActions.listIoTRules();
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Search things using the Thing name.");
        waitForInputToContinue(scanner);
        String queryString = "thingName:"+thingName ;
        iotActions.searchThings(queryString);
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println(DASHES);
        if (certificateArn.length() > 0) {
            System.out.print("Do you want to detach and delete the certificate
for " +thingName +"? (y/n)");
            String delAns = scanner.nextLine();
            if (delAns != null && delAns.trim().equalsIgnoreCase("y")) {
```

```
                System.out.println("11. You selected to detach amd delete the
certificate.");
                waitForInputToContinue(scanner);
                iotActions.detachThingPrincipal(thingName, certificateArn);
                iotActions.deleteCertificate(certificateArn);
                waitForInputToContinue(scanner);
            } else {
                System.out.println("11. You selected not to delete the
certificate.");
            }
        } else {
            System.out.println("11. You did not create a certificate so there is
nothing to delete.");
        }
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("12. Delete the AWS IoT Thing.");
        System.out.print("Do you want to delete the IoT Thing? (y/n)");
        String delAns = scanner.nextLine();
        if (delAns != null && delAns.trim().equalsIgnoreCase("y")) {
            iotActions.deleteIoTThing(thingName);
        } else {
            System.out.println("The IoT Thing was not deleted.");
        }
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("The AWS IoT workflow has successfully completed.");
        System.out.println(DASHES);
    }


    private static void waitForInputToContinue(Scanner scanner) {
        while (true) {
            System.out.println("");
            System.out.println("Enter 'c' followed by <ENTER> to continue:");
            String input = scanner.nextLine();

            if (input.trim().equalsIgnoreCase("c")) {
                System.out.println("Continuing with the program...");
                System.out.println("");
                break;
            } else {
```

```
                // Handle invalid input.
                System.out.println("Invalid input. Please try again.");
            }
        }
    }
}
```

Eine Wrapper-Klasse für AWS IoT SDK-Methoden.

```
import
 software.amazon.awssdk.auth.credentials.EnvironmentVariableCredentialsProvider;
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.core.client.config.ClientOverrideConfiguration;
import software.amazon.awssdk.core.retry.RetryPolicy;
import software.amazon.awssdk.http.async.SdkAsyncHttpClient;
import software.amazon.awssdk.http.nio.netty.NettyNioAsyncHttpClient;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iot.IotAsyncClient;
import software.amazon.awssdk.services.iot.model.Action;
import software.amazon.awssdk.services.iot.model.AttachThingPrincipalRequest;
import software.amazon.awssdk.services.iot.model.AttachThingPrincipalResponse;
import software.amazon.awssdk.services.iot.model.Certificate;
import
 software.amazon.awssdk.services.iot.model.CreateKeysAndCertificateResponse;
import software.amazon.awssdk.services.iot.model.CreateThingRequest;
import software.amazon.awssdk.services.iot.model.CreateThingResponse;
import software.amazon.awssdk.services.iot.model.CreateTopicRuleRequest;
import software.amazon.awssdk.services.iot.model.CreateTopicRuleResponse;
import software.amazon.awssdk.services.iot.model.DeleteCertificateRequest;
import software.amazon.awssdk.services.iot.model.DeleteCertificateResponse;
import software.amazon.awssdk.services.iot.model.DeleteThingRequest;
import software.amazon.awssdk.services.iot.model.DeleteThingResponse;
import software.amazon.awssdk.services.iot.model.DescribeEndpointRequest;
import software.amazon.awssdk.services.iot.model.DescribeEndpointResponse;
import software.amazon.awssdk.services.iot.model.DescribeThingRequest;
import software.amazon.awssdk.services.iot.model.DescribeThingResponse;
import software.amazon.awssdk.services.iot.model.DetachThingPrincipalRequest;
import software.amazon.awssdk.services.iot.model.DetachThingPrincipalResponse;
import software.amazon.awssdk.services.iot.model.IotException;
import software.amazon.awssdk.services.iot.model.ListCertificatesResponse;
import software.amazon.awssdk.services.iot.model.ListTopicRulesRequest;
import software.amazon.awssdk.services.iot.model.ListTopicRulesResponse;
```

```
import software.amazon.awssdk.services.iot.model.SearchIndexRequest;
import software.amazon.awssdk.services.iot.model.SearchIndexResponse;
import software.amazon.awssdk.services.iot.model.TopicRuleListItem;
import software.amazon.awssdk.services.iot.model.SnsAction;
import software.amazon.awssdk.services.iot.model.TopicRulePayload;
import software.amazon.awssdk.services.iotdataplane.IotDataPlaneAsyncClient;
import software.amazon.awssdk.services.iotdataplane.model.GetThingShadowRequest;
import software.amazon.awssdk.services.iotdataplane.model.GetThingShadowResponse;
import
 software.amazon.awssdk.services.iotdataplane.model.UpdateThingShadowRequest;
import
 software.amazon.awssdk.services.iotdataplane.model.UpdateThingShadowResponse;
import java.nio.charset.StandardCharsets;
import java.time.Duration;
import java.util.List;
import java.util.concurrent.CompletableFuture;
import java.util.concurrent.CompletionException;
import java.util.regex.Matcher;
import java.util.regex.Pattern;

public class IotActions {

    private static IotAsyncClient iotAsyncClient;

    private static IotDataPlaneAsyncClient iotAsyncDataPlaneClient;

    private static final String TOPIC = "your-iot-topic";

    private static IotDataPlaneAsyncClient getAsyncDataPlaneClient() {
        SdkAsyncHttpClient httpClient = NettyNioAsyncHttpClient.builder()
            .maxConcurrency(100)
            .connectionTimeout(Duration.ofSeconds(60))
            .readTimeout(Duration.ofSeconds(60))
            .writeTimeout(Duration.ofSeconds(60))
            .build();

        ClientOverrideConfiguration overrideConfig =
 ClientOverrideConfiguration.builder()
            .apiCallTimeout(Duration.ofMinutes(2))
            .apiCallAttemptTimeout(Duration.ofSeconds(90))
            .retryPolicy(RetryPolicy.builder()
                .numRetries(3)
                .build())
            .build();
```

```
        if (iotAsyncDataPlaneClient == null) {
            iotAsyncDataPlaneClient = IotDataPlaneAsyncClient.builder()
                .region(Region.US_EAST_1)
                .httpClient(httpClient)
                .overrideConfiguration(overrideConfig)
                .build();
        }
        return iotAsyncDataPlaneClient;
    }


    private static IotAsyncClient getAsyncClient() {
        SdkAsyncHttpClient httpClient = NettyNioAsyncHttpClient.builder()
            .maxConcurrency(100)
            .connectionTimeout(Duration.ofSeconds(60))
            .readTimeout(Duration.ofSeconds(60))
            .writeTimeout(Duration.ofSeconds(60))
            .build();

        ClientOverrideConfiguration overrideConfig =
ClientOverrideConfiguration.builder()
            .apiCallTimeout(Duration.ofMinutes(2))
            .apiCallAttemptTimeout(Duration.ofSeconds(90))
            .retryPolicy(RetryPolicy.builder()
                .numRetries(3)
                .build())
            .build();

        if (iotAsyncClient == null) {
            iotAsyncClient = IotAsyncClient.builder()
                .region(Region.US_EAST_1)
                .httpClient(httpClient)
                .overrideConfiguration(overrideConfig)
                .build();
        }
        return iotAsyncClient;
    }

    /**
     * Creates an IoT certificate asynchronously.
     *
     * @return The ARN of the created certificate.
     * <p>
```

```
    * This method initiates an asynchronous request to create an IoT
certificate.
    * If the request is successful, it prints the certificate details and
returns the certificate ARN.
    * If an exception occurs, it prints the error message.
    */
   public String createCertificate() {
       CompletableFuture<CreateKeysAndCertificateResponse> future =
getAsyncClient().createKeysAndCertificate();
       final String[] certificateArn = {null};
       future.whenComplete((response, ex) -> {
           if (response != null) {
               String certificatePem = response.certificatePem();
               certificateArn[0] = response.certificateArn();

               // Print the details.
               System.out.println("\nCertificate:");
               System.out.println(certificatePem);
               System.out.println("\nCertificate ARN:");
               System.out.println(certificateArn[0]);

           } else {
               Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
               if (cause instanceof IotException) {
                   System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
               } else {
                   System.err.println("Unexpected error: " +
cause.getMessage());
               }
           }
       });

       future.join();
       return certificateArn[0];
   }

   /**
    * Creates an IoT Thing with the specified name asynchronously.
    *
    * @param thingName The name of the IoT Thing to create.
    *
```

```
    * This method initiates an asynchronous request to create an IoT Thing with
the specified name.
    * If the request is successful, it prints the name of the thing and its ARN
value.
    * If an exception occurs, it prints the error message.
    */
   public void createIoTThing(String thingName) {
       CreateThingRequest createThingRequest = CreateThingRequest.builder()
           .thingName(thingName)
           .build();

       CompletableFuture<CreateThingResponse> future =
getAsyncClient().createThing(createThingRequest);
       future.whenComplete((createThingResponse, ex) -> {
           if (createThingResponse != null) {
               System.out.println(thingName + " was successfully created. The
ARN value is " + createThingResponse.thingArn());
           } else {
               Throwable cause = ex.getCause();
               if (cause instanceof IotException) {
                   System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
               } else {
                   System.err.println("Unexpected error: " +
cause.getMessage());
               }
           }
       });

       future.join();
   }

   /**
    * Attaches a certificate to an IoT Thing asynchronously.
    *
    * @param thingName The name of the IoT Thing.
    * @param certificateArn The ARN of the certificate to attach.
    *
    * This method initiates an asynchronous request to attach a certificate to
an IoT Thing.
    * If the request is successful, it prints a confirmation message and
additional information about the Thing.
    * If an exception occurs, it prints the error message.
    */
```

```
   public void attachCertificateToThing(String thingName, String certificateArn)
{
       AttachThingPrincipalRequest principalRequest =
AttachThingPrincipalRequest.builder()
           .thingName(thingName)
           .principal(certificateArn)
           .build();

       CompletableFuture<AttachThingPrincipalResponse> future =
getAsyncClient().attachThingPrincipal(principalRequest);
       future.whenComplete((attachResponse, ex) -> {
           if (attachResponse != null &&
attachResponse.sdkHttpResponse().isSuccessful()) {
               System.out.println("Certificate attached to Thing
successfully.");

               // Print additional information about the Thing.
               describeThing(thingName);
           } else {
               Throwable cause = ex != null ? ex.getCause() : null;
               if (cause instanceof IotException) {
                   System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
               } else if (cause != null) {
                   System.err.println("Unexpected error: " +
cause.getMessage());
               } else {
                   System.err.println("Failed to attach certificate to Thing.
HTTP Status Code: " +
                           attachResponse.sdkHttpResponse().statusCode());
               }
           }
       });

       future.join();
   }

   /**
    * Describes an IoT Thing asynchronously.
    *
    * @param thingName The name of the IoT Thing.
    *
    * This method initiates an asynchronous request to describe an IoT Thing.
    * If the request is successful, it prints the Thing details.
```

```
     * If an exception occurs, it prints the error message.
     */
    private void describeThing(String thingName) {
        DescribeThingRequest thingRequest = DescribeThingRequest.builder()
            .thingName(thingName)
            .build();

        CompletableFuture<DescribeThingResponse> future =
getAsyncClient().describeThing(thingRequest);
        future.whenComplete((describeResponse, ex) -> {
            if (describeResponse != null) {
                System.out.println("Thing Details:");
                System.out.println("Thing Name: " +
describeResponse.thingName());
                System.out.println("Thing ARN: " + describeResponse.thingArn());
            } else {
                Throwable cause = ex != null ? ex.getCause() : null;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
                    System.err.println("Unexpected error: " +
cause.getMessage());
                } else {
                    System.err.println("Failed to describe Thing.");
                }
            }
        });

        future.join();
    }

    /**
     * Updates the shadow of an IoT Thing asynchronously.
     *
     * @param thingName The name of the IoT Thing.
     *
     * This method initiates an asynchronous request to update the shadow of an
IoT Thing.
     * If the request is successful, it prints a confirmation message.
     * If an exception occurs, it prints the error message.
     */
    public void updateShadowThing(String thingName) {
        // Create Thing Shadow State Document.
```

```
        String stateDocument = "{\"state\":{\"reported\":{\"temperature\":25,
\"humidity\":50}}}";
        SdkBytes data = SdkBytes.fromString(stateDocument,
StandardCharsets.UTF_8);
        UpdateThingShadowRequest updateThingShadowRequest =
UpdateThingShadowRequest.builder()
            .thingName(thingName)
            .payload(data)
            .build();

        CompletableFuture<UpdateThingShadowResponse> future =
getAsyncDataPlaneClient().updateThingShadow(updateThingShadowRequest);
        future.whenComplete((updateResponse, ex) -> {
            if (updateResponse != null) {
                System.out.println("Thing Shadow updated successfully.");
            } else {
                Throwable cause = ex != null ? ex.getCause() : null;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
                    System.err.println("Unexpected error: " +
cause.getMessage());
                } else {
                    System.err.println("Failed to update Thing Shadow.");
                }
            }
        });

        future.join();
    }

    /**
     * Describes the endpoint of the IoT service asynchronously.
     *
     * @return A CompletableFuture containing the full endpoint URL.
     *
     * This method initiates an asynchronous request to describe the endpoint of
the IoT service.
     * If the request is successful, it prints and returns the full endpoint URL.
     * If an exception occurs, it prints the error message.
     */
    public String describeEndpoint() {
```

```
        CompletableFuture<DescribeEndpointResponse> future =
 getAsyncClient().describeEndpoint(DescribeEndpointRequest.builder().endpointType("iot:Da
ATS").build());
        final String[] result = {null};

        future.whenComplete((endpointResponse, ex) -> {
            if (endpointResponse != null) {
                String endpointUrl = endpointResponse.endpointAddress();
                String exString = getValue(endpointUrl);
                String fullEndpoint = "https://" + exString + "-ats.iot.us-
east-1.amazonaws.com";

                System.out.println("Full Endpoint URL: " + fullEndpoint);
                result[0] = fullEndpoint;
            } else {
                Throwable cause = (ex instanceof CompletionException) ?
 ex.getCause() : ex;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
 cause).awsErrorDetails().errorMessage());
                } else {
                    System.err.println("Unexpected error: " +
 cause.getMessage());
                }
            }
        });

        future.join();
        return result[0];
    }

    /**
     * Extracts a specific value from the endpoint URL.
     *
     * @param input The endpoint URL to process.
     * @return The extracted value from the endpoint URL.
     */
    private static String getValue(String input) {
        // Define a regular expression pattern for extracting the subdomain.
        Pattern pattern = Pattern.compile("^(.*?)\\.iot\\.us-east-1\\.amazonaws\
\.com");

        // Match the pattern against the input string.
        Matcher matcher = pattern.matcher(input);
```

```
        // Check if a match is found.
        if (matcher.find()) {
            // Extract the subdomain from the first capturing group.
            String subdomain = matcher.group(1);
            System.out.println("Extracted subdomain: " + subdomain);
            return subdomain ;
        } else {
            System.out.println("No match found");
        }
        return "" ;
    }

    /**
     * Lists all certificates asynchronously.
     *
     * This method initiates an asynchronous request to list all certificates.
     * If the request is successful, it prints the certificate IDs and ARNs.
     * If an exception occurs, it prints the error message.
     */
    public void listCertificates() {
        CompletableFuture<ListCertificatesResponse> future =
getAsyncClient().listCertificates();
        future.whenComplete((response, ex) -> {
            if (response != null) {
                List<Certificate> certList = response.certificates();
                for (Certificate cert : certList) {
                    System.out.println("Cert id: " + cert.certificateId());
                    System.out.println("Cert Arn: " + cert.certificateArn());
                }
            } else {
                Throwable cause = ex != null ? ex.getCause() : null;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
                    System.err.println("Unexpected error: " +
cause.getMessage());
                } else {
                    System.err.println("Failed to list certificates.");
                }
            }
        });
```

```
        future.join();
    }

    /**
     * Retrieves the payload of a Thing's shadow asynchronously.
     *
     * @param thingName The name of the IoT Thing.
     *
     * This method initiates an asynchronous request to get the payload of a
Thing's shadow.
     * If the request is successful, it prints the shadow data.
     * If an exception occurs, it prints the error message.
     */
    public void getPayload(String thingName) {
        GetThingShadowRequest getThingShadowRequest =
GetThingShadowRequest.builder()
            .thingName(thingName)
            .build();

        CompletableFuture<GetThingShadowResponse> future =
getAsyncDataPlaneClient().getThingShadow(getThingShadowRequest);
        future.whenComplete((getThingShadowResponse, ex) -> {
            if (getThingShadowResponse != null) {
                // Extracting payload from response.
                SdkBytes payload = getThingShadowResponse.payload();
                String payloadString = payload.asUtf8String();
                System.out.println("Received Shadow Data: " + payloadString);
            } else {
                Throwable cause = ex != null ? ex.getCause() : null;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
                    System.err.println("Unexpected error: " +
cause.getMessage());
                } else {
                    System.err.println("Failed to get Thing Shadow payload.");
                }
            }
        });

        future.join();
    }
```

```
   /**
    * Creates an IoT rule asynchronously.
    *
    * @param roleARN The ARN of the IAM role that grants access to the rule's
actions.
    * @param ruleName The name of the IoT rule.
    * @param action The ARN of the action to perform when the rule is triggered.
    *
    * This method initiates an asynchronous request to create an IoT rule.
    * If the request is successful, it prints a confirmation message.
    * If an exception occurs, it prints the error message.
    */
   public void createIoTRule(String roleARN, String ruleName, String action) {
       String sql = "SELECT * FROM '" + TOPIC + "'";
       SnsAction action1 = SnsAction.builder()
           .targetArn(action)
           .roleArn(roleARN)
           .build();

       // Create the action.
       Action myAction = Action.builder()
           .sns(action1)
           .build();

       // Create the topic rule payload.
       TopicRulePayload topicRulePayload = TopicRulePayload.builder()
           .sql(sql)
           .actions(myAction)
           .build();

       // Create the topic rule request.
       CreateTopicRuleRequest topicRuleRequest =
CreateTopicRuleRequest.builder()
           .ruleName(ruleName)
           .topicRulePayload(topicRulePayload)
           .build();

       CompletableFuture<CreateTopicRuleResponse> future =
getAsyncClient().createTopicRule(topicRuleRequest);
       future.whenComplete((response, ex) -> {
           if (response != null) {
               System.out.println("IoT Rule created successfully.");
           } else {
               Throwable cause = ex != null ? ex.getCause() : null;
```

```
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
                    System.err.println("Unexpected error: " +
cause.getMessage());
                } else {
                    System.err.println("Failed to create IoT Rule.");
                }
            }
        });

        future.join();
    }

    /**
     * Lists IoT rules asynchronously.
     *
     * This method initiates an asynchronous request to list IoT rules.
     * If the request is successful, it prints the names and ARNs of the rules.
     * If an exception occurs, it prints the error message.
     */
    public void listIoTRules() {
        ListTopicRulesRequest listTopicRulesRequest =
ListTopicRulesRequest.builder().build();
        CompletableFuture<ListTopicRulesResponse> future =
getAsyncClient().listTopicRules(listTopicRulesRequest);
        future.whenComplete((listTopicRulesResponse, ex) -> {
            if (listTopicRulesResponse != null) {
                System.out.println("List of IoT Rules:");
                List<TopicRuleListItem> ruleList =
listTopicRulesResponse.rules();
                for (TopicRuleListItem rule : ruleList) {
                    System.out.println("Rule Name: " + rule.ruleName());
                    System.out.println("Rule ARN: " + rule.ruleArn());
                    System.out.println("--------------");
                }
            } else {
                Throwable cause = ex != null ? ex.getCause() : null;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
```

```
                    System.err.println("Unexpected error: " +
cause.getMessage());
                } else {
                    System.err.println("Failed to list IoT Rules.");
                }
            }
        });

        future.join();
    }

    /**
     * Searches for IoT Things asynchronously based on a query string.
     *
     * @param queryString The query string to search for Things.
     *
     * This method initiates an asynchronous request to search for IoT Things.
     * If the request is successful and Things are found, it prints their IDs.
     * If no Things are found, it prints a message indicating so.
     * If an exception occurs, it prints the error message.
     */
    public void searchThings(String queryString) {
        SearchIndexRequest searchIndexRequest = SearchIndexRequest.builder()
            .queryString(queryString)
            .build();

        CompletableFuture<SearchIndexResponse> future =
getAsyncClient().searchIndex(searchIndexRequest);
        future.whenComplete((searchIndexResponse, ex) -> {
            if (searchIndexResponse != null) {
                // Process the result.
                if (searchIndexResponse.things().isEmpty()) {
                    System.out.println("No things found.");
                } else {
                    searchIndexResponse.things().forEach(thing ->
System.out.println("Thing id found using search is " + thing.thingId()));
                }
            } else {
                Throwable cause = ex != null ? ex.getCause() : null;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
```

```
                    System.err.println("Unexpected error: " +
cause.getMessage());
                } else {
                    System.err.println("Failed to search for IoT Things.");
                }
            }
        });

        future.join();
    }

    /**
     * Detaches a principal (certificate) from an IoT Thing asynchronously.
     *
     * @param thingName The name of the IoT Thing.
     * @param certificateArn The ARN of the certificate to detach.
     *
     * This method initiates an asynchronous request to detach a certificate from
an IoT Thing.
     * If the detachment is successful, it prints a confirmation message.
     * If an exception occurs, it prints the error message.
     */
    public void detachThingPrincipal(String thingName, String certificateArn) {
        DetachThingPrincipalRequest thingPrincipalRequest =
DetachThingPrincipalRequest.builder()
            .principal(certificateArn)
            .thingName(thingName)
            .build();

        CompletableFuture<DetachThingPrincipalResponse> future =
getAsyncClient().detachThingPrincipal(thingPrincipalRequest);
        future.whenComplete((voidResult, ex) -> {
            if (ex == null) {
                System.out.println(certificateArn + " was successfully removed
from " + thingName);
            } else {
                Throwable cause = ex.getCause();
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else {
                    System.err.println("Unexpected error: " + ex.getMessage());
                }
            }
```

```
        });

        future.join();
    }

    /**
     * Deletes a certificate asynchronously.
     *
     * @param certificateArn The ARN of the certificate to delete.
     *
     * This method initiates an asynchronous request to delete a certificate.
     * If the deletion is successful, it prints a confirmation message.
     * If an exception occurs, it prints the error message.
     */
    public void deleteCertificate(String certificateArn) {
        DeleteCertificateRequest certificateProviderRequest =
DeleteCertificateRequest.builder()
            .certificateId(extractCertificateId(certificateArn))
            .build();

        CompletableFuture<DeleteCertificateResponse> future =
getAsyncClient().deleteCertificate(certificateProviderRequest);
        future.whenComplete((voidResult, ex) -> {
            if (ex == null) {
                System.out.println(certificateArn + " was successfully
deleted.");
            } else {
                Throwable cause = ex.getCause();
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else {
                    System.err.println("Unexpected error: " + ex.getMessage());
                }
            }
        });

        future.join();
    }

    /**
     * Deletes an IoT Thing asynchronously.
     *
     * @param thingName The name of the IoT Thing to delete.
```

```
     *
     * This method initiates an asynchronous request to delete an IoT Thing.
     * If the deletion is successful, it prints a confirmation message.
     * If an exception occurs, it prints the error message.
     */
    public void deleteIoTThing(String thingName) {
        DeleteThingRequest deleteThingRequest = DeleteThingRequest.builder()
            .thingName(thingName)
            .build();

        CompletableFuture<DeleteThingResponse> future =
 getAsyncClient().deleteThing(deleteThingRequest);
        future.whenComplete((voidResult, ex) -> {
            if (ex == null) {
                System.out.println("Deleted Thing " + thingName);
            } else {
                Throwable cause = ex.getCause();
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
 cause).awsErrorDetails().errorMessage());
                } else {
                    System.err.println("Unexpected error: " + ex.getMessage());
                }
            }
        });

        future.join();
    }

    // Get the cert Id  from the Cert ARN value.
    private String extractCertificateId(String certificateArn) {
        // Example ARN: arn:aws:iot:region:account-id:cert/certificate-id.
        String[] arnParts = certificateArn.split(":");
        String certificateIdPart = arnParts[arnParts.length - 1];
        return certificateIdPart.substring(certificateIdPart.lastIndexOf("/") +
 1);
    }
}
```

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import aws.sdk.kotlin.services.iot.IotClient
import aws.sdk.kotlin.services.iot.model.Action
import aws.sdk.kotlin.services.iot.model.AttachThingPrincipalRequest
import aws.sdk.kotlin.services.iot.model.AttributePayload
import aws.sdk.kotlin.services.iot.model.CreateThingRequest
import aws.sdk.kotlin.services.iot.model.CreateTopicRuleRequest
import aws.sdk.kotlin.services.iot.model.DeleteCertificateRequest
import aws.sdk.kotlin.services.iot.model.DeleteThingRequest
import aws.sdk.kotlin.services.iot.model.DescribeEndpointRequest
import aws.sdk.kotlin.services.iot.model.DescribeThingRequest
import aws.sdk.kotlin.services.iot.model.DetachThingPrincipalRequest
import aws.sdk.kotlin.services.iot.model.ListTopicRulesRequest
import aws.sdk.kotlin.services.iot.model.SearchIndexRequest
import aws.sdk.kotlin.services.iot.model.SnsAction
import aws.sdk.kotlin.services.iot.model.TopicRulePayload
import aws.sdk.kotlin.services.iot.model.UpdateThingRequest
import aws.sdk.kotlin.services.iotdataplane.IotDataPlaneClient
import aws.sdk.kotlin.services.iotdataplane.model.GetThingShadowRequest
import aws.sdk.kotlin.services.iotdataplane.model.UpdateThingShadowRequest
import aws.smithy.kotlin.runtime.content.ByteStream
import aws.smithy.kotlin.runtime.content.toByteArray
import java.util.Scanner
import java.util.regex.Pattern
import kotlin.system.exitProcess

/**
 * Before running this Kotlin code example, ensure that your development
 environment
 * is set up, including configuring your credentials.
 *
 * For detailed instructions, refer to the following documentation topic:
```

```
 * [Setting Up Your Development Environment](https://docs.aws.amazon.com/sdk-for-
kotlin/latest/developer-guide/setup.html)
 *
 * This code example requires an SNS topic and an IAM Role.
 * Follow the steps in the documentation to set up these resources:
 *
 * - [Creating an SNS Topic](https://docs.aws.amazon.com/sns/latest/dg/sns-
getting-started.html#step-create-topic)
 * - [Creating an IAM Role](https://docs.aws.amazon.com/IAM/latest/UserGuide/
id_roles_create.html)
 */

val DASHES = String(CharArray(80)).replace("\u0000", "-")
val TOPIC = "your-iot-topic"

suspend fun main(args: Array<String>) {
    val usage =
        """
        Usage:
            <roleARN> <snsAction>

        Where:
            roleARN - The ARN of an IAM role that has permission to work with AWS
 IOT.
            snsAction  - An ARN of an SNS topic.

        """.trimIndent()

    if (args.size != 2) {
        println(usage)
        exitProcess(1)
    }

    var thingName: String
    val roleARN = args[0]
    val snsAction = args[1]
    val scanner = Scanner(System.`in`)

    println(DASHES)
    println("Welcome to the AWS IoT example scenario.")
    println(
        """
        This example program demonstrates various interactions with the AWS
 Internet of Things (IoT) Core service.
```

```
        The program guides you through a series of steps, including creating an
IoT thing, generating a device certificate,
        updating the thing with attributes, and so on.

        It utilizes the AWS SDK for Kotlin and incorporates functionality for
creating and managing IoT things, certificates, rules,
        shadows, and performing searches. The program aims to showcase AWS IoT
capabilities and provides a comprehensive example for
        developers working with AWS IoT in a Kotlin environment.
        """.trimIndent(),
    )

    print("Press Enter to continue...")
    scanner.nextLine()
    println(DASHES)

    println(DASHES)
    println("1. Create an AWS IoT thing.")
    println(
        """
        An AWS IoT thing represents a virtual entity in the AWS IoT service that
can be associated with a physical device.
        """.trimIndent(),
    )
    // Prompt the user for input.
    print("Enter thing name: ")
    thingName = scanner.nextLine()
    createIoTThing(thingName)
    describeThing(thingName)
    println(DASHES)

    println(DASHES)
    println("2. Generate a device certificate.")
    println(
        """
        A device certificate performs a role in securing the communication
between devices (things) and the AWS IoT platform.
        """.trimIndent(),
    )

    print("Do you want to create a certificate for $thingName? (y/n)")
    val certAns = scanner.nextLine()
    var certificateArn: String? = ""
```

```
    if (certAns != null && certAns.trim { it <= ' ' }.equals("y", ignoreCase =
true)) {
        certificateArn = createCertificate()
        println("Attach the certificate to the AWS IoT thing.")
        attachCertificateToThing(thingName, certificateArn)
    } else {
        println("A device certificate was not created.")
    }
    println(DASHES)

    println(DASHES)
    println("3. Update an AWS IoT thing with Attributes.")
    println(
        """
        IoT thing attributes, represented as key-value pairs, offer a pivotal
advantage in facilitating efficient data
        management and retrieval within the AWS IoT ecosystem.
        """.trimIndent(),
    )
    print("Press Enter to continue...")
    scanner.nextLine()
    updateThing(thingName)
    println(DASHES)

    println(DASHES)
    println("4. Return a unique endpoint specific to the Amazon Web Services
account.")
    println(
        """
        An IoT Endpoint refers to a specific URL or Uniform Resource Locator that
serves as the entry point for communication between IoT devices and the AWS IoT
service.
        """.trimIndent(),
    )
    print("Press Enter to continue...")
    scanner.nextLine()
    val endpointUrl = describeEndpoint()
    println(DASHES)

    println(DASHES)
    println("5. List your AWS IoT certificates")
    print("Press Enter to continue...")
    scanner.nextLine()
    if (certificateArn!!.isNotEmpty()) {
```

```
        listCertificates()
    } else {
        println("You did not create a certificates. Skipping this step.")
    }
    println(DASHES)

    println(DASHES)
    println("6. Create an IoT shadow that refers to a digital representation or
virtual twin of a physical IoT device")
    println(
        """
        A thing shadow refers to a feature that enables you to create a virtual
representation, or "shadow,"
        of a physical device or thing. The thing shadow allows you to synchronize
and control the state of a device between
        the cloud and the device itself. and the AWS IoT service. For example,
you can write and retrieve JSON data from a thing shadow.

        """.trimIndent(),
    )
    print("Press Enter to continue...")
    scanner.nextLine()
    updateShawdowThing(thingName)
    println(DASHES)

    println(DASHES)
    println("7. Write out the state information, in JSON format.")
    print("Press Enter to continue...")
    scanner.nextLine()
    getPayload(thingName)
    println(DASHES)

    println(DASHES)
    println("8. Creates a rule")
    println(
        """
        Creates a rule that is an administrator-level action.
        Any user who has permission to create rules will be able to access data
processed by the rule.
        """.trimIndent(),
    )
    print("Enter Rule name: ")
    val ruleName = scanner.nextLine()
    createIoTRule(roleARN, ruleName, snsAction)
```

```
    println(DASHES)

    println(DASHES)
    println("9. List your rules.")
    print("Press Enter to continue...")
    scanner.nextLine()
    listIoTRules()
    println(DASHES)

    println(DASHES)
    println("10. Search things using the name.")
    print("Press Enter to continue...")
    scanner.nextLine()
    val queryString = "thingName:$thingName"
    searchThings(queryString)
    println(DASHES)

    println(DASHES)
    if (certificateArn.length > 0) {
        print("Do you want to detach and delete the certificate for $thingName?
(y/n)")
        val delAns = scanner.nextLine()
        if (delAns != null && delAns.trim { it <= ' ' }.equals("y", ignoreCase =
true)) {
            println("11. You selected to detach amd delete the certificate.")
            print("Press Enter to continue...")
            scanner.nextLine()
            detachThingPrincipal(thingName, certificateArn)
            deleteCertificate(certificateArn)
        } else {
            println("11. You selected not to delete the certificate.")
        }
    } else {
        println("11. You did not create a certificate so there is nothing to
delete.")
    }
    println(DASHES)

    println(DASHES)
    println("12. Delete the AWS IoT thing.")
    print("Do you want to delete the IoT thing? (y/n)")
    val delAns = scanner.nextLine()
    if (delAns != null && delAns.trim { it <= ' ' }.equals("y", ignoreCase =
true)) {
```

```
        deleteIoTThing(thingName)
    } else {
        println("The IoT thing was not deleted.")
    }
    println(DASHES)

    println(DASHES)
    println("The AWS IoT workflow has successfully completed.")
    println(DASHES)
}

suspend fun deleteIoTThing(thingNameVal: String) {
    val deleteThingRequest =
        DeleteThingRequest {
            thingName = thingNameVal
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.deleteThing(deleteThingRequest)
        println("Deleted $thingNameVal")
    }
}

suspend fun deleteCertificate(certificateArn: String) {
    val certificateProviderRequest =
        DeleteCertificateRequest {
            certificateId = extractCertificateId(certificateArn)
        }
    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.deleteCertificate(certificateProviderRequest)
        println("$certificateArn was successfully deleted.")
    }
}

private fun extractCertificateId(certificateArn: String): String? {
    // Example ARN: arn:aws:iot:region:account-id:cert/certificate-id.
    val arnParts = certificateArn.split(":".toRegex()).dropLastWhile
 { it.isEmpty() }.toTypedArray()
    val certificateIdPart = arnParts[arnParts.size - 1]
    return certificateIdPart.substring(certificateIdPart.lastIndexOf("/") + 1)
}

suspend fun detachThingPrincipal(
    thingNameVal: String,
```

```
    certificateArn: String,
) {
    val thingPrincipalRequest =
        DetachThingPrincipalRequest {
            principal = certificateArn
            thingName = thingNameVal
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.detachThingPrincipal(thingPrincipalRequest)
        println("$certificateArn was successfully removed from $thingNameVal")
    }
}

suspend fun searchThings(queryStringVal: String?) {
    val searchIndexRequest =
        SearchIndexRequest {
            queryString = queryStringVal
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        val searchIndexResponse = iotClient.searchIndex(searchIndexRequest)
        if (searchIndexResponse.things?.isEmpty() == true) {
            println("No things found.")
        } else {
            searchIndexResponse.things
                ?.forEach { thing -> println("Thing id found using search is
 ${thing.thingId}") }
        }
    }
}

suspend fun listIoTRules() {
    val listTopicRulesRequest = ListTopicRulesRequest {}

    IotClient { region = "us-east-1" }.use { iotClient ->
        val listTopicRulesResponse =
 iotClient.listTopicRules(listTopicRulesRequest)
        println("List of IoT rules:")
        val ruleList = listTopicRulesResponse.rules
        ruleList?.forEach { rule ->
            println("Rule name: ${rule.ruleName}")
            println("Rule ARN: ${rule.ruleArn}")
            println("--------------")
```

```
        }
    }
}

suspend fun createIoTRule(
    roleARNVal: String?,
    ruleNameVal: String?,
    action: String?,
) {
    val sqlVal = "SELECT * FROM '$TOPIC '"
    val action1 =
        SnsAction {
            targetArn = action
            roleArn = roleARNVal
        }

    val myAction =
        Action {
            sns = action1
        }

    val topicRulePayloadVal =
        TopicRulePayload {
            sql = sqlVal
            actions = listOf(myAction)
        }

    val topicRuleRequest =
        CreateTopicRuleRequest {
            ruleName = ruleNameVal
            topicRulePayload = topicRulePayloadVal
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.createTopicRule(topicRuleRequest)
        println("IoT rule created successfully.")
    }
}

suspend fun getPayload(thingNameVal: String?) {
    val getThingShadowRequest =
        GetThingShadowRequest {
            thingName = thingNameVal
        }
```

```
    IotDataPlaneClient { region = "us-east-1" }.use { iotPlaneClient ->
        val getThingShadowResponse =
 iotPlaneClient.getThingShadow(getThingShadowRequest)
        val payload = getThingShadowResponse.payload
        val payloadString = payload?.let { java.lang.String(it, Charsets.UTF_8) }
        println("Received shadow data: $payloadString")
    }
}

suspend fun listCertificates() {
    IotClient { region = "us-east-1" }.use { iotClient ->
        val response = iotClient.listCertificates()
        val certList = response.certificates
        certList?.forEach { cert ->
            println("Cert id: ${cert.certificateId}")
            println("Cert Arn: ${cert.certificateArn}")
        }
    }
}

suspend fun describeEndpoint(): String? {
    val request = DescribeEndpointRequest {}
    IotClient { region = "us-east-1" }.use { iotClient ->
        val endpointResponse = iotClient.describeEndpoint(request)
        val endpointUrl: String? = endpointResponse.endpointAddress
        val exString: String = getValue(endpointUrl)
        val fullEndpoint = "https://$exString-ats.iot.us-east-1.amazonaws.com"
        println("Full endpoint URL: $fullEndpoint")
        return fullEndpoint
    }
}

private fun getValue(input: String?): String {
    // Define a regular expression pattern for extracting the subdomain.
    val pattern = Pattern.compile("^(.*?)\\.iot\\.us-east-1\\.amazonaws\\.com")

    // Match the pattern against the input string.
    val matcher = pattern.matcher(input)

    // Check if a match is found.
    if (matcher.find()) {
        val subdomain = matcher.group(1)
        println("Extracted subdomain: $subdomain")
```

```
        return subdomain
    } else {
        println("No match found")
    }
    return ""
}

suspend fun updateThing(thingNameVal: String?) {
    val newLocation = "Office"
    val newFirmwareVersion = "v2.0"
    val attMap: MutableMap<String, String> = HashMap()
    attMap["location"] = newLocation
    attMap["firmwareVersion"] = newFirmwareVersion

    val attributePayloadVal =
        AttributePayload {
            attributes = attMap
        }

    val updateThingRequest =
        UpdateThingRequest {
            thingName = thingNameVal
            attributePayload = attributePayloadVal
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        // Update the IoT thing attributes.
        iotClient.updateThing(updateThingRequest)
        println("$thingNameVal attributes updated successfully.")
    }
}

suspend fun updateShawdowThing(thingNameVal: String?) {
    // Create the thing shadow state document.
    val stateDocument = "{\"state\":{\"reported\":{\"temperature\":25, \"humidity
\":50}}}"
    val byteStream: ByteStream = ByteStream.fromString(stateDocument)
    val byteArray: ByteArray = byteStream.toByteArray()

    val updateThingShadowRequest =
        UpdateThingShadowRequest {
            thingName = thingNameVal
            payload = byteArray
        }
```

```
    IotDataPlaneClient { region = "us-east-1" }.use { iotPlaneClient ->
        iotPlaneClient.updateThingShadow(updateThingShadowRequest)
        println("The thing shadow was updated successfully.")
    }
}

suspend fun attachCertificateToThing(
    thingNameVal: String?,
    certificateArn: String?,
) {
    val principalRequest =
        AttachThingPrincipalRequest {
            thingName = thingNameVal
            principal = certificateArn
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.attachThingPrincipal(principalRequest)
        println("Certificate attached to $thingNameVal successfully.")
    }
}

suspend fun describeThing(thingNameVal: String) {
    val thingRequest =
        DescribeThingRequest {
            thingName = thingNameVal
        }

    // Print Thing details.
    IotClient { region = "us-east-1" }.use { iotClient ->
        val describeResponse = iotClient.describeThing(thingRequest)
        println("Thing details:")
        println("Thing name: ${describeResponse.thingName}")
        println("Thing ARN:  ${describeResponse.thingArn}")
    }
}

suspend fun createCertificate(): String? {
    IotClient { region = "us-east-1" }.use { iotClient ->
        val response = iotClient.createKeysAndCertificate()
        val certificatePem = response.certificatePem
        val certificateArn = response.certificateArn
```

```
        // Print the details.
        println("\nCertificate:")
        println(certificatePem)
        println("\nCertificate ARN:")
        println(certificateArn)
        return certificateArn
    }
}

suspend fun createIoTThing(thingNameVal: String) {
    val createThingRequest =
        CreateThingRequest {
            thingName = thingNameVal
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.createThing(createThingRequest)
        println("Created $thingNameVal}")
    }
}
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Aktionen zur AWS IoT Verwendung AWS SDKs

Die folgenden Codebeispiele zeigen, wie Sie einzelne AWS IoT Aktionen mit ausführen können AWS SDKs. Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen des Codes finden.

Die folgenden Beispiele enthalten nur die am häufigsten verwendeten Aktionen. Eine vollständige Liste finden Sie in der AWS IoT -API-Referenz.

Beispiele

- Verwendung AttachThingPrincipal mit einem AWS SDK oder CLI
- Verwendung CreateKeysAndCertificate mit einem AWS SDK oder CLI
- Verwendung CreateThing mit einem AWS SDK oder CLI
- Verwendung CreateTopicRule mit einem AWS SDK oder CLI

- Verwendung DeleteCertificate mit einem AWS SDK oder CLI
- Verwendung DeleteThing mit einem AWS SDK oder CLI
- Verwendung DeleteTopicRule mit einem AWS SDK oder CLI
- Verwendung DescribeEndpoint mit einem AWS SDK oder CLI
- Verwendung DescribeThing mit einem AWS SDK oder CLI
- Verwendung DetachThingPrincipal mit einem AWS SDK oder CLI
- Verwendung ListCertificates mit einem AWS SDK oder CLI
- Verwendung ListThings mit einem AWS SDK oder CLI
- Verwendung SearchIndex mit einem AWS SDK oder CLI
- Verwendung UpdateIndexingConfiguration mit einem AWS SDK oder CLI
- Verwendung UpdateThing mit einem AWS SDK oder CLI

## Verwendung **`AttachThingPrincipal`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `AttachThingPrincipal` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Attach a principal to an AWS IoT thing.
/*!
  \param principal: A principal to attach.
  \param thingName: The name for the thing.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::attachThingPrincipal(const Aws::String &principal,
                                       const Aws::String &thingName,
                                       const Aws::Client::ClientConfiguration
 &clientConfiguration) {
```

```
    Aws::IoT::IoTClient client(clientConfiguration);
    Aws::IoT::Model::AttachThingPrincipalRequest request;
    request.SetPrincipal(principal);
    request.SetThingName(thingName);
    Aws::IoT::Model::AttachThingPrincipalOutcome outcome =
 client.AttachThingPrincipal(
            request);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully attached principal to thing." << std::endl;
    }
    else {
        std::cerr << "Failed to attach principal to thing." <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie AttachThingPrincipalin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Um ein Zertifikat an dein Ding anzuhängen

Im folgenden `attach-thing-principal` Beispiel wird ein Zertifikat an das MyTemperatureSensor Ding angehängt. Das Zertifikat wird durch einen ARN identifiziert. Sie finden den ARN für ein Zertifikat in der AWS IoT-Konsole.

```
aws iot attach-thing-principal \
    --thing-name MyTemperatureSensor \
    --principal arn:aws:iot:us-
west-2:123456789012:cert/2e1eb273792174ec2b9bf4e9b37e6c6c692345499506002a35159767055278e8
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter How to Manage Things with the Registry im AWS IoT Developers Guide.

- Einzelheiten zur API finden Sie AttachThingPrincipalin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   /**
    * Attaches a certificate to an IoT Thing asynchronously.
    *
    * @param thingName The name of the IoT Thing.
    * @param certificateArn The ARN of the certificate to attach.
    *
    * This method initiates an asynchronous request to attach a certificate to
an IoT Thing.
    * If the request is successful, it prints a confirmation message and
additional information about the Thing.
    * If an exception occurs, it prints the error message.
    */
   public void attachCertificateToThing(String thingName, String certificateArn)
{
       AttachThingPrincipalRequest principalRequest =
AttachThingPrincipalRequest.builder()
           .thingName(thingName)
           .principal(certificateArn)
           .build();

       CompletableFuture<AttachThingPrincipalResponse> future =
getAsyncClient().attachThingPrincipal(principalRequest);
       future.whenComplete((attachResponse, ex) -> {
           if (attachResponse != null &&
attachResponse.sdkHttpResponse().isSuccessful()) {
               System.out.println("Certificate attached to Thing
successfully.");

               // Print additional information about the Thing.
               describeThing(thingName);
           } else {
               Throwable cause = ex != null ? ex.getCause() : null;
```

```
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
                    System.err.println("Unexpected error: " +
cause.getMessage());
                } else {
                    System.err.println("Failed to attach certificate to Thing.
HTTP Status Code: " +
                        attachResponse.sdkHttpResponse().statusCode());
                }
            }
        });

        future.join();
    }
```

- Einzelheiten zur API finden Sie AttachThingPrincipalin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun attachCertificateToThing(
    thingNameVal: String?,
    certificateArn: String?,
) {
    val principalRequest =
        AttachThingPrincipalRequest {
            thingName = thingNameVal
            principal = certificateArn
        }
```

```
    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.attachThingPrincipal(principalRequest)
        println("Certificate attached to $thingNameVal successfully.")
    }
}
```

- Einzelheiten zur API finden Sie AttachThingPrincipalin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`CreateKeysAndCertificate`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `CreateKeysAndCertificate` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Create keys and certificate for an Aws IoT device.
//! This routine will save certificates and keys to an output folder, if
 provided.
/*!
  \param outputFolder: Location for storing output in files, ignored when string
 is empty.
  \param certificateARNResult: A string to receive the ARN of the created
 certificate.
  \param certificateID: A string to receive the ID of the created certificate.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::createKeysAndCertificate(const Aws::String &outputFolder,
```

```
                                                Aws::String &certificateARNResult,
                                                Aws::String &certificateID,
                                                const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient client(clientConfiguration);
    Aws::IoT::Model::CreateKeysAndCertificateRequest
 createKeysAndCertificateRequest;

    Aws::IoT::Model::CreateKeysAndCertificateOutcome outcome =
            client.CreateKeysAndCertificate(createKeysAndCertificateRequest);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully created a certificate and keys" << std::endl;
        certificateARNResult = outcome.GetResult().GetCertificateArn();
        certificateID = outcome.GetResult().GetCertificateId();
        std::cout << "Certificate ARN: " << certificateARNResult << ",
 certificate ID: "
                  << certificateID << std::endl;

        if (!outputFolder.empty()) {
            std::cout << "Writing certificate and keys to the folder '" <<
 outputFolder
                      << "'." << std::endl;
            std::cout << "Be sure these files are stored securely." << std::endl;

            Aws::String certificateFilePath = outputFolder + "/
certificate.pem.crt";
            std::ofstream certificateFile(certificateFilePath);
            if (!certificateFile.is_open()) {
                std::cerr << "Error opening certificate file, '" <<
 certificateFilePath
                          << "'."
                          << std::endl;
                return false;
            }
            certificateFile << outcome.GetResult().GetCertificatePem();
            certificateFile.close();

            const Aws::IoT::Model::KeyPair &keyPair =
 outcome.GetResult().GetKeyPair();

            Aws::String privateKeyFilePath = outputFolder + "/private.pem.key";
            std::ofstream privateKeyFile(privateKeyFilePath);
            if (!privateKeyFile.is_open()) {
```

```
                std::cerr << "Error opening private key file, '" <<
 privateKeyFilePath
                          << "'."
                          << std::endl;
                return false;
            }
            privateKeyFile << keyPair.GetPrivateKey();
            privateKeyFile.close();

            Aws::String publicKeyFilePath = outputFolder + "/public.pem.key";
            std::ofstream publicKeyFile(publicKeyFilePath);
            if (!publicKeyFile.is_open()) {
                std::cerr << "Error opening public key file, '" <<
 publicKeyFilePath
                          << "'."
                          << std::endl;
                return false;
            }
            publicKeyFile << keyPair.GetPublicKey();
        }
    }
    else {
        std::cerr << "Error creating keys and certificate: "
                  << outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie CreateKeysAndCertificatein der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Um ein RSA-Schlüsselpaar zu erstellen und ein X.509-Zertifikat auszustellen

Im Folgenden `create-keys-and-certificate` wird ein 2048-Bit-RSA-Schlüsselpaar erstellt und ein X.509-Zertifikat unter Verwendung des ausgegebenen öffentlichen Schlüssels

ausgestellt. Da dies das einzige Mal ist, dass AWS IoT den privaten Schlüssel für dieses Zertifikat bereitstellt, sollten Sie es an einem sicheren Ort aufbewahren.

```
aws iot create-keys-and-certificate \
    --certificate-pem-outfile "myTest.cert.pem" \
    --public-key-outfile "myTest.public.key" \
    --private-key-outfile "myTest.private.key"
```

Ausgabe:

```
{
    "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/9894ba17925e663f1d29c23af4582b8e3b7619c31f3fbd93adcb51ae54b83dc2
    "certificateId":
 "9894ba17925e663f1d29c23af4582b8e3b7619c31f3fbd93adcb51ae54b83dc2",
    "certificatePem": "
-----BEGIN CERTIFICATE-----
MIICiTCCEXAMPLE6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgEXAMPLEAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSEXAMPLE2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYEXAMPLEb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCEXAMPLEJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDAEXAMPLEsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEXAMPLE25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+aEXAMPLE
EXAMPLEfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZEXAMPLELG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAEXAMPLEWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9qEXAMPLEyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDEXAMPLEBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----\n",
    "keyPair": {
        "PublicKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkEXAMPLEQEFAAOCAQ8AMIIBCgKCAQEAEXAMPLE1nnyJwKSMHw4h\nMMEXAMPLEuuN/
dMAS3fyce8DW/4+EXAMPLEyjmoF/YVF/gHr99VEEXAMPLE5VF13\n59VK7cEXAMPLE67GK+y
+jikqXOgHh/xJTwo
+sGpWEXAMPLEDz18xOd2ka4tCzuWEXAMPLEahJbYkCPUBSU8opVkR7qkEXAMPLE1DR6sx2HocliOOLtu6Fkw91swQ
\GB3ZPrNh0PzQYvjUStZeccyNCx2EXAMPLEvp9mQOUXP6plfgxwKRX2fEXAMPLEDa
\nhJLXkX3rHU2xbxJSq7D+XEXAMPLEcw+LyFhI5mgFRl88eGdsAEXAMPLElnI9EesG\nFQIDAQAB
\n-----END PUBLIC KEY-----\n",
        "PrivateKey": "-----BEGIN RSA PRIVATE KEY-----\nkey omittted for security
 reasons\n-----END RSA PRIVATE KEY-----\n"
```

```
    }
}
```

Weitere Informationen finden Sie unter Erstellen und Registrieren eines AWS IoT-Gerätezertifikats im AWS IoT Developer Guide.

- Einzelheiten zur API finden Sie CreateKeysAndCertificatein der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   /**
    * Creates an IoT certificate asynchronously.
    *
    * @return The ARN of the created certificate.
    * <p>
    * This method initiates an asynchronous request to create an IoT
certificate.
    * If the request is successful, it prints the certificate details and
returns the certificate ARN.
    * If an exception occurs, it prints the error message.
    */
   public String createCertificate() {
       CompletableFuture<CreateKeysAndCertificateResponse> future =
getAsyncClient().createKeysAndCertificate();
       final String[] certificateArn = {null};
       future.whenComplete((response, ex) -> {
           if (response != null) {
               String certificatePem = response.certificatePem();
               certificateArn[0] = response.certificateArn();

               // Print the details.
               System.out.println("\nCertificate:");
               System.out.println(certificatePem);
               System.out.println("\nCertificate ARN:");
```

```
                System.out.println(certificateArn[0]);

            } else {
                Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else {
                    System.err.println("Unexpected error: " +
cause.getMessage());
                }
            }
        });

        future.join();
        return certificateArn[0];
    }
```

- Einzelheiten zur API finden Sie CreateKeysAndCertificatein der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun createCertificate(): String? {
    IotClient { region = "us-east-1" }.use { iotClient ->
        val response = iotClient.createKeysAndCertificate()
        val certificatePem = response.certificatePem
        val certificateArn = response.certificateArn

        // Print the details.
        println("\nCertificate:")
```

```
        println(certificatePem)
        println("\nCertificate ARN:")
        println(certificateArn)
        return certificateArn
    }
}
```

- Einzelheiten zur API finden Sie CreateKeysAndCertificatein der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`CreateThing`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `CreateThing` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Create an AWS IoT thing.
/*!
  \param thingName: The name for the thing.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::createThing(const Aws::String &thingName,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::CreateThingRequest createThingRequest;
    createThingRequest.SetThingName(thingName);
```

```
    Aws::IoT::Model::CreateThingOutcome outcome = iotClient.CreateThing(
            createThingRequest);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully created thing " << thingName << std::endl;
    }
    else {
        std::cerr << "Failed to create thing " << thingName << ": " <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie CreateThingin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Beispiel 1: Um einen Ding-Datensatz in der Registrierung zu erstellen

Das folgende `create-thing` Beispiel erstellt einen Eintrag für ein Gerät in der AWS IoT-Dingregistrierung.

```
aws iot create-thing \
    --thing-name SampleIoTThing
```

Ausgabe:

```
{
    "thingName": "SampleIoTThing",
    "thingArn": "arn:aws:iot:us-west-2: 123456789012:thing/SampleIoTThing",
    "thingId": " EXAMPLE1-90ab-cdef-fedc-ba987EXAMPLE "
}
```

Beispiel 2: Um ein Ding zu definieren, das einem Dingtyp zugeordnet ist

Im folgenden `create-thing` Beispiel wird ein Ding mit dem angegebenen Dingtyp und seinen Attributen erstellt.

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

Ausgabe:

```
{
    "thingName": "MyLightBulb",
    "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyLightBulb",
    "thingId": "40da2e73-c6af-406e-b415-15acae538797"
}
```

Weitere Informationen finden Sie unter How to Manage Things with the Registry and Thing Types im AWS IoT Developers Guide.

- Einzelheiten zur API finden Sie CreateThingin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /**
     * Creates an IoT Thing with the specified name asynchronously.
     *
     * @param thingName The name of the IoT Thing to create.
     *
     * This method initiates an asynchronous request to create an IoT Thing with
the specified name.
     * If the request is successful, it prints the name of the thing and its ARN
value.
     * If an exception occurs, it prints the error message.
     */
    public void createIoTThing(String thingName) {
        CreateThingRequest createThingRequest = CreateThingRequest.builder()
```

```
            .thingName(thingName)
            .build();

        CompletableFuture<CreateThingResponse> future =
getAsyncClient().createThing(createThingRequest);
        future.whenComplete((createThingResponse, ex) -> {
            if (createThingResponse != null) {
                System.out.println(thingName + " was successfully created. The
ARN value is " + createThingResponse.thingArn());
            } else {
                Throwable cause = ex.getCause();
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else {
                    System.err.println("Unexpected error: " +
cause.getMessage());
                }
            }
        });

        future.join();
    }
```

- Einzelheiten zur API finden Sie CreateThingin der AWS SDK for Java 2.x API-Referenz.

## Kotlin

### SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun createIoTThing(thingNameVal: String) {
    val createThingRequest =
        CreateThingRequest {
            thingName = thingNameVal
        }
```

```
    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.createThing(createThingRequest)
        println("Created $thingNameVal}")
    }
}
```

- Einzelheiten zur API finden Sie CreateThingin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`CreateTopicRule`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `CreateTopicRule` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Create an AWS IoT rule with an SNS topic as the target.
/*!
  \param ruleName: The name for the rule.
  \param snsTopic: The SNS topic ARN for the action.
  \param sql: The SQL statement used to query the topic.
  \param roleARN: The IAM role ARN for the action.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool
AwsDoc::IoT::createTopicRule(const Aws::String &ruleName,
                             const Aws::String &snsTopicARN, const Aws::String
 &sql,
```

```
                            const Aws::String &roleARN,
                            const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);

    Aws::IoT::Model::CreateTopicRuleRequest request;
    request.SetRuleName(ruleName);

    Aws::IoT::Model::SnsAction snsAction;
    snsAction.SetTargetArn(snsTopicARN);
    snsAction.SetRoleArn(roleARN);

    Aws::IoT::Model::Action action;
    action.SetSns(snsAction);

    Aws::IoT::Model::TopicRulePayload topicRulePayload;
    topicRulePayload.SetSql(sql);
    topicRulePayload.SetActions({action});

    request.SetTopicRulePayload(topicRulePayload);
    auto outcome = iotClient.CreateTopicRule(request);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully created topic rule " << ruleName << "." <<
 std::endl;
    }
    else {
        std::cerr << "Error creating topic rule " << ruleName << ": " <<
                  outcome.GetError().GetMessage() << std::endl;
    }
    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie CreateTopicRulein der AWS SDK für C++ API-Referenz.

## CLI

### AWS CLI

#### Um eine Regel zu erstellen, die eine Amazon SNS SNS-Warnung sendet

Das folgende `create-topic-rule` Beispiel erstellt eine Regel, die eine Amazon SNS SNS-Nachricht sendet, wenn die Bodenfeuchtewerte, wie sie in einem Geräteschatten gefunden wurden, niedrig sind.

```
aws iot create-topic-rule \
    --rule-name "LowMoistureRule" \
    --topic-rule-payload file://plant-rule.json
```

Für das Beispiel muss der folgende JSON-Code in einer Datei mit dem Namen `plant-rule.json` gespeichert werden:

```
{
    "sql": "SELECT * FROM '$aws/things/MyRPi/shadow/update/accepted' WHERE
 state.reported.moisture = 'low'\n",
    "description": "Sends an alert whenever soil moisture level readings are too
 low.",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [{
            "sns": {
                "targetArn": "arn:aws:sns:us-
west-2:123456789012:MyRPiLowMoistureTopic",
                "roleArn": "arn:aws:iam::123456789012:role/service-role/
MyRPiLowMoistureTopicRole",
                "messageFormat": "RAW"
            }
    }]
}
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter Erstellen einer AWS IoT-Regel im AWS IoT-Entwicklerhandbuch.

- Einzelheiten zur API finden Sie CreateTopicRulein der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /**
     * Creates an IoT rule asynchronously.
     *
     * @param roleARN The ARN of the IAM role that grants access to the rule's
actions.
     * @param ruleName The name of the IoT rule.
     * @param action The ARN of the action to perform when the rule is triggered.
     *
     * This method initiates an asynchronous request to create an IoT rule.
     * If the request is successful, it prints a confirmation message.
     * If an exception occurs, it prints the error message.
     */
    public void createIoTRule(String roleARN, String ruleName, String action) {
        String sql = "SELECT * FROM '" + TOPIC + "'";
        SnsAction action1 = SnsAction.builder()
            .targetArn(action)
            .roleArn(roleARN)
            .build();

        // Create the action.
        Action myAction = Action.builder()
            .sns(action1)
            .build();

        // Create the topic rule payload.
        TopicRulePayload topicRulePayload = TopicRulePayload.builder()
            .sql(sql)
            .actions(myAction)
            .build();

        // Create the topic rule request.
```

```
        CreateTopicRuleRequest topicRuleRequest =
CreateTopicRuleRequest.builder()
            .ruleName(ruleName)
            .topicRulePayload(topicRulePayload)
            .build();

        CompletableFuture<CreateTopicRuleResponse> future =
getAsyncClient().createTopicRule(topicRuleRequest);
        future.whenComplete((response, ex) -> {
            if (response != null) {
                System.out.println("IoT Rule created successfully.");
            } else {
                Throwable cause = ex != null ? ex.getCause() : null;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
                    System.err.println("Unexpected error: " +
cause.getMessage());
                } else {
                    System.err.println("Failed to create IoT Rule.");
                }
            }
        });

        future.join();
    }
```

- Einzelheiten zur API finden Sie CreateTopicRulein der AWS SDK for Java 2.x API-Referenz.

## Kotlin

### SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun createIoTRule(
```

```
    roleARNVal: String?,
    ruleNameVal: String?,
    action: String?,
) {
    val sqlVal = "SELECT * FROM '$TOPIC '"
    val action1 =
        SnsAction {
            targetArn = action
            roleArn = roleARNVal
        }

    val myAction =
        Action {
            sns = action1
        }

    val topicRulePayloadVal =
        TopicRulePayload {
            sql = sqlVal
            actions = listOf(myAction)
        }

    val topicRuleRequest =
        CreateTopicRuleRequest {
            ruleName = ruleNameVal
            topicRulePayload = topicRulePayloadVal
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.createTopicRule(topicRuleRequest)
        println("IoT rule created successfully.")
    }
}
```

- Einzelheiten zur API finden Sie CreateTopicRulein der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`DeleteCertificate`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `DeleteCertificate` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Delete a certificate.
/*!
  \param certificateID: The ID of a certificate.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::deleteCertificate(const Aws::String &certificateID,
                                    const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);

    Aws::IoT::Model::DeleteCertificateRequest request;
    request.SetCertificateId(certificateID);

    Aws::IoT::Model::DeleteCertificateOutcome outcome =
 iotClient.DeleteCertificate(
            request);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted certificate " << certificateID <<
 std::endl;
    }
    else {
        std::cerr << "Error deleting certificate " << certificateID << ": " <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
```

```
}
```

- Einzelheiten zur API finden Sie DeleteCertificatein der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Um ein Gerätezertifikat zu löschen

Im folgenden `delete-certificate` Beispiel wird das Gerätezertifikat mit der angegebenen ID gelöscht.

```
aws iot delete-certificate \
    --certificate-
id c0c57bbc8baaf4631a9a0345c957657f5e710473e3ddbee1428d216d54d53ac9
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie DeleteCertificatein der AWS IoT-API-Referenz.

- Einzelheiten zur API finden Sie DeleteCertificatein der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /**
     * Deletes a certificate asynchronously.
     *
     * @param certificateArn The ARN of the certificate to delete.
     *
     * This method initiates an asynchronous request to delete a certificate.
     * If the deletion is successful, it prints a confirmation message.
```

```
     * If an exception occurs, it prints the error message.
     */
    public void deleteCertificate(String certificateArn) {
        DeleteCertificateRequest certificateProviderRequest =
DeleteCertificateRequest.builder()
            .certificateId(extractCertificateId(certificateArn))
            .build();

        CompletableFuture<DeleteCertificateResponse> future =
getAsyncClient().deleteCertificate(certificateProviderRequest);
        future.whenComplete((voidResult, ex) -> {
            if (ex == null) {
                System.out.println(certificateArn + " was successfully
deleted.");
            } else {
                Throwable cause = ex.getCause();
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else {
                    System.err.println("Unexpected error: " + ex.getMessage());
                }
            }
        });

        future.join();
    }
```

- Einzelheiten zur API finden Sie DeleteCertificatein der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun deleteCertificate(certificateArn: String) {
```

```
    val certificateProviderRequest =
        DeleteCertificateRequest {
            certificateId = extractCertificateId(certificateArn)
        }
    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.deleteCertificate(certificateProviderRequest)
        println("$certificateArn was successfully deleted.")
    }
}
```

- Einzelheiten zur API finden Sie DeleteCertificatein der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`DeleteThing`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `DeleteThing` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Delete an AWS IoT thing.
/*!
  \param thingName: The name for the thing.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::deleteThing(const Aws::String &thingName,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
```

```
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::DeleteThingRequest request;
    request.SetThingName(thingName);
    const auto outcome = iotClient.DeleteThing(request);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted thing " << thingName << std::endl;
    }
    else {
        std::cerr << "Error deleting thing " << thingName << ": " <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie DeleteThingin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Um detaillierte Informationen zu einer Sache anzuzeigen

Das folgende `delete-thing` Beispiel löscht eine Sache aus der AWS IoT-Registrierung für Ihr AWS Konto.

as iot delete-thing --thing-name“ FourthBulb

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter How to Manage Things with the Registry im AWS IoT Developers Guide.

- Einzelheiten zur API finden Sie DeleteThingin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /**
     * Deletes an IoT Thing asynchronously.
     *
     * @param thingName The name of the IoT Thing to delete.
     *
     * This method initiates an asynchronous request to delete an IoT Thing.
     * If the deletion is successful, it prints a confirmation message.
     * If an exception occurs, it prints the error message.
     */
    public void deleteIoTThing(String thingName) {
        DeleteThingRequest deleteThingRequest = DeleteThingRequest.builder()
            .thingName(thingName)
            .build();

        CompletableFuture<DeleteThingResponse> future =
getAsyncClient().deleteThing(deleteThingRequest);
        future.whenComplete((voidResult, ex) -> {
            if (ex == null) {
                System.out.println("Deleted Thing " + thingName);
            } else {
                Throwable cause = ex.getCause();
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else {
                    System.err.println("Unexpected error: " + ex.getMessage());
                }
            }
        });

        future.join();
    }
```

- Einzelheiten zur API finden Sie DeleteThingin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun deleteIoTThing(thingNameVal: String) {
    val deleteThingRequest =
        DeleteThingRequest {
            thingName = thingNameVal
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.deleteThing(deleteThingRequest)
        println("Deleted $thingNameVal")
    }
}
```

- Einzelheiten zur API finden Sie DeleteThingin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`DeleteTopicRule`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `DeleteTopicRule` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Delete an AWS IoT rule.
/*!
  \param ruleName: The name for the rule.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::deleteTopicRule(const Aws::String &ruleName,
                                  const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::DeleteTopicRuleRequest request;
    request.SetRuleName(ruleName);

    Aws::IoT::Model::DeleteTopicRuleOutcome outcome = iotClient.DeleteTopicRule(
            request);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted rule " << ruleName << std::endl;
    }
    else {
        std::cerr << "Failed to delete rule " << ruleName <<
                  ": " << outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie DeleteTopicRulein der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

So löschen Sie eine Regel

Im folgenden `delete-topic-rule` Beispiel wird die angegebene Regel gelöscht.

```
aws iot delete-topic-rule \
    --rule-name "LowMoistureRule"
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter Löschen einer Regel im AWS IoT Developers Guide.

- Einzelheiten zur API finden Sie DeleteTopicRulein der AWS CLI Befehlsreferenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`DescribeEndpoint`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `DescribeEndpoint` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Describe the endpoint specific to the AWS account making the call.
/*!
  \param endpointResult: String to receive the endpoint result.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
```

```
 */
bool AwsDoc::IoT::describeEndpoint(Aws::String &endpointResult,
                                   const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::String endpoint;
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::DescribeEndpointRequest describeEndpointRequest;
    describeEndpointRequest.SetEndpointType(
            "iot:Data-ATS"); // Recommended endpoint type.

    Aws::IoT::Model::DescribeEndpointOutcome outcome =
 iotClient.DescribeEndpoint(
            describeEndpointRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully described endpoint." << std::endl;
        endpointResult = outcome.GetResult().GetEndpointAddress();
    }
    else {
        std::cerr << "Error describing endpoint" <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie DescribeEndpointin der AWS SDK für C++ API-Referenz.

## CLI

### AWS CLI

#### Beispiel 1: Um Ihren aktuellen AWS Endpunkt zu ermitteln

Im folgenden `describe-endpoint` Beispiel wird der AWS Standardendpunkt abgerufen, auf den alle Befehle angewendet werden.

```
aws iot describe-endpoint
```

Ausgabe:

```
{
    "endpointAddress": "abc123defghijk.iot.us-west-2.amazonaws.com"
}
```

Weitere Informationen finden Sie DescribeEndpointim AWS IoT Developer Guide.

Beispiel 2: Um Ihren ATS-Endpunkt zu ermitteln

Im folgenden `describe-endpoint` Beispiel wird der Amazon Trust Services (ATS) -Endpunkt abgerufen.

```
aws iot describe-endpoint \
    --endpoint-type iot:Data-ATS
```

Ausgabe:

```
{
    "endpointAddress": "abc123defghijk-ats.iot.us-west-2.amazonaws.com"
}
```

Weitere Informationen finden Sie unter X.509-Zertifikate und AWS IoT im AWS IoT Developer Guide.

- Einzelheiten zur API finden Sie DescribeEndpointin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /**
     * Describes the endpoint of the IoT service asynchronously.
     *
```

```
     * @return A CompletableFuture containing the full endpoint URL.
     *
     * This method initiates an asynchronous request to describe the endpoint of
 the IoT service.
     * If the request is successful, it prints and returns the full endpoint URL.
     * If an exception occurs, it prints the error message.
     */
    public String describeEndpoint() {
        CompletableFuture<DescribeEndpointResponse> future =
 getAsyncClient().describeEndpoint(DescribeEndpointRequest.builder().endpointType("iot:Da
ATS").build());
        final String[] result = {null};

        future.whenComplete((endpointResponse, ex) -> {
            if (endpointResponse != null) {
                String endpointUrl = endpointResponse.endpointAddress();
                String exString = getValue(endpointUrl);
                String fullEndpoint = "https://" + exString + "-ats.iot.us-
east-1.amazonaws.com";

                System.out.println("Full Endpoint URL: " + fullEndpoint);
                result[0] = fullEndpoint;
            } else {
                Throwable cause = (ex instanceof CompletionException) ?
 ex.getCause() : ex;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
 cause).awsErrorDetails().errorMessage());
                } else {
                    System.err.println("Unexpected error: " +
 cause.getMessage());
                }
            }
        });

        future.join();
        return result[0];
    }
```

- Einzelheiten zur API finden Sie DescribeEndpointin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun describeEndpoint(): String? {
    val request = DescribeEndpointRequest {}
    IotClient { region = "us-east-1" }.use { iotClient ->
        val endpointResponse = iotClient.describeEndpoint(request)
        val endpointUrl: String? = endpointResponse.endpointAddress
        val exString: String = getValue(endpointUrl)
        val fullEndpoint = "https://$exString-ats.iot.us-east-1.amazonaws.com"
        println("Full endpoint URL: $fullEndpoint")
        return fullEndpoint
    }
}
```

- Einzelheiten zur API finden Sie DescribeEndpointin der API-Referenz zum AWS SDK für Kotlin.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
async fn show_address(client: &Client, endpoint_type: &str) -> Result<(), Error>
 {
    let resp = client
```

```
        .describe_endpoint()
        .endpoint_type(endpoint_type)
        .send()
        .await?;

    println!("Endpoint address: {}", resp.endpoint_address.unwrap());

    println!();

    Ok(())
}
```

- Einzelheiten zur API finden Sie DescribeEndpointin der API-Referenz zum AWS SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`DescribeThing`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `DescribeThing` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Describe an AWS IoT thing.
/*!
  \param thingName: The name for the thing.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
```

```
bool AwsDoc::IoT::describeThing(const Aws::String &thingName,
                                const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);

    Aws::IoT::Model::DescribeThingRequest request;
    request.SetThingName(thingName);

    Aws::IoT::Model::DescribeThingOutcome outcome =
 iotClient.DescribeThing(request);

    if (outcome.IsSuccess()) {
        const Aws::IoT::Model::DescribeThingResult &result = outcome.GetResult();
        std::cout << "Retrieved thing '" << result.GetThingName() << "'" <<
 std::endl;
        std::cout << "thingArn: " << result.GetThingArn() << std::endl;
        std::cout << result.GetAttributes().size() << " attribute(s) retrieved"
                  << std::endl;
        for (const auto &attribute: result.GetAttributes()) {
            std::cout << "  attribute: " << attribute.first << "=" <<
 attribute.second
                      << std::endl;
        }
    }
    else {
        std::cerr << "Error describing thing " << thingName << ": " <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie DescribeThingin der AWS SDK für C++ API-Referenz.

## CLI

### AWS CLI

#### Um detaillierte Informationen zu einer Sache anzuzeigen

Im folgenden `describe-thing` Beispiel werden Informationen zu einer Sache (einem Gerät) angezeigt, die in der AWS IoT-Registrierung für Ihr AWS Konto definiert ist.

als iot describe-thing --thing-name“ MyLightBulb

Ausgabe:

```
{
    "defaultClientId": "MyLightBulb",
    "thingName": "MyLightBulb",
    "thingId": "40da2e73-c6af-406e-b415-15acae538797",
    "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyLightBulb",
    "thingTypeName": "LightBulb",
    "attributes": {
        "model": "123",
        "wattage": "75"
    },
    "version": 1
}
```

Weitere Informationen finden Sie unter How to Manage Things with the Registry im AWS IoT Developers Guide.

- Einzelheiten zur API finden Sie DescribeThingin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /**
     * Describes an IoT Thing asynchronously.
     *
     * @param thingName The name of the IoT Thing.
     *
     * This method initiates an asynchronous request to describe an IoT Thing.
     * If the request is successful, it prints the Thing details.
     * If an exception occurs, it prints the error message.
     */
```

```
    private void describeThing(String thingName) {
        DescribeThingRequest thingRequest = DescribeThingRequest.builder()
            .thingName(thingName)
            .build();

        CompletableFuture<DescribeThingResponse> future =
getAsyncClient().describeThing(thingRequest);
        future.whenComplete((describeResponse, ex) -> {
            if (describeResponse != null) {
                System.out.println("Thing Details:");
                System.out.println("Thing Name: " +
describeResponse.thingName());
                System.out.println("Thing ARN: " + describeResponse.thingArn());
            } else {
                Throwable cause = ex != null ? ex.getCause() : null;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
                    System.err.println("Unexpected error: " +
cause.getMessage());
                } else {
                    System.err.println("Failed to describe Thing.");
                }
            }
        });

        future.join();
    }
```

- Einzelheiten zur API finden Sie DescribeThingin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun describeThing(thingNameVal: String) {
    val thingRequest =
        DescribeThingRequest {
            thingName = thingNameVal
        }

    // Print Thing details.
    IotClient { region = "us-east-1" }.use { iotClient ->
        val describeResponse = iotClient.describeThing(thingRequest)
        println("Thing details:")
        println("Thing name: ${describeResponse.thingName}")
        println("Thing ARN:  ${describeResponse.thingArn}")
    }
}
```

- Einzelheiten zur API finden Sie DescribeThingin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`DetachThingPrincipal`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `DetachThingPrincipal` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Detach a principal from an AWS IoT thing.
/*!
  \param principal: A principal to detach.
  \param thingName: The name for the thing.
```

```
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::detachThingPrincipal(const Aws::String &principal,
                                       const Aws::String &thingName,
                                       const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);

    Aws::IoT::Model::DetachThingPrincipalRequest detachThingPrincipalRequest;
    detachThingPrincipalRequest.SetThingName(thingName);
    detachThingPrincipalRequest.SetPrincipal(principal);

    Aws::IoT::Model::DetachThingPrincipalOutcome outcome =
 iotClient.DetachThingPrincipal(
            detachThingPrincipalRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully detached principal " << principal << " from
 thing "
                  << thingName << std::endl;
    }
    else {
        std::cerr << "Failed to detach principal " << principal << " from thing "
                  << thingName << ": "
                  << outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie DetachThingPrincipalin der AWS SDK für C++ API-Referenz.

## CLI

### AWS CLI

#### Um ein Zertifikat/einen Prinzipal von einer Sache zu trennen

Im folgenden `detach-thing-principal` Beispiel wird ein Zertifikat, das einen Prinzipal darstellt, aus dem angegebenen Objekt entfernt.

```
aws iot detach-thing-principal \
    --thing-name "MyLightBulb" \
    --principal "arn:aws:iot:us-
west-2:123456789012:cert/604c48437a57b7d5fc5d137c5be75011c6ee67c9a6943683a1acb4b1626bac36
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter How to Manage Things with the Registry im AWS IoT Developers Guide.

- Einzelheiten zur API finden Sie DetachThingPrincipalin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   /**
    * Detaches a principal (certificate) from an IoT Thing asynchronously.
    *
    * @param thingName The name of the IoT Thing.
    * @param certificateArn The ARN of the certificate to detach.
    *
    * This method initiates an asynchronous request to detach a certificate from
an IoT Thing.
    * If the detachment is successful, it prints a confirmation message.
    * If an exception occurs, it prints the error message.
    */
   public void detachThingPrincipal(String thingName, String certificateArn) {
       DetachThingPrincipalRequest thingPrincipalRequest =
DetachThingPrincipalRequest.builder()
           .principal(certificateArn)
           .thingName(thingName)
           .build();
```

```
        CompletableFuture<DetachThingPrincipalResponse> future =
 getAsyncClient().detachThingPrincipal(thingPrincipalRequest);
        future.whenComplete((voidResult, ex) -> {
            if (ex == null) {
                System.out.println(certificateArn + " was successfully removed
 from " + thingName);
            } else {
                Throwable cause = ex.getCause();
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
 cause).awsErrorDetails().errorMessage());
                } else {
                    System.err.println("Unexpected error: " + ex.getMessage());
                }
            }
        });

        future.join();
    }
```

- Einzelheiten zur API finden Sie DetachThingPrincipalin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun detachThingPrincipal(
    thingNameVal: String,
    certificateArn: String,
) {
    val thingPrincipalRequest =
        DetachThingPrincipalRequest {
            principal = certificateArn
```

```
            thingName = thingNameVal
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        iotClient.detachThingPrincipal(thingPrincipalRequest)
        println("$certificateArn was successfully removed from $thingNameVal")
    }
}
```

- Einzelheiten zur API finden Sie DetachThingPrincipalin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`ListCertificates`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `ListCertificates` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! List certificates registered in the AWS account making the call.
/*!
   \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::listCertificates(
        const Aws::Client::ClientConfiguration &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::ListCertificatesRequest request;
```

```
    Aws::Vector<Aws::IoT::Model::Certificate> allCertificates;
    Aws::String marker; // Used to paginate results.
    do {
        if (!marker.empty()) {
            request.SetMarker(marker);
        }

        Aws::IoT::Model::ListCertificatesOutcome outcome =
iotClient.ListCertificates(
                request);

        if (outcome.IsSuccess()) {
            const Aws::IoT::Model::ListCertificatesResult &result =
outcome.GetResult();
            marker = result.GetNextMarker();
            allCertificates.insert(allCertificates.end(),
                                   result.GetCertificates().begin(),
                                   result.GetCertificates().end());
        }
        else {
            std::cerr << "Error: " << outcome.GetError().GetMessage() <<
std::endl;
            return false;
        }
    } while (!marker.empty());

    std::cout << allCertificates.size() << " certificate(s) found." << std::endl;

    for (auto &certificate: allCertificates) {
        std::cout << "Certificate ID: " << certificate.GetCertificateId() <<
std::endl;
        std::cout << "Certificate ARN: " << certificate.GetCertificateArn()
                  << std::endl;
        std::cout << std::endl;
    }

    return true;
}
```

- Einzelheiten zur API finden Sie ListCertificatesin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Beispiel 1: Um die in Ihrem AWS Konto registrierten Zertifikate aufzulisten

Das folgende `list-certificates` Beispiel listet alle in Ihrem Konto registrierten Zertifikate auf. Wenn Sie mehr als das standardmäßige Paging-Limit von 25 haben, können Sie den `nextMarker` Antwortwert aus diesem Befehl verwenden und ihn dem nächsten Befehl übergeben, um den nächsten Stapel von Ergebnissen zu erhalten. Wiederholen Sie den Vorgang, bis kein Wert `nextMarker` zurückgegeben wird.

```
aws iot list-certificates
```

Ausgabe:

```
{
    "certificates": [
        {
            "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/604c48437a57b7d5fc5d137c5be75011c6ee67c9a6943683a1acb4b1626bac36
            "certificateId":
 "604c48437a57b7d5fc5d137c5be75011c6ee67c9a6943683a1acb4b1626bac36",
            "status": "ACTIVE",
            "creationDate": 1556810537.617
        },
        {
            "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/262a1ac8a7d8aa72f6e96e365480f7313aa9db74b8339ec65d34dc3074e1c31e
            "certificateId":
 "262a1ac8a7d8aa72f6e96e365480f7313aa9db74b8339ec65d34dc3074e1c31e",
            "status": "ACTIVE",
            "creationDate": 1546447050.885
        },
        {
            "certificateArn": "arn:aws:iot:us-west-2:123456789012:cert/
b193ab7162c0fadca83246d24fa090300a1236fe58137e121b011804d8ac1d6b",
            "certificateId":
 "b193ab7162c0fadca83246d24fa090300a1236fe58137e121b011804d8ac1d6b",
            "status": "ACTIVE",
            "creationDate": 1546292258.322
        },
```

```
        {
            "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/7aebeea3845d14a44ec80b06b8b78a89f3f8a706974b8b34d18f5adf0741db42
            "certificateId":
 "7aebeea3845d14a44ec80b06b8b78a89f3f8a706974b8b34d18f5adf0741db42",
            "status": "ACTIVE",
            "creationDate": 1541457693.453
        },
        {
            "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/54458aa39ebb3eb39c91ffbbdcc3a6ca1c7c094d1644b889f735a6fc2cd9a7e3
            "certificateId":
 "54458aa39ebb3eb39c91ffbbdcc3a6ca1c7c094d1644b889f735a6fc2cd9a7e3",
            "status": "ACTIVE",
            "creationDate": 1541113568.611
        },
        {
            "certificateArn": "arn:aws:iot:us-
west-2:123456789012:cert/4f0ba725787aa94d67d2fca420eca022242532e8b3c58e7465c7778b443fd65e
            "certificateId":
 "4f0ba725787aa94d67d2fca420eca022242532e8b3c58e7465c7778b443fd65e",
            "status": "ACTIVE",
            "creationDate": 1541022751.983
        }
    ]
}
```

- Einzelheiten zur API finden Sie ListCertificatesin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /**
     * Lists all certificates asynchronously.
     *
```

```
     * This method initiates an asynchronous request to list all certificates.
     * If the request is successful, it prints the certificate IDs and ARNs.
     * If an exception occurs, it prints the error message.
     */
    public void listCertificates() {
        CompletableFuture<ListCertificatesResponse> future =
getAsyncClient().listCertificates();
        future.whenComplete((response, ex) -> {
            if (response != null) {
                List<Certificate> certList = response.certificates();
                for (Certificate cert : certList) {
                    System.out.println("Cert id: " + cert.certificateId());
                    System.out.println("Cert Arn: " + cert.certificateArn());
                }
            } else {
                Throwable cause = ex != null ? ex.getCause() : null;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
                    System.err.println("Unexpected error: " +
cause.getMessage());
                } else {
                    System.err.println("Failed to list certificates.");
                }
            }
        });

        future.join();
    }
```

- Einzelheiten zur API finden Sie ListCertificatesin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun listCertificates() {
    IotClient { region = "us-east-1" }.use { iotClient ->
        val response = iotClient.listCertificates()
        val certList = response.certificates
        certList?.forEach { cert ->
            println("Cert id: ${cert.certificateId}")
            println("Cert Arn: ${cert.certificateArn}")
        }
    }
}
```

- Einzelheiten zur API finden Sie ListCertificatesin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`ListThings`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `ListThings` verwendet wird.

CLI

AWS CLI

Beispiel 1: Um alle Dinge in der Registrierung aufzulisten

Das folgende `list-things` Beispiel listet die Dinge (Geräte) auf, die in der AWS IoT-Registrierung für Ihr AWS Konto definiert sind.

```
aws iot list-things
```

Ausgabe:

```
{
    "things": [
        {
            "thingName": "ThirdBulb",
            "thingTypeName": "LightBulb",
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/ThirdBulb",
```

```
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "version": 2
        },
        {
            "thingName": "MyOtherLightBulb",
            "thingTypeName": "LightBulb",
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/
MyOtherLightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "version": 3
        },
        {
            "thingName": "MyLightBulb",
            "thingTypeName": "LightBulb",
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyLightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "version": 1
        },
        {
        "thingName": "SampleIoTThing",
        "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/SampleIoTThing",
        "attributes": {},
        "version": 1
        }
    ]
}
```

Beispiel 2: Um die definierten Dinge aufzulisten, die ein bestimmtes Attribut haben

Im folgenden `list-things` Beispiel wird eine Liste von Dingen angezeigt, für die ein Attribut benannt ist`wattage`.

```
aws iot list-things \
    --attribute-name wattage
```

Ausgabe:

```
{
    "things": [
        {
            "thingName": "MyLightBulb",
            "thingTypeName": "LightBulb",
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyLightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "version": 1
        },
        {
            "thingName": "MyOtherLightBulb",
            "thingTypeName": "LightBulb",
            "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/
MyOtherLightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "version": 3
        }
    ]
}
```

Weitere Informationen finden Sie unter How to Manage Things with the Registry im AWS IoT Developers Guide.

- Einzelheiten zur API finden Sie ListThingsin der AWS CLI Befehlsreferenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
async fn show_things(client: &Client) -> Result<(), Error> {
    let resp = client.list_things().send().await?;

    println!("Things:");

    for thing in resp.things.unwrap() {
        println!(
            "  Name:  {}",
            thing.thing_name.as_deref().unwrap_or_default()
        );
        println!(
            "  Type:  {}",
            thing.thing_type_name.as_deref().unwrap_or_default()
        );
        println!(
            "  ARN:   {}",
            thing.thing_arn.as_deref().unwrap_or_default()
        );
        println!();
    }

    println!();

    Ok(())
}
```

- Einzelheiten zur API finden Sie ListThingsin der API-Referenz zum AWS SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`SearchIndex`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `SearchIndex` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Query the AWS IoT fleet index.
//! For query information, see https://docs.aws.amazon.com/iot/latest/
developerguide/query-syntax.html
/*!
  \param: query: The query string.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::searchIndex(const Aws::String &query,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);

    Aws::IoT::Model::SearchIndexRequest request;
    request.SetQueryString(query);

    Aws::Vector<Aws::IoT::Model::ThingDocument> allThingDocuments;
    Aws::String nextToken; // Used for pagination.
    do {
        if (!nextToken.empty()) {
            request.SetNextToken(nextToken);
        }

        Aws::IoT::Model::SearchIndexOutcome outcome =
 iotClient.SearchIndex(request);

        if (outcome.IsSuccess()) {
            const Aws::IoT::Model::SearchIndexResult &result =
 outcome.GetResult();
            allThingDocuments.insert(allThingDocuments.end(),
                                     result.GetThings().cbegin(),
                                     result.GetThings().cend());
```

```
            nextToken = result.GetNextToken();

        }
        else {
            std::cerr << "Error in SearchIndex: " <<
 outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    } while (!nextToken.empty());

    std::cout << allThingDocuments.size() << " thing document(s) found." <<
 std::endl;
    for (const auto thingDocument: allThingDocuments) {
        std::cout << "  Thing name: " << thingDocument.GetThingName() << "."
                  << std::endl;
    }
    return true;
}
```

- Einzelheiten zur API finden Sie SearchIndexin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Um den Dingindex abzufragen

Im folgenden `search-index` Beispiel wird der `AWS_Things` Index nach Dingen abgefragt, die den Typ haben`LightBulb`.

```
aws iot search-index \
    --index-name "AWS_Things" \
    --query-string "thingTypeName:LightBulb"
```

Ausgabe:

```
{
    "things": [
        {
            "thingName": "MyLightBulb",
```

```
            "thingId": "40da2e73-c6af-406e-b415-15acae538797",
            "thingTypeName": "LightBulb",
            "thingGroupNames": [
                "LightBulbs",
                "DeadBulbs"
            ],
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "connectivity": {
                "connected": false
            }
        },
        {
            "thingName": "ThirdBulb",
            "thingId": "615c8455-33d5-40e8-95fd-3ee8b24490af",
            "thingTypeName": "LightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "connectivity": {
                "connected": false
            }
        },
        {
            "thingName": "MyOtherLightBulb",
            "thingId": "6dae0d3f-40c1-476a-80c4-1ed24ba6aa11",
            "thingTypeName": "LightBulb",
            "attributes": {
                "model": "123",
                "wattage": "75"
            },
            "connectivity": {
                "connected": false
            }
        }
    ]
}
```

Weitere Informationen finden Sie unter Managing Thing Indexing im AWS IoT Developer Guide.

- Einzelheiten zur API finden Sie SearchIndexin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /**
     * Searches for IoT Things asynchronously based on a query string.
     *
     * @param queryString The query string to search for Things.
     *
     * This method initiates an asynchronous request to search for IoT Things.
     * If the request is successful and Things are found, it prints their IDs.
     * If no Things are found, it prints a message indicating so.
     * If an exception occurs, it prints the error message.
     */
    public void searchThings(String queryString) {
        SearchIndexRequest searchIndexRequest = SearchIndexRequest.builder()
            .queryString(queryString)
            .build();

        CompletableFuture<SearchIndexResponse> future =
getAsyncClient().searchIndex(searchIndexRequest);
        future.whenComplete((searchIndexResponse, ex) -> {
            if (searchIndexResponse != null) {
                // Process the result.
                if (searchIndexResponse.things().isEmpty()) {
                    System.out.println("No things found.");
                } else {
                    searchIndexResponse.things().forEach(thing ->
System.out.println("Thing id found using search is " + thing.thingId()));
                }
            } else {
                Throwable cause = ex != null ? ex.getCause() : null;
                if (cause instanceof IotException) {
```

```
                    System.err.println(((IotException)
 cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
                    System.err.println("Unexpected error: " +
 cause.getMessage());
                } else {
                    System.err.println("Failed to search for IoT Things.");
                }
            }
        });

        future.join();
    }
```

- Einzelheiten zur API finden Sie SearchIndexin der AWS SDK for Java 2.x API-Referenz.

## Kotlin

### SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun searchThings(queryStringVal: String?) {
    val searchIndexRequest =
        SearchIndexRequest {
            queryString = queryStringVal
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        val searchIndexResponse = iotClient.searchIndex(searchIndexRequest)
        if (searchIndexResponse.things?.isEmpty() == true) {
            println("No things found.")
        } else {
            searchIndexResponse.things
                ?.forEach { thing -> println("Thing id found using search is
 ${thing.thingId}") }
        }
```

```
    }
}
```

- Einzelheiten zur API finden Sie SearchIndexin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`UpdateIndexingConfiguration`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `UpdateIndexingConfiguration` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Update the indexing configuration.
/*!
  \param thingIndexingConfiguration: A ThingIndexingConfiguration object which is
 ignored if not set.
  \param thingGroupIndexingConfiguration: A ThingGroupIndexingConfiguration
 object which is ignored if not set.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::updateIndexingConfiguration(
        const Aws::IoT::Model::ThingIndexingConfiguration
 &thingIndexingConfiguration,
        const Aws::IoT::Model::ThingGroupIndexingConfiguration
 &thingGroupIndexingConfiguration,
        const Aws::Client::ClientConfiguration &clientConfiguration) {
    Aws::IoT::IoTClient iotClient(clientConfiguration);
```

```
    Aws::IoT::Model::UpdateIndexingConfigurationRequest request;

    if (thingIndexingConfiguration.ThingIndexingModeHasBeenSet()) {
        request.SetThingIndexingConfiguration(thingIndexingConfiguration);
    }

    if (thingGroupIndexingConfiguration.ThingGroupIndexingModeHasBeenSet()) {

 request.SetThingGroupIndexingConfiguration(thingGroupIndexingConfiguration);
    }

    Aws::IoT::Model::UpdateIndexingConfigurationOutcome outcome =
 iotClient.UpdateIndexingConfiguration(
            request);

    if (outcome.IsSuccess()) {
        std::cout << "UpdateIndexingConfiguration succeeded." << std::endl;
    }
    else {
        std::cerr << "UpdateIndexingConfiguration failed."
                  << outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie UpdateIndexingConfigurationin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Um die Indizierung von Dingen zu aktivieren

Im folgenden `update-indexing-configuration` Beispiel wird die Dingindizierung aktiviert, sodass die Suche nach Registrierungsdaten, Shadow-Daten und dem Status der Ding-Konnektivität mithilfe des AWS_Things-Index unterstützt wird.

```
aws iot update-indexing-configuration
```

```
    --thing-indexing-
configuration thingIndexingMode=REGISTRY_AND_SHADOW,thingConnectivityIndexingMode=STATUS
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter Managing Thing Indexing im AWS IoT Developers Guide.

- Einzelheiten zur API finden Sie UpdateIndexingConfigurationin der AWS CLI Befehlsreferenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

## Verwendung **`UpdateThing`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `UpdateThing` verwendet wird.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Update an AWS IoT thing with attributes.
/*!
  \param thingName: The name for the thing.
  \param attributeMap: A map of key/value attributes/
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::IoT::updateThing(const Aws::String &thingName,
                              const std::map<Aws::String, Aws::String>
 &attributeMap,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
```

```
    Aws::IoT::IoTClient iotClient(clientConfiguration);
    Aws::IoT::Model::UpdateThingRequest request;
    request.SetThingName(thingName);
    Aws::IoT::Model::AttributePayload attributePayload;
    for (const auto &attribute: attributeMap) {
        attributePayload.AddAttributes(attribute.first, attribute.second);
    }
    request.SetAttributePayload(attributePayload);

    Aws::IoT::Model::UpdateThingOutcome outcome = iotClient.UpdateThing(request);
    if (outcome.IsSuccess()) {
        std::cout << "Successfully updated thing " << thingName << std::endl;
    }
    else {
        std::cerr << "Failed to update thing " << thingName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie UpdateThingin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Um ein Ding einem Dingtyp zuzuordnen

Das folgende `update-thing` Beispiel ordnet ein Ding in der AWS IoT-Registrierung einem Dingtyp zu. Wenn Sie die Zuordnung vornehmen, geben Sie Werte für die Attribute an, die durch den Dingtyp definiert sind.

```
aws iot update-thing \
    --thing-name "MyOtherLightBulb" \
    --thing-type-name "LightBulb" \
    --attribute-payload "{"attributes": {"wattage":"75", "model":"123"}}"
```

Dieser Befehl erzeugt keine Ausgabe. Verwenden Sie den `describe-thing` Befehl, um das Ergebnis zu sehen.

Weitere Informationen finden Sie unter Thing Types im AWS IoT Developers Guide.

- Einzelheiten zur API finden Sie UpdateThingin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   /**
    * Updates the shadow of an IoT Thing asynchronously.
    *
    * @param thingName The name of the IoT Thing.
    *
    * This method initiates an asynchronous request to update the shadow of an
IoT Thing.
    * If the request is successful, it prints a confirmation message.
    * If an exception occurs, it prints the error message.
    */
   public void updateShadowThing(String thingName) {
       // Create Thing Shadow State Document.
       String stateDocument = "{\"state\":{\"reported\":{\"temperature\":25,
\"humidity\":50}}}";
       SdkBytes data = SdkBytes.fromString(stateDocument,
StandardCharsets.UTF_8);
       UpdateThingShadowRequest updateThingShadowRequest =
UpdateThingShadowRequest.builder()
           .thingName(thingName)
           .payload(data)
           .build();

       CompletableFuture<UpdateThingShadowResponse> future =
getAsyncDataPlaneClient().updateThingShadow(updateThingShadowRequest);
       future.whenComplete((updateResponse, ex) -> {
           if (updateResponse != null) {
               System.out.println("Thing Shadow updated successfully.");
           } else {
```

```
                Throwable cause = ex != null ? ex.getCause() : null;
                if (cause instanceof IotException) {
                    System.err.println(((IotException)
 cause).awsErrorDetails().errorMessage());
                } else if (cause != null) {
                    System.err.println("Unexpected error: " +
 cause.getMessage());
                } else {
                    System.err.println("Failed to update Thing Shadow.");
                }
            }
        });

        future.join();
    }
```

- Einzelheiten zur API finden Sie UpdateThingin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun updateThing(thingNameVal: String?) {
    val newLocation = "Office"
    val newFirmwareVersion = "v2.0"
    val attMap: MutableMap<String, String> = HashMap()
    attMap["location"] = newLocation
    attMap["firmwareVersion"] = newFirmwareVersion

    val attributePayloadVal =
        AttributePayload {
            attributes = attMap
        }

    val updateThingRequest =
```

```
        UpdateThingRequest {
            thingName = thingNameVal
            attributePayload = attributePayloadVal
        }

    IotClient { region = "us-east-1" }.use { iotClient ->
        // Update the IoT thing attributes.
        iotClient.updateThing(updateThingRequest)
        println("$thingNameVal attributes updated successfully.")
    }
}
```

- Einzelheiten zur API finden Sie UpdateThingin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS IoT mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

# AWS IoT-Kontingente

Weitere Informationen finden SieAWS IoTKontingente imAWS– Allgemeine Referenzaus.

- FürAWS IoT CoreInformationen zu Quoten finden Sie unterAWS IoT CoreEndpunkte und Kontingenteaus.
- FürAWS IoT Device ManagementInformationen zu Quoten finden Sie unterAWS IoT Device ManagementEndpunkte und Kontingenteaus.
- FürAWS IoT Device DefenderInformationen zu Quoten finden Sie unterAWS IoT Device DefenderEndpunkte und Kontingenteaus.

# AWS IoT Core – Preise

Informationen zur AWS IoT Core Preisgestaltung finden Sie auf der AWSMarketingseite und im AWSPreisrechner.

- Informationen zu den AWS IoT Core Preisen finden Sie unter AWS IoT CorePreise.
- Informationen zur Schätzung der Kosten Ihrer Architektenlösung finden Sie unter AWSPreisrechner.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.