
AWS IoT

Guida per gli sviluppatori



AWS IoT: Guida per gli sviluppatori

Copyright © 2019 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

| | |
|--|-----|
| Che cos'è AWS IoT | 1 |
| Componenti di AWS IoT | 1 |
| Nozioni di base su AWS IoT | 2 |
| Accesso a AWS IoT | 2 |
| Servizi correlati | 3 |
| Funzionamento di AWS IoT | 3 |
| Nozioni di base su AWS IoT | 5 |
| Accesso alla console AWS IoT | 5 |
| Registrazione di un dispositivo nel registro | 6 |
| Creazione e attivazione di un certificato del dispositivo | 15 |
| Creazione di una policy AWS IoT | 17 |
| Collegamento di una policy AWS IoT a un certificato del dispositivo | 20 |
| Collegamento di un certificato a un oggetto | 22 |
| Configurazione del dispositivo | 25 |
| Visualizzazione di messaggi MQTT del dispositivo con il client MQTT AWS IoT | 25 |
| Configurazione e test delle regole | 27 |
| Creazione di un argomento SNS | 27 |
| Sottoscrizione di un argomento Amazon SNS | 29 |
| Creazione di una regola | 30 |
| Test della regola Amazon SNS | 36 |
| Fasi successive | 37 |
| Creazione e monitoraggio di un processo AWS IoT | 37 |
| Connessione del dispositivo ad AWS IoT | 37 |
| Esecuzione del processo di esempio | 37 |
| Creazione di un documento del processo | 38 |
| Creazione di un processo | 38 |
| Esecuzione del processo in un dispositivo | 45 |
| Monitoraggio dello stato del processo con eventi di processo e di esecuzione di processi | 46 |
| Tutorial sulle regole AWS IoT | 50 |
| Creazione di una regola Amazon DynamoDB | 50 |
| Test di una regola Amazon DynamoDB | 60 |
| Creazione di una regola AWS Lambda | 61 |
| Creare una funzione Lambda | 61 |
| Test della funzione Lambda | 66 |
| Creare una regola Lambda | 68 |
| Test della regola Lambda | 78 |
| Risoluzione dei problemi relativi alle regole Lambda | 79 |
| Creazione di una regola Amazon SNS | 80 |
| AWS IoTTutorial SDK | 89 |
| Prerequisiti | 89 |
| Creazione di un oggetto AWS IoT per Raspberry Pi | 89 |
| Uso dell'SDK AWS IoT per Embedded C | 104 |
| Configurazione dell'ambiente di runtime per l'SDK AWS IoT per Embedded C | 104 |
| Configurazione delle app di esempio | 104 |
| Esecuzione delle applicazioni di esempio | 106 |
| Uso dell'SDK di dispositivo AWS IoT per JavaScript | 107 |
| Configurazione dell'ambiente di runtime per l'SDK di dispositivo AWS IoT per JavaScript | 107 |
| Installazione dell'SDK di dispositivo AWS IoT per JavaScript | 107 |
| Preparazione dell'esecuzione delle applicazioni di esempio | 107 |
| Esecuzione delle applicazioni di esempio | 108 |
| Tutorial AWS IoT aggiuntivi | 110 |
| Esempio di irrigatura AWS IoT | 110 |
| Modulo 1: Configurazione di AWS IoT e invio dei dati con il computer di sviluppo | 111 |
| Modulo 2: Invio di dati con il Raspberry Pi | 132 |

| | |
|---|-----|
| Pulizia | 151 |
| Fasi successive | 155 |
| Gestione di dispositivi con AWS IoT | 157 |
| Come gestire gli oggetti con il registro | 157 |
| Creare un oggetto | 157 |
| Elenco di oggetti | 158 |
| Ricerca di oggetti | 158 |
| Aggiornamento di un oggetto | 159 |
| Eliminazione di un oggetto | 160 |
| Collegamento di un principale a un oggetto | 160 |
| Scollegamento di un principale da un oggetto | 160 |
| Tipi di oggetti | 160 |
| Creazione di un tipo di oggetto | 161 |
| Elenco di tipi di oggetti | 161 |
| Descrizione di un tipo di oggetto | 161 |
| Associazione di un tipo di oggetto a un oggetto | 162 |
| Impostazione di un tipo di oggetto come obsoleto | 162 |
| Eliminazione di un tipo di oggetto | 163 |
| Gruppi di oggetti | 163 |
| Creazione di un gruppo di oggetti | 164 |
| Descrizione di un gruppo di oggetti | 165 |
| Aggiunta di un oggetto a un gruppo di oggetti | 166 |
| Rimozione di un oggetto da un gruppo di oggetti | 166 |
| Elenco di oggetti in un gruppo di oggetti | 166 |
| Elenco di gruppi di oggetti | 167 |
| Elenco dei gruppi per un oggetto | 168 |
| Aggiornamento di un gruppo di oggetti | 169 |
| Eliminazione di un gruppo di oggetti | 169 |
| Collegamento di una policy a un gruppo di oggetti | 170 |
| Scollegamento di una policy da un gruppo di oggetti | 170 |
| Elenco di policy collegate a un gruppo di oggetti | 170 |
| Elenco di gruppi per una policy | 171 |
| Recupero delle policy valide per un oggetto | 171 |
| Test dell'autorizzazione per le operazioni MQTT | 172 |
| Gruppo di oggetti dinamici | 173 |
| Creazione di un gruppo di oggetti dinamico | 174 |
| Descrizione di un gruppo di oggetti dinamico | 174 |
| Aggiornamento di un gruppo di oggetti dinamico | 175 |
| Eliminazione di un gruppo di oggetti dinamico | 175 |
| Restrizioni e conflitti | 176 |
| Tagging delle risorse AWS IoT | 178 |
| Nozioni di base sui tag | 178 |
| Restrizioni e limitazioni di tag | 179 |
| Utilizzo dei tag con policy IAM | 179 |
| Gruppi di fatturazione | 181 |
| Visualizzazione dell'allocazione dei costi e dei dati di utilizzo | 181 |
| Limiti | 182 |
| Sicurezza e identità | 183 |
| Autenticazione AWS IoT | 183 |
| Certificati X.509 | 184 |
| Utenti, gruppi e ruoli IAM | 191 |
| Identità di Amazon Cognito | 191 |
| Autenticazione personalizzata | 192 |
| Autorizzazioni ad hoc | 192 |
| Configurazione di autorizzazioni ad hoc | 194 |
| Flusso di lavoro delle autorizzazioni ad hoc | 195 |
| Autorizzazione | 196 |

| | |
|---|-----|
| Policy AWS IoT | 198 |
| Policy IoT IAM | 226 |
| Autorizzazione di chiamate dirette a servizi AWS | 232 |
| Come utilizzare un certificato per ottenere un token di sicurezza | 234 |
| Accesso tra account | 236 |
| Sicurezza del trasporto | 237 |
| Supporto per i pacchetti di crittografia TLS | 238 |
| Broker di messaggi | 239 |
| Protocolli | 239 |
| Associazioni tra protocolli e porte | 239 |
| MQTT | 240 |
| HTTP | 249 |
| MQTT tramite il protocollo WebSocket | 250 |
| Regole | 254 |
| Concessione dell'accesso richiesto ad AWS IoT | 254 |
| Passaggio delle autorizzazioni di un ruolo | 256 |
| Creazione di una regola AWS IoT | 256 |
| Visualizzazione delle regole | 260 |
| Eliminazione di una regola | 260 |
| Operazioni delle regole AWS IoT | 261 |
| Operazione per gli allarmi CloudWatch | 261 |
| Operazione per i parametri CloudWatch | 262 |
| Operazione DynamoDB | 263 |
| Operazione DynamoDBv2 | 265 |
| Operazione Elasticsearch | 266 |
| Operazione Firehose | 267 |
| Operazione IoT Analytics | 267 |
| Operazione IoT Events | 269 |
| Operazione Kinesis | 270 |
| Operazione Lambda | 271 |
| Operazione Republish | 272 |
| Operazione S3 | 273 |
| Operazione Salesforce | 274 |
| Operazione SNS | 275 |
| Operazione SQS | 275 |
| Step Functions Action | 276 |
| Risoluzione dei problemi relativi a una regola | 277 |
| Gestione degli errori (operazione in caso di errore) | 277 |
| Formato del messaggio dell'operazione da eseguire in caso di errore | 278 |
| Esempio di operazione in caso di errore | 279 |
| Documentazione di riferimento su SQL per AWS IoT | 279 |
| Tipi di dati | 280 |
| Operatori | 283 |
| Funzioni | 289 |
| Clausola SELECT | 324 |
| Clausola FROM | 326 |
| Clausola WHERE | 327 |
| Valori letterali | 328 |
| Istruzioni case | 328 |
| Estensioni JSON | 329 |
| Modelli di sostituzione | 330 |
| Versioni SQL | 330 |
| Novità della versione del motore di regole SQL 2016-03-23 | 331 |
| Basic Ingest | 333 |
| Per utilizzare Basic Ingest | 333 |
| Servizio Device Shadow | 335 |
| Flusso di dati del servizio Device Shadow | 335 |

| | |
|--|-----|
| Rilevamento della connessione di un oggetto | 342 |
| Documenti del servizio Device Shadow | 343 |
| Proprietà del documento | 343 |
| Funzione Versioni multiple per una copia shadow di un dispositivo | 344 |
| Token client | 344 |
| Documento di esempio | 344 |
| Sezioni vuote | 345 |
| Matrici | 345 |
| Uso delle copie shadow | 346 |
| Supporto dei protocolli | 346 |
| Aggiornamento di una copia shadow | 347 |
| Recupero di un documento di una copia shadow | 347 |
| Eliminazione di dati | 350 |
| Eliminazione di una copia shadow | 351 |
| Stato delta | 351 |
| Osservazione delle modifiche dello stato | 353 |
| Ordine dei messaggi | 353 |
| Taglio dei messaggi delle copie shadow | 354 |
| API RESTful | 355 |
| GetThingShadow | 355 |
| UpdateThingShadow | 356 |
| DeleteThingShadow | 357 |
| Argomenti MQTT di pubblicazione/sottoscrizione | 357 |
| /update | 358 |
| /update/accepted | 359 |
| /update/documents | 359 |
| /update/rejected | 360 |
| /update/delta | 360 |
| /get | 361 |
| /get/accepted | 362 |
| /get/rejected | 362 |
| /delete | 363 |
| /delete/accepted | 363 |
| /delete/rejected | 364 |
| Sintassi dei documenti | 364 |
| Documenti sullo stato della richiesta | 365 |
| Documenti sullo stato della risposta | 365 |
| Documenti di risposta di errore | 366 |
| Messaggi di errore | 367 |
| Jobs | 368 |
| Concetti chiave di Jobs | 368 |
| Gestione dei processi | 370 |
| Creazione e gestione di processi (Console) | 372 |
| Creazione e gestione di processi (CLI) | 373 |
| Dispositivi e servizio Jobs | 381 |
| Programmazione dei dispositivi per l'uso di Jobs | 383 |
| Uso delle API di AWS IoT Jobs | 393 |
| API di gestione e controllo dei processi | 394 |
| API MQTT e HTTPS per i dispositivi per il servizio Jobs | 453 |
| Configurazione dei rollout e delle interruzioni di processo | 479 |
| Utilizzo delle velocità di rollout di un processo | 479 |
| Utilizzo delle configurazioni dei rollout e delle interruzioni di processo | 480 |
| Limiti dei processi | 481 |
| Provisioning dei dispositivi | 482 |
| Modelli di provisioning | 482 |
| Sezione Parameters | 482 |
| Sezione Resources | 483 |

| | |
|---|-----|
| Esempio di modello | 487 |
| Provisioning programmatico | 488 |
| Provisioning Just-in-Time | 489 |
| Provisioning in blocco | 492 |
| Servizio Fleet Indexing | 493 |
| Gestione dell'indicizzazione degli oggetti | 493 |
| Abilitazione dell'indicizzazione degli oggetti | 493 |
| Descrizione di un indice dell'oggetto | 494 |
| Esecuzione di query su un indice di oggetti | 495 |
| Restrizioni e limitazioni | 496 |
| Autorizzazione | 497 |
| Gestione dell'indicizzazione di gruppi di oggetti | 498 |
| Abilitazione dell'indicizzazione di gruppi di oggetti | 498 |
| Descrizione degli indici di gruppi | 499 |
| Esecuzione di query su un indice di gruppi di oggetti | 499 |
| Autorizzazione | 499 |
| Ottenimento di statistiche sul parco istanze del dispositivo | 499 |
| Sintassi di query | 500 |
| Esempio di query per oggetti | 501 |
| Esempio di query per gruppi di oggetti | 503 |
| AWS IoT Device Defender | 505 |
| Audit | 505 |
| Controlli di auditing | 505 |
| Come eseguire gli audit | 524 |
| Notifiche | 525 |
| Autorizzazioni | 527 |
| Restrizioni dei servizi | 531 |
| Comandi di auditing | 532 |
| Gestione delle impostazioni di auditing | 532 |
| Pianificazione di audit | 536 |
| Esecuzione di un audit on demand | 545 |
| Gestione di istanze di audit | 546 |
| Controllo dei risultati dell'audit | 552 |
| Rilevamento | 558 |
| Concetti | 559 |
| Comportamenti | 560 |
| Parametri | 561 |
| Monitoraggio del comportamento dei dispositivi non registrati | 572 |
| Come utilizzare AWS IoT Device Defender Detect | 573 |
| Autorizzazioni | 574 |
| Restrizioni dei servizi | 575 |
| Invio di parametri dai dispositivi | 575 |
| Comandi di rilevamento | 580 |
| AttachSecurityProfile | 580 |
| CreateSecurityProfile | 582 |
| DeleteSecurityProfile | 587 |
| DescribeSecurityProfile | 588 |
| DetachSecurityProfile | 592 |
| ListActiveViolations | 593 |
| ListSecurityProfiles | 598 |
| ListSecurityProfilesForTarget | 600 |
| ListTargetsForSecurityProfile | 601 |
| ListViolationEvents | 603 |
| UpdateSecurityProfile | 608 |
| ValidateSecurityProfileBehaviors | 616 |
| Integrazione dell'agente dei dispositivi con AWS IoT Greengrass | 620 |
| Best practice per la sicurezza degli agenti dei dispositivi | 622 |

| | |
|--|-----|
| Risoluzione dei problemi di AWS IoT Device Defender | 624 |
| Messaggi di eventi | 627 |
| Eventi del registro | 628 |
| Eventi del servizio Jobs | 634 |
| Eventi del ciclo di vita | 637 |
| Eventi di connessione/disconnessione | 637 |
| Eventi di sottoscrizione/annullamento della sottoscrizione | 639 |
| SDK AWS IoT | 641 |
| SDK AWS Mobile per Android | 641 |
| SDK Arduino Yún | 641 |
| SDK di dispositivo AWS IoT per Embedded C | 641 |
| SDK di dispositivo AWS IoT per C++ | 642 |
| SDK AWS Mobile per iOS | 642 |
| SDK di dispositivo AWS IoT per Java | 642 |
| SDK di dispositivo AWS IoT per JavaScript | 642 |
| SDK di dispositivo AWS IoT per Python | 643 |
| Monitoraggio | 644 |
| Strumenti di monitoraggio | 644 |
| Strumenti automatici | 645 |
| Strumenti manuali | 645 |
| Monitoraggio con Amazon CloudWatch | 646 |
| Parametri e dimensioni | 646 |
| Utilizzo dei parametri di AWS IoT | 653 |
| Creazione di allarmi CloudWatch | 653 |
| Monitoraggio con CloudWatch Logs | 655 |
| Creazione di un ruolo di logging | 656 |
| Livello di log | 657 |
| Configurazione del logging di AWS IoT | 657 |
| Formato delle voci di log di CloudWatch | 660 |
| Visualizzazione dei log | 675 |
| Registrazione delle chiamate API AWS IoT con AWS CloudTrail | 676 |
| Informazioni di AWS IoT in CloudTrail | 676 |
| Comprensione delle voci dei file di log di AWS IoT | 677 |
| Risoluzione dei problemi | 679 |
| Diagnosi dei problemi di connettività | 679 |
| Autenticazione | 679 |
| Autorizzazione | 679 |
| Diagnosi dei problemi relativi alle regole | 679 |
| Diagnosi dei problemi relativi a Shadows | 680 |
| Diagnosi dei problemi relativi alle operazioni di Salesforce | 682 |
| Traccia di esecuzione | 682 |
| Esito dell'operazione | 682 |
| Limiti per AWS IoT | 683 |
| Errori di AWS IoT | 683 |
| Comandi IOT | 684 |
| AcceptCertificateTransfer | 688 |
| AddThingToBillingGroup | 689 |
| AddThingToThingGroup | 690 |
| AssociateTargetsWithJob | 692 |
| AttachPolicy | 693 |
| AttachPrincipalPolicy | 694 |
| AttachSecurityProfile | 696 |
| AttachThingPrincipal | 697 |
| CancelAuditTask | 698 |
| CancelCertificateTransfer | 699 |
| CancelJob | 700 |
| CancelJobExecution | 702 |

| | |
|---|-----|
| ClearDefaultAuthorizer | 704 |
| CreateAuthorizer | 705 |
| CreateBillingGroup | 706 |
| CreateCertificateFromCsr | 708 |
| CreateDynamicThingGroup | 710 |
| CreateJob | 713 |
| CreateKeysAndCertificate | 719 |
| CreateOTAUpdate | 720 |
| CreatePolicy | 726 |
| CreatePolicyVersion | 727 |
| CreateRoleAlias | 729 |
| CreateScheduledAudit | 731 |
| CreateSecurityProfile | 733 |
| CreateStream | 737 |
| CreateThing | 740 |
| CreateThingGroup | 742 |
| CreateThingType | 745 |
| CreateTopicRule | 747 |
| DeleteAccountAuditConfiguration | 762 |
| DeleteAuthorizer | 763 |
| DeleteBillingGroup | 764 |
| DeleteCACertificate | 765 |
| DeleteCertificate | 766 |
| DeleteDynamicThingGroup | 768 |
| DeleteJob | 769 |
| DeleteJobExecution | 770 |
| DeleteOTAUpdate | 772 |
| DeletePolicy | 774 |
| DeletePolicyVersion | 775 |
| DeleteRegistrationCode | 776 |
| DeleteRoleAlias | 776 |
| DeleteScheduledAudit | 777 |
| DeleteSecurityProfile | 778 |
| DeleteStream | 779 |
| DeleteThing | 780 |
| DeleteThingGroup | 781 |
| DeleteThingShadow | 782 |
| DeleteThingType | 784 |
| DeleteTopicRule | 785 |
| DeleteV2LogLevel | 786 |
| DeprecateThingType | 786 |
| DescribeAccountAuditConfiguration | 788 |
| DescribeAuditTask | 789 |
| DescribeAuthorizer | 792 |
| DescribeBillingGroup | 794 |
| DescribeCACertificate | 795 |
| DescribeCertificate | 798 |
| DescribeDefaultAuthorizer | 800 |
| DescribeEndpoint | 802 |
| DescribeEventConfigurations | 803 |
| DescribeIndex | 804 |
| DescribeJob | 806 |
| DescribeJobExecution | 812 |
| DescribeJobExecution | 815 |
| DescribeRoleAlias | 818 |
| DescribeScheduledAudit | 820 |
| DescribeSecurityProfile | 822 |

| | |
|--|-----|
| DescribeStream | 826 |
| DescribeThing | 828 |
| DescribeThingGroup | 830 |
| DescribeThingRegistrationTask | 833 |
| DescribeThingType | 835 |
| DetachPolicy | 837 |
| DetachPrincipalPolicy | 838 |
| DetachSecurityProfile | 839 |
| DetachThingPrincipal | 840 |
| DisableTopicRule | 842 |
| EnableTopicRule | 842 |
| GetEffectivePolicies | 843 |
| GetIndexingConfiguration | 845 |
| GetJobDocument | 847 |
| GetLoggingOptions | 848 |
| GetOTAUpdate | 848 |
| GetPendingJobExecutions | 854 |
| GetPolicy | 856 |
| GetPolicyVersion | 858 |
| GetRegistrationCode | 859 |
| GetStatistics | 860 |
| GetThingShadow | 862 |
| GetTopicRule | 863 |
| GetV2LoggingOptions | 878 |
| ListActiveViolations | 879 |
| ListAttachedPolicies | 884 |
| ListAuditFindings | 886 |
| ListAuditTasks | 891 |
| ListAuthorizers | 894 |
| ListBillingGroups | 895 |
| ListCACertificates | 897 |
| ListCertificates | 899 |
| ListCertificatesByCA | 901 |
| ListIndices | 903 |
| ListJobExecutionsForJob | 904 |
| ListJobExecutionsForThing | 906 |
| ListJobs | 909 |
| ListOTAUpdates | 912 |
| ListOutgoingCertificates | 914 |
| ListPolicies | 916 |
| ListPolicyPrincipals | 917 |
| ListPolicyVersions | 919 |
| ListPrincipalPolicies | 920 |
| ListPrincipalThings | 922 |
| ListRoleAliases | 923 |
| ListScheduledAudits | 925 |
| ListSecurityProfiles | 927 |
| ListSecurityProfilesForTarget | 928 |
| ListStreams | 930 |
| ListTagsForResource | 932 |
| ListTargetsForPolicy | 933 |
| ListTargetsForSecurityProfile | 934 |
| ListThingGroups | 936 |
| ListThingGroupsForThing | 938 |
| ListThingPrincipals | 939 |
| ListThingRegistrationTaskReports | 940 |
| ListThingRegistrationTasks | 942 |

| | |
|--|------|
| ListThingTypes | 943 |
| ListThings | 946 |
| ListThingsInBillingGroup | 948 |
| ListThingsInThingGroup | 949 |
| ListTopicRules | 951 |
| ListV2LoggingLevels | 952 |
| ListViolationEvents | 954 |
| Publish | 959 |
| RegisterCACertificate | 960 |
| RegisterCertificate | 962 |
| RegisterThing | 964 |
| RejectCertificateTransfer | 965 |
| RemoveThingFromBillingGroup | 966 |
| RemoveThingFromThingGroup | 967 |
| ReplaceTopicRule | 969 |
| SearchIndex | 983 |
| SetDefaultAuthorizer | 987 |
| SetDefaultPolicyVersion | 988 |
| SetLoggingOptions | 989 |
| SetV2LogLevel | 990 |
| SetV2LoggingOptions | 991 |
| StartNextPendingJobExecution | 992 |
| StartOnDemandAuditTask | 995 |
| StartThingRegistrationTask | 997 |
| StopThingRegistrationTask | 998 |
| TagResource | 999 |
| TestAuthorization | 1000 |
| TestInvokeAuthorizer | 1004 |
| TransferCertificate | 1006 |
| UntagResource | 1007 |
| UpdateAccountAuditConfiguration | 1008 |
| UpdateAuthorizer | 1010 |
| UpdateBillingGroup | 1012 |
| UpdateCACertificate | 1014 |
| UpdateCertificate | 1015 |
| UpdateDynamicThingGroup | 1017 |
| UpdateEventConfigurations | 1019 |
| UpdateIndexingConfiguration | 1020 |
| UpdateJob | 1022 |
| UpdateJobExecution | 1026 |
| UpdateRoleAlias | 1030 |
| UpdateScheduledAudit | 1031 |
| UpdateSecurityProfile | 1033 |
| UpdateStream | 1041 |
| UpdateThing | 1043 |
| UpdateThingGroup | 1046 |
| UpdateThingGroupsForThing | 1048 |
| UpdateThingShadow | 1049 |
| ValidateSecurityProfileBehaviors | 1050 |

Che cos'è AWS IoT?

AWS IoT offre una comunicazione bidirezionale e sicura tra i dispositivi connessi a Internet (come sensori, attuatori, microcontroller integrati o smart appliance) e il cloud AWS. In questo modo, puoi raccogliere dati di telemetria da più dispositivi e quindi archiviarli e analizzarli. Puoi anche creare applicazioni che permettono agli utenti di controllare questi dispositivi dai propri telefoni o tablet.

Componenti di AWS IoT

AWS IoT è costituito dai componenti seguenti:

Gateway dei dispositivi

Permette ai dispositivi di comunicare in modo sicuro ed efficiente con AWS IoT.

Broker di messaggi

Offre ai dispositivi e alle applicazioni di AWS IoT un sistema sicuro per la pubblicazione e la ricezione di messaggi. Puoi usare il protocollo MQTT direttamente o MQTT tramite WebSocket per la pubblicazione e la sottoscrizione. Puoi usare l'interfaccia HTTP REST per la pubblicazione.

Motore di regole

Fornisce elaborazione dei messaggi e integrazione con altri servizi AWS. Puoi usare un linguaggio basato su SQL per selezionare i dati dai payload dei messaggi e quindi elaborare e inviare i dati ad altri servizi, come Amazon S3, Amazon DynamoDB e AWS Lambda. Puoi usare il broker di messaggi anche per ripubblicare messaggi per altri sottoscrittori.

Servizio di sicurezza e identità

Garantisce una responsabilità condivisa per la sicurezza nel cloud AWS. I dispositivi devono mantenere protette le proprie credenziali per poter inviare dati al broker di messaggi in tutta sicurezza. Il broker di messaggi e il motore di regole usano le funzionalità di sicurezza di AWS per inviare dati in modo sicuro ai dispositivi o ad altri servizi AWS.

Registry

Organizza le risorse associate a ogni dispositivo nel cloud AWS. Puoi registrare i dispositivi e associare fino a tre attributi personalizzati a ognuno. Puoi anche associare certificati e ID client MQTT a ogni dispositivo per migliorare la tua capacità di gestirli e di risolvere i problemi.

Registro di gruppi

I gruppi ti permettono di gestire diversi dispositivi contemporaneamente classificandoli in gruppi. I gruppi possono contenere anche altri gruppi — puoi creare una gerarchia di gruppi. Qualsiasi operazione eseguita su un gruppo padre si applica anche ai rispettivi gruppi figlio e a tutti i dispositivi al suo interno e all'interno di tutti i gruppi figlio. Le autorizzazioni concesse a un gruppo vengono applicate a tutti i dispositivi nel gruppo e in tutti i rispettivi gruppi figlio.

Shadow dei dispositivi

Documento JSON usato per archiviare e recuperare informazioni sullo stato corrente per un dispositivo.

Servizio Device Shadow

Fornisce rappresentazioni persistenti dei dispositivi nel cloud AWS. Puoi pubblicare informazioni sullo stato aggiornate in una copia shadow di un dispositivo perché questo possa sincronizzare il proprio

stato quando si connette. I dispositivi possono anche pubblicare il proprio stato corrente in una copia shadow, usata da applicazioni o altri dispositivi.

Servizio di provisioning dei dispositivi

Permette di effettuare il provisioning dei dispositivi tramite un modello che descrive le risorse necessarie per il dispositivo: un oggetto, un certificato e una o più policy. Un oggetto è una voce nel registro che contiene attributi che descrivono un dispositivo. I dispositivi usano certificati per eseguire l'autenticazione con AWS IoT. Le policy determinano le operazioni che un dispositivo può eseguire in AWS IoT.

I modelli contengono variabili che vengono sostituite da valori in un dizionario (mappa). Puoi usare lo stesso modello per effettuare il provisioning di più dispositivi semplicemente passando valori diversi per le variabili del modello nel dizionario.

Servizio di autenticazione personalizzata

Puoi definire autorizzazioni ad hoc che ti permettono di gestire la tua strategia di autenticazione e autorizzazione tramite un servizio di autenticazione personalizzato e una funzione Lambda. Le autorizzazioni ad hoc permettono a AWS IoT di autenticare i dispositivi e autorizzare le operazioni tramite strategie di autenticazione e autorizzazione con token di connessione.

Le autorizzazioni ad hoc possono implementare diverse strategie di autenticazione, ad esempio la verifica Web Token JSON, la chiamata del provider OAuth e così via, e devono restituire documenti di policy che vengono usati dal gateway dei dispositivi per autorizzare le operazioni MQTT.

Servizio Jobs

Ti permette di definire un set di operazioni remote inviate a ed eseguite in uno o più dispositivi connessi a AWS IoT. Puoi ad esempio definire un processo che indichi a un set di dispositivi di scaricare e installare aggiornamenti per le applicazioni o il firmware, eseguire il riavvio, ruotare i certificati o eseguire operazioni di risoluzione dei problemi in remoto.

Per creare un processo, devi specificare una descrizione delle operazioni remote da eseguire e un elenco di target che devono eseguirle. I target possono essere singoli dispositivi, gruppi o entrambi.

Per informazioni sui limiti di AWS IoT, consulta la sezione [Limiti per AWS IoT](#).

Nozioni di base su AWS IoT

- Per ulteriori informazioni su AWS IoT, consulta [Funzionamento di AWS IoT \(p. 3\)](#).
- Per informazioni sulla connessione di un dispositivo a AWS IoT, consulta [Nozioni di base su AWS IoT \(p. 5\)](#).

Accesso a AWS IoT

In AWS IoT sono disponibili le interfacce seguenti per creare e interagire con i dispositivi:

- AWS Command Line Interface (AWS CLI)—Per eseguire i comandi di AWS IoT su Windows, macOS e Linux. Con questi comandi puoi creare e gestire oggetti, certificati, regole e policy. Per iniziare, consulta [Guida per l'utente di AWS Command Line Interface](#). Per ulteriori informazioni sui comandi di AWS IoT, consulta la sezione relativa a `iot` della AWS CLI Command Reference.
- API di AWS IoT—Per compilare applicazioni IoT tramite richieste HTTP o HTTPS. Con queste operazioni dell'API puoi creare e gestire in modo programmatico oggetti, certificati, regole e policy. Per ulteriori

informazioni sulle operazioni dell'API per AWS IoT, consulta la sezione relativa alle [operazioni](#) della documentazione di riferimento sull'API di AWS IoT.

- **SDK AWS**—Per creare applicazioni IoT tramite API specifiche del linguaggio. Questi SDK includono l'API HTTP/HTTPS e ti permettono di programmare in qualsiasi linguaggio supportato. Per ulteriori informazioni, consulta la sezione [SDK e strumenti di AWS](#).
- **SDK di AWS IoT per dispositivi**—Per creare applicazioni da eseguire sui dispositivi che inviano e ricevono messaggi da e verso AWS IoT. Per ulteriori informazioni, consulta la sezione relativa agli [SDK di AWS IoT](#).

Servizi correlati

AWS IoT si integra direttamente con i servizi AWS seguenti:

- Amazon Simple Storage Service—Fornisce storage scalabile nel cloud AWS. Per ulteriori informazioni, consulta [Amazon S3](#).
- Amazon DynamoDB—Fornisce database NoSQL gestiti. Per ulteriori informazioni, consulta [Amazon DynamoDB](#).
- Amazon Kinesis—Permette l'elaborazione in tempo reale dei dati di streaming su vasta scala. Per ulteriori informazioni, consulta [Amazon Kinesis](#).
- AWS Lambda—Esegue il codice su server virtuali da Amazon EC2 in risposta a eventi. Per ulteriori informazioni, consulta [AWS Lambda](#).
- Amazon Simple Notification Service—Invia o riceve notifiche. Per ulteriori informazioni, consulta [Amazon SNS](#).
- Amazon Simple Queue Service—Archivia i dati in una coda per consentirne il recupero dalle applicazioni. Per ulteriori informazioni, consulta [Amazon SQS](#).

Funzionamento di AWS IoT

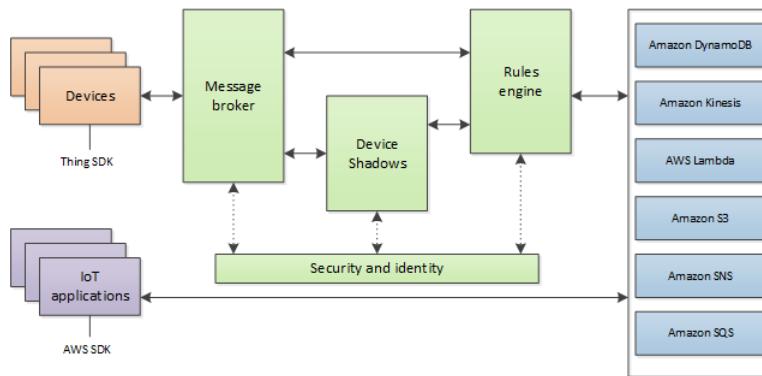
AWS IoT consente ai dispositivi connessi a Internet di connettersi al cloud AWS e alle applicazioni nel cloud di interagire con tali dispositivi. Le comuni applicazioni IoT raccolgono ed elaborano dati di telemetria dai dispositivi oppure permettono agli utenti di controllare un dispositivo in remoto.

I dispositivi segnalano il proprio stato pubblicando messaggi, in formato JSON, in argomenti MQTT. Ogni argomento MQTT ha un nome gerarchico che identifica il dispositivo il cui stato è in fase di aggiornamento. Quando vengono pubblicati in un argomento MQTT, i messaggi vengono inviati al broker di messaggi MQTT AWS IoT, responsabile dell'invio di tutti i messaggi pubblicati in un argomento MQTT a tutti i client che hanno sottoscritto l'argomento.

La comunicazione tra un dispositivo e AWS IoT è protetta dai certificati X.509. AWS IoT è in grado di generare un certificato per tuo conto oppure puoi scegliere di utilizzarne uno creato da te. In entrambi i casi, il certificato deve essere registrato e attivato su AWS IoT e quindi copiato nel dispositivo. Quando il dispositivo comunica con AWS IoT, presenta il certificato a AWS IoT come credenziale.

Consigliamo che per tutti i dispositivi che si connettono a AWS IoT sia presente una voce nel registro di oggetti. Nel registro vengono archiviate le informazioni sui dispositivi e sui certificati usati da questi ultimi per proteggere la comunicazione con AWS IoT.

Puoi creare regole che definiscono una o più operazioni da eseguire in base ai dati contenuti in un messaggio. Ad esempio, puoi inserire, aggiornare o interrogare una tabella di DynamoDB o richiamare una funzione Lambda. Le regole usano espressioni per filtrare i messaggi. Quando una regola corrisponde a un messaggio, il motore di regole attiva l'operazione usando le proprietà selezionate. Le regole contengono inoltre un ruolo IAM che concede a AWS IoT l'autorizzazione per le risorse AWS usate per eseguire l'operazione.



Ogni dispositivo è associato a una copia shadow che archivia e recupera le informazioni sullo stato. Ogni elemento nelle informazioni sullo stato ha due voci: l'ultimo stato segnalato dal dispositivo e lo stato desiderato richiesto da un'applicazione. Un'applicazione può richiedere informazioni sullo stato corrente per un dispositivo. La copia shadow risponde alla richiesta fornendo un documento JSON con le informazioni sullo stato (segnalato e desiderato), i metadati e un numero di versione. Un'applicazione può controllare un dispositivo richiedendo una modifica nel suo stato. La copia shadow accetta la richiesta di modifica dello stato, aggiorna le informazioni sullo stato e invia un messaggio per indicare che le informazioni sullo stato sono state aggiornate. Il dispositivo riceve il messaggio, modifica il proprio stato e quindi segnala il nuovo stato.

Nozioni di base su AWS IoT

Questo tutorial mostra come creare le risorse necessarie per inviare, ricevere ed elaborare messaggi MQTT da dispositivi tramite AWS IoT. Utilizzerai un client MQTT per emulare un dispositivo IoT.

Per ulteriori informazioni su AWS IoT, consulta [Che cos'è AWS IoT? \(p. 1\)](#).

Argomenti

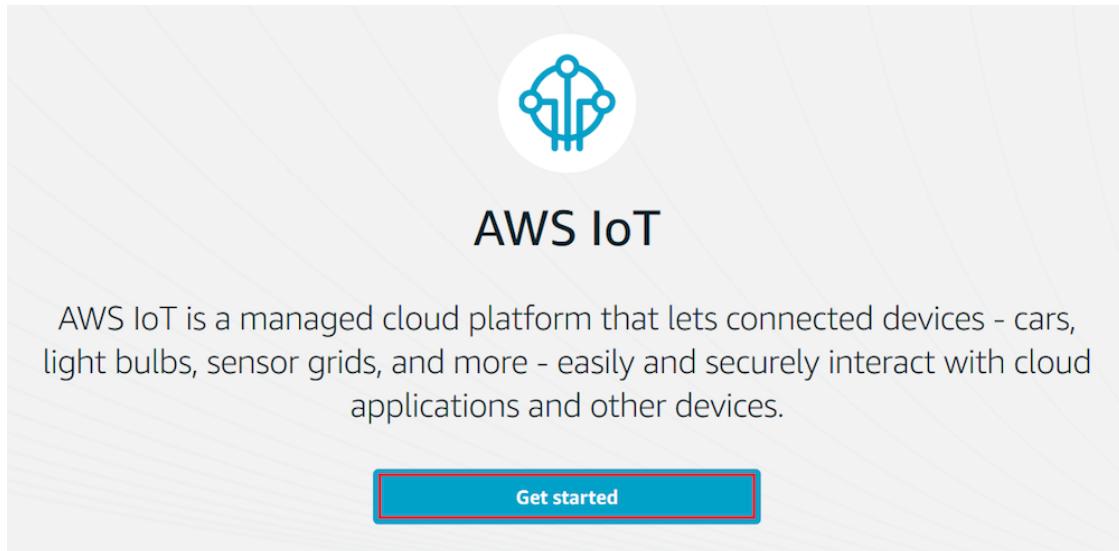
- [Accesso alla console AWS IoT \(p. 5\)](#)
- [Registrazione di un dispositivo nel registro \(p. 6\)](#)
- [Configurazione del dispositivo \(p. 25\)](#)
- [Visualizzazione di messaggi MQTT del dispositivo con il client MQTT AWS IoT \(p. 25\)](#)
- [Configurazione e test delle regole \(p. 27\)](#)
- [Creazione e monitoraggio di un processo AWS IoT \(p. 37\)](#)

Accesso alla console AWS IoT

Se non disponi di un account AWS, creane uno.

Per creare un account AWS:

1. Apri la [home page di AWS](#) e fai clic su Crea un account gratuito.
2. Seguire le istruzioni online. Come parte della procedura di registrazione riceverai una chiamata telefonica e dovrà immettere un PIN usando la tastiera del telefono.
3. Accedi alla Console di gestione AWS e apri la [console AWS IoT](#).
4. Nella pagina Welcome (Benvenuto) scegli Get started (Inizia).



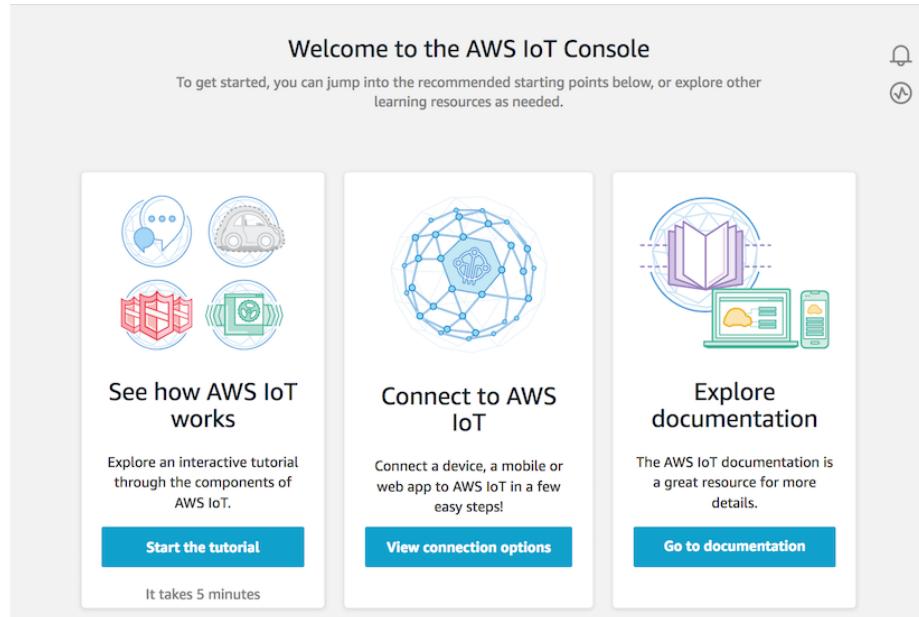
Se usi la console AWS IoT per la prima volta, verrà visualizzata la pagina Benvenuto nella console AWS IoT.

Registrazione di un dispositivo nel registro

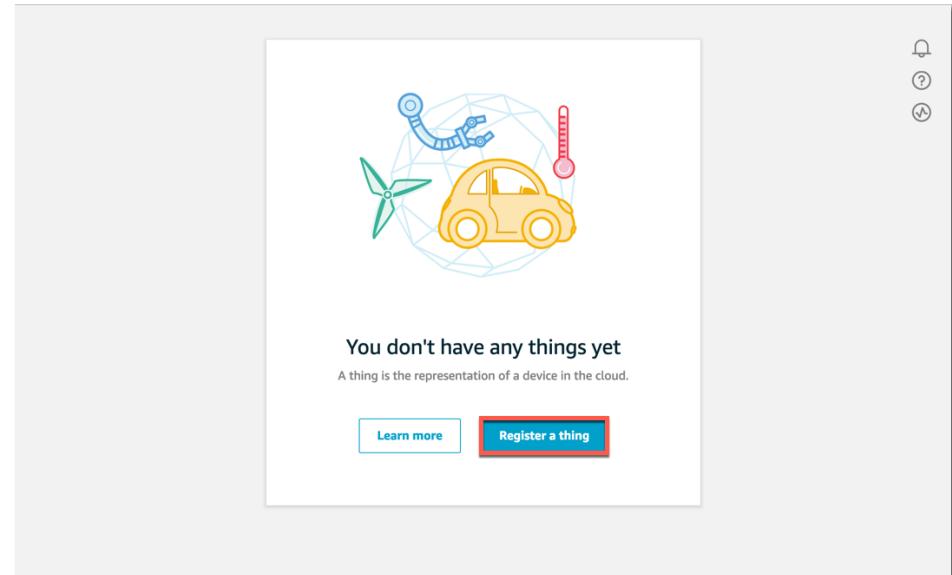
I dispositivi connessi a AWS IoT sono rappresentati da oggetti IoT nel registro AWS IoT. Il registro permette di tenere traccia di un record di tutti i dispositivi registrati nell'account AWS IoT.

Per registrare un dispositivo nel registro:

- Nella pagina Benvenuto nella console AWS IoT del riquadro di navigazione, scegliere Gestisci.



- Nella pagina You don't have any things yet (Non hai ancora oggetti), scegliere Register a thing (Registra un oggetto).



- Nella pagina Creazione oggetti AWS IoT, scegliere Crea un oggetto singolo.

The screenshot shows the 'Creating AWS IoT things' page. It has a blue header bar with the title. Below it, a text block explains what an IoT thing is: 'An IoT thing is a representation and record of your physical device in the cloud. Any physical device needs a thing record in order to work with AWS IoT.' A link to 'Learn more' is provided. There are two main sections: 'Register a single AWS IoT thing' and 'Bulk register many AWS IoT things'. The 'Register a single AWS IoT thing' section contains a sub-section 'Create a thing in your registry' and a red-bordered 'Create a single thing' button. The 'Bulk register many AWS IoT things' section contains a sub-section 'Create things in your registry for a large number of devices already using AWS IoT, or register devices so they are ready to connect to AWS IoT.' and a 'Create many things' button. At the bottom left is a 'Cancel' button, and at the bottom right is another 'Create a single thing' button.

4. Nel campo Name (Nome) della pagina Create a thing (Crea un oggetto), digitare un nome per l'oggetto, ad esempio **MyIoTThing**. Seleziona Next (Avanti).

Note

Non è consigliabile utilizzare informazioni di identificazione personale nel nome degli oggetti.

CREATE A THING

Add your device to the thing registry

STEP
1/3

This step creates an entry in the thing registry and a thing shadow for your device.

Name

Apply a type to this thing

Using a thing type simplifies device management by providing consistent registry data for things that share a type. Types provide things with a common set of attributes, which describe the identity and capabilities of your device, and a description.

Thing Type

No type selected

Create a type

Add this thing to a group

Adding your thing to a group allows you to manage devices remotely using jobs.

Thing Group

Groups /

Create group Change

Set searchable thing attributes (optional)

Enter a value for one or more of these attributes so that you can search for your things in the registry.

Attribute key

Value

Clear

Add another

Show thing shadow ▾

Cancel

Back

Next

5. Nella pagina Add a certificate for your thing (Aggiungi un certificato per l'oggetto), scegliere Create certificate (Crea certificato). Questa operazione genera un certificato e una coppia di chiavi X.509.

CREATE A THING

Add a certificate for your thing

A certificate is used to authenticate your device's connection to AWS IoT.

One-click certificate creation (recommended)

This will generate a certificate, public key, and private key using AWS IoT's certificate authority.

[Create certificate](#)

Create with CSR

Upload your own certificate signing request (CSR) based on a private key you own.

[Create with CSR](#)

Use my certificate

Register your CA certificate and use your own certificates for one or many devices.

[Get started](#)

Skip certificate and create thing

You will need to add a certificate to your thing later before your device can connect to AWS IoT.

[Create thing without certificate](#)

6. Nella pagina Certificato creato scaricare le chiavi pubbliche e private, il certificato e l'autorità di certificazione (CA) root.
 - a. Scegliere Scarica per il certificato.
 - b. Scegliere Scarica per la chiave privata.
 - c. Scegliere Scarica per l'autorità di certificazione root Amazon. Viene visualizzata una nuova pagina Web. Scegliere RSA 2048 bit key: Amazon Root CA 1 (Chiave RSA a 2048 bit: autorità di certificazione root Amazon 1. Viene visualizzata un'altra pagina Web con il testo del certificato CA root. Copiare il testo e incollarlo in un file denominato `Amazon_Root_CA_1.pem`.

La maggior parte dei browser Web salva i file scaricati in una directory di download. È possibile copiare questi file in una directory diversa quando si eseguono le applicazioni di esempio. Scegliere Activate (Programma Activate) per attivare il certificato X.509, quindi scegliere Attach a policy (Collega una policy).

Certificate created!

Download these files and save them in a safe place. Certificates can be retrieved at any time, but the private and public keys cannot be retrieved after you close this page.

In order to connect a device, you need to download the following:

| | | |
|------------------------------|------------------------|--------------------------|
| A certificate for this thing | 0488f55a11.cert.pem | Download |
| A public key | 0488f55a11.public.key | Download |
| A private key | 0488f55a11.private.key | Download |

You also need to download a root CA for AWS IoT:

A root CA for AWS IoT [Download](#)

[Activate](#)

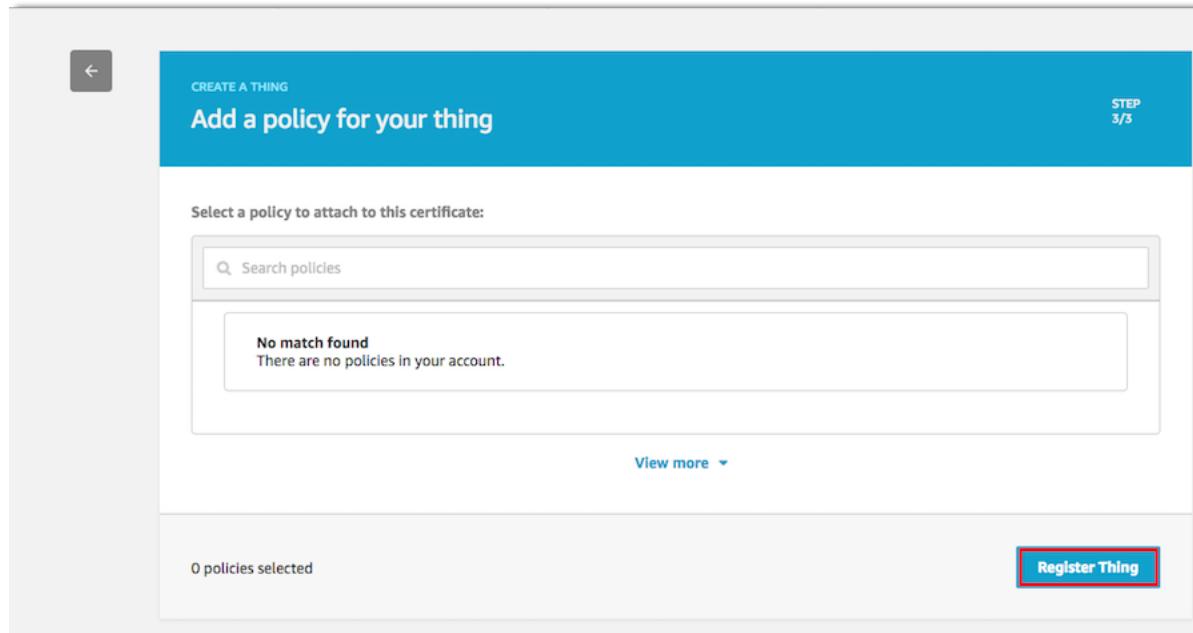
[Cancel](#)

[Done](#)

[Attach a policy](#)

7. Nella pagina Add a policy for your thing (Aggiungi una policy per l'oggetto), scegliere Register Thing (Registra l'oggetto).

Dopo avere registrato l'oggetto, è necessario creare e collegare una nuova policy al certificato.



8. Nella console AWS IoT del riquadro di navigazione, scegliere Secure (Sicurezza) e Policies (Policy).

Scegliere Create (Crea).

9. Nella pagina Create a policy (Crea una policy):

- Immettere un Name (Nome) per la policy, ad esempio **MyIoTPolicy**.
- In Action (Operazione), immettere **iot:***. In Resource ARN (ARN risorsa), immettere *****.
- In Effect (Effetto), scegliere Allow (Consenti), quindi scegliere Create (Crea).

Questa policy consente al dispositivo di eseguire tutte le operazioni AWS IoT su tutte le risorse AWS IoT.

Important

Queste impostazioni sono eccessivamente permissive. In un ambiente di produzione restringere l'ambito delle autorizzazioni a quelle che sono richieste dal dispositivo. Per ulteriori informazioni, consulta [Autorizzazione \(p. 196\)](#).

Create a policy

Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters). To learn more about IoT policies go to the [AWS IoT Policies documentation page](#).

Name

MyIoTPolicy

Add statements

Policy statements define the types of actions that can be performed by a resource.

Advanced

Action

iot:*

Resource ARN

*

Effect

Allow Deny

Remove

Add statement

Create

10. Scegliere Manage (Gestisci), quindi selezionare l'oggetto AWS IoT.

THING
MyIoTThing
NO TYPE

Actions

Details

Security

Thing Groups
Billing Groups
Shadow
Interact
Activity
Jobs
Violations

Thing ARN

A thing Amazon Resource Name uniquely identifies this thing.
arn:aws:iot:us-west-2:...:thing/MyIoTThing

Type

Q No type

11. Scegliere Security (Sicurezza).

THING
MyIoTThing
NO TYPE

Actions

Details

Security

Thing Groups
Billing Groups
Shadow
Interact
Activity
Jobs
Violations

Certificates

Create certificate View other options

c290b87d4ece080f3a...

12. Scegliere il certificato.
13. Nella pagina dei dettagli del certificato, scegliere Actions (Operazioni), quindi Attach policy (Allega policy).

The screenshot shows the AWS IoT Certificate Details page. At the top, there's a dark header with the word "CERTIFICATE" and a certificate ID "c290b87d4ece080f3a6d3085f9971e939b300c20d8503766a92aecc4bcdf75f7" followed by the word "ACTIVE". To the right, a vertical "Actions" menu is open, showing options like "Activate", "Deactivate", "Revoke", "Accept transfer", "Reject transfer", "Revoke transfer", "Start transfer", "Attach policy" (which is highlighted with a red box), "Attach thing", "Download", and "Delete". Below the header, there's a "Details" section with tabs for "Policies", "Things", and "Non-compliance". The "Policies" tab is selected, showing the ARN of the certificate: "arn:aws:iot:us-west-2:030714055129:cert/c290b87d4ece080f3a6d3085". Under the "Details" section, there are fields for "Issuer" (OU=Amazon Web Services O=Amazon.com Inc. L=Seattle ST=Washington C=US), "Subject" (CN=AWS IoT Certificate), "Create date" (Feb 18, 2019 2:41:59 PM -0800), "Effective date" (Feb 18, 2019 2:39:59 PM -0800), and "Expiration date" (Dec 31, 2049 3:59:59 PM -0800).

14. Scegliere la policy creata (MyIotPolicy) e selezionare Attach (Collega).

This screenshot shows a modal dialog titled "Attach policies to certificate(s)". It contains a message stating "Policies will be attached to the following certificate(s):" followed by the certificate ID "c290b87d4ece080f3a6d3085f9971e939b300c20d8503766a92aecc4bcdf75f7". Below this, there's a section titled "Choose one or more policies" with a search bar and a list of policies. A single policy, "MyIotPolicy", is selected with a checked checkbox. To the right of the checkbox is a "View" link. At the bottom of the dialog, there are buttons for "Cancel" and "Attach". The "Attach" button is highlighted with a red box.

Creazione e attivazione di un certificato del dispositivo

La comunicazione tra il dispositivo e AWS IoT è protetta tramite certificati X.509. AWS IoT può generare un certificato per conto tuo oppure puoi scegliere di usare il tuo certificato X.509. In questo tutorial il certificato X.509 viene generato per te da AWS IoT. I certificati devono essere attivati prima dell'uso.

1. Scegli Crea certificato.



A certificate is used to authenticate your device's connection to AWS IoT.

One-click certificate creation (recommended)

This will generate a certificate, public key, and private key using AWS IoT's certificate authority.

Create certificate

STEP
2/3

Create with CSR

Upload your own certificate signing request (CSR) based on a private key you own.

Create with CSR

Use my certificate

Register your CA certificate and use your own certificates for one or many devices.

Get started

Skip certificate and create thing

You will need to add a certificate to your thing later before your device can connect to AWS IoT.

Create thing without certificate

2. Nella pagina Certificato creato scegli Scarica per il certificato, la chiave privata e la CA root per AWS IoT (la chiave pubblica non deve essere scaricata). Salva ognuno di questi elementi nel computer e quindi scegli Activate (Attiva) per continuare.

Note

Il link Scarica per il certificato CA root per AWS IoT consente di andare alla pagina [Certificati X.509 e AWS IoT \(p. 184\)](#) in cui è possibile scegliere un certificato CA. A differenza degli altri link Scarica della pagina, il file non viene scaricato direttamente.

Certificate created!

Download these files and save them in a safe place. Certificates can be retrieved at any time, but the private and public keys cannot be retrieved after you close this page.

In order to connect a device, you need to download the following:

| | | |
|------------------------------|------------------------|--------------------------|
| A certificate for this thing | 09eb9ae91d.cert.pem | Download |
| A public key | 09eb9ae91d.public.key | Download |
| A private key | 09eb9ae91d.private.key | Download |

You also need to download a root CA for AWS IoT:

A root CA for AWS IoT [Download](#)

[Activate](#)

[Cancel](#)

[Done](#)

[Attach a policy](#)

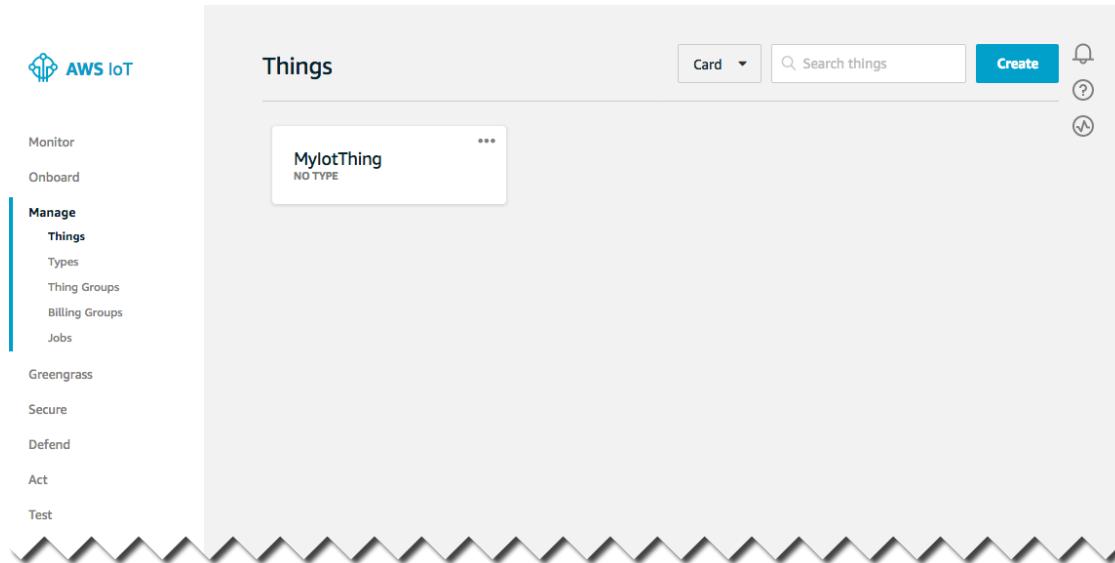
Tieni presente che i nomi di file scaricati possono essere diversi da quelli indicati nella pagina Certificato creato. Ad esempio:

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

Note

Anche se improbabile, i certificati dell'autorità di certificazione root sono soggetti a scadenza e/o revoca. Qualora ciò accadesse, dovrà copiare un nuovo certificato dell'autorità di certificazione root nel dispositivo.

3. Scegliere Done (Fatto) per tornare alla pagina principale della console AWS IoT.



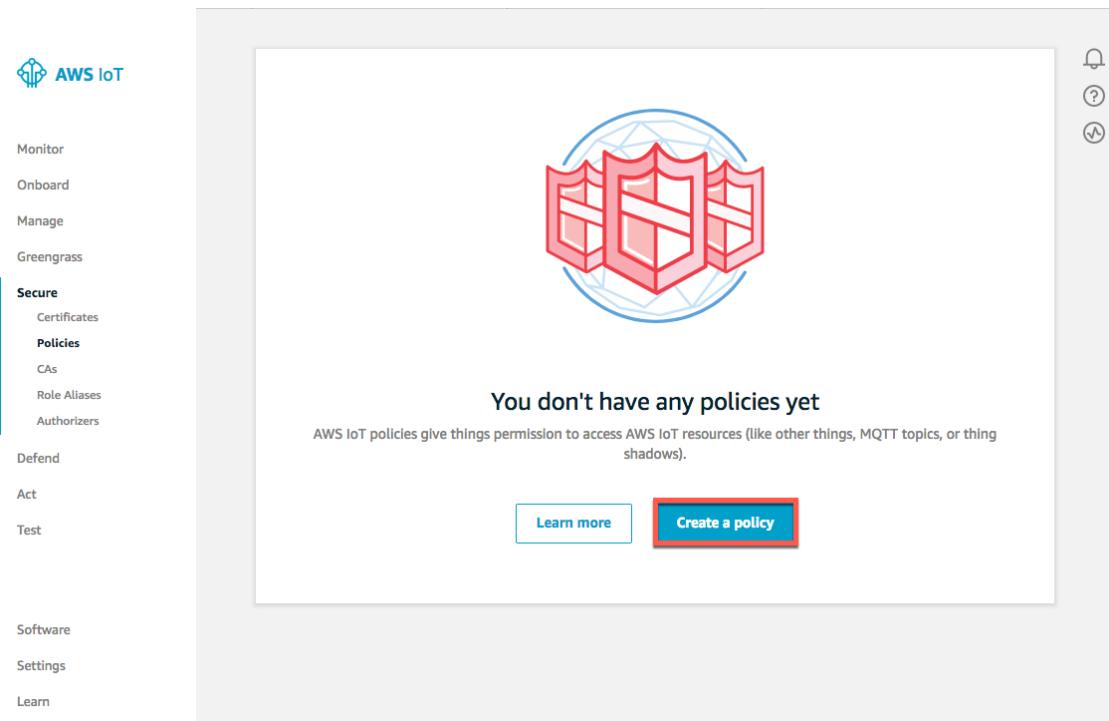
Quando si utilizza un dispositivo, è necessario copiare la chiave privata e il certificato CA root sul dispositivo. Questa guida presume che non si stia utilizzando un dispositivo e che si stia provando AWS IoT utilizzando la console.

Creazione di una policy AWS IoT

I certificati X.509 vengono usati per l'autenticazione del dispositivo con AWS IoT. Le policy AWS IoT vengono usate per autorizzare il dispositivo a eseguire operazioni AWS IoT, come la sottoscrizione o la pubblicazione di argomenti MQTT. Il dispositivo presenta il proprio certificato durante l'invio di messaggi a AWS IoT. Per permettere al dispositivo di eseguire operazioni AWS IoT, devi creare una policy AWS IoT e collegarla al certificato del dispositivo.

Per creare una policy AWS IoT:

1. Nel riquadro di navigazione a sinistra scegli Secure (Sicurezza) e quindi Policies (Policy). Nella pagina You don't have a policy yet (Al momento non sono disponibili policy) scegli Create a policy (Crea una policy).



2. Nella pagina Create a policy (Crea una policy), nel campo Name (Nome), digita un nome per la policy, ad esempio **MyIoTPolicy**.

Note

Non è consigliabile utilizzare informazioni di identificazione personale nei nomi delle policy.

Nel campo Action (Operazione) digita iot:Connect. Nel campo Resource ARN (ARN risorsa) digita *. Seleziona la casella di controllo Allow (Permetti). In questo modo, tutti i client potranno connettersi ad AWS IoT.

Create a policy

Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters). To learn more about IoT policies go to the [AWS IoT Policies documentation page](#).

Name

MyiotPolicy

Add statements

Policy statements define the types of actions that can be performed by a resource.

Advanced mode

Action

iot:Connect

Resource ARN

*

Effect

Allow Deny

Remove

Add statement

The screenshot shows the 'Create a policy' interface. At the top, it says 'Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters). To learn more about IoT policies go to the [AWS IoT Policies documentation page](#)'. Below this, there's a 'Name' field containing 'MyiotPolicy'. Under 'Add statements', there's a section for a single policy statement. It includes fields for 'Action' (set to 'iot:Connect'), 'Resource ARN' (containing '*'), and 'Effect' (with 'Allow' checked and 'Deny' uncheckable). A 'Remove' button is also present. At the bottom of this section is a 'Add statement' button. The entire interface has a wavy decorative border at the bottom.

Note

È possibile limitare i client (dispositivi) che possono connettersi specificando un ARN client come risorsa. Gli ARN client hanno il formato seguente:

`arn:aws:iot:<your-region>:<your-aws-account>:client/<my-client-id>`

Fai clic sul pulsante Add Statement (Aggiungi dichiarazione) per aggiungere un'altra dichiarazione della policy. Nel campo Action (Operazione) digita iot:Publish. Nel campo Resource ARN (ARN risorsa) digita l'ARN dell'argomento in cui il dispositivo eseguirà la pubblicazione.

Note

L'ARN dell'argomento ha il formato seguente:

`arn:aws:iot:<your-region>:<your-aws-account>:topic/<your/topic>`

Ad esempio:

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

Infine, seleziona la casella di controllo Allow (Permetti). In questo modo il dispositivo può pubblicare i messaggi nell'argomento specificato.

3. Dopo avere immesso le informazioni per la policy, scegli Create (Crea).

The screenshot shows the AWS IoT Policy Management interface. At the top, there is a decorative header with a wavy pattern. Below it, the title "Add statements" is displayed, followed by a descriptive text: "Policy statements define the types of actions that can be performed by a resource." On the right, there is a link to "Advanced mode".

The main area contains two policy statements:

- Statement 1:** Action: iot:Connect; Resource ARN: *; Effect: Allow (checked). A red-bordered "Remove" button is located to the right.
- Statement 2:** Action: iot:Publish; Resource ARN: arn:aws:iot:us-west-2:123456789012:topic/mytopic; Effect: Allow (checked). A red-bordered "Remove" button is located to the right.

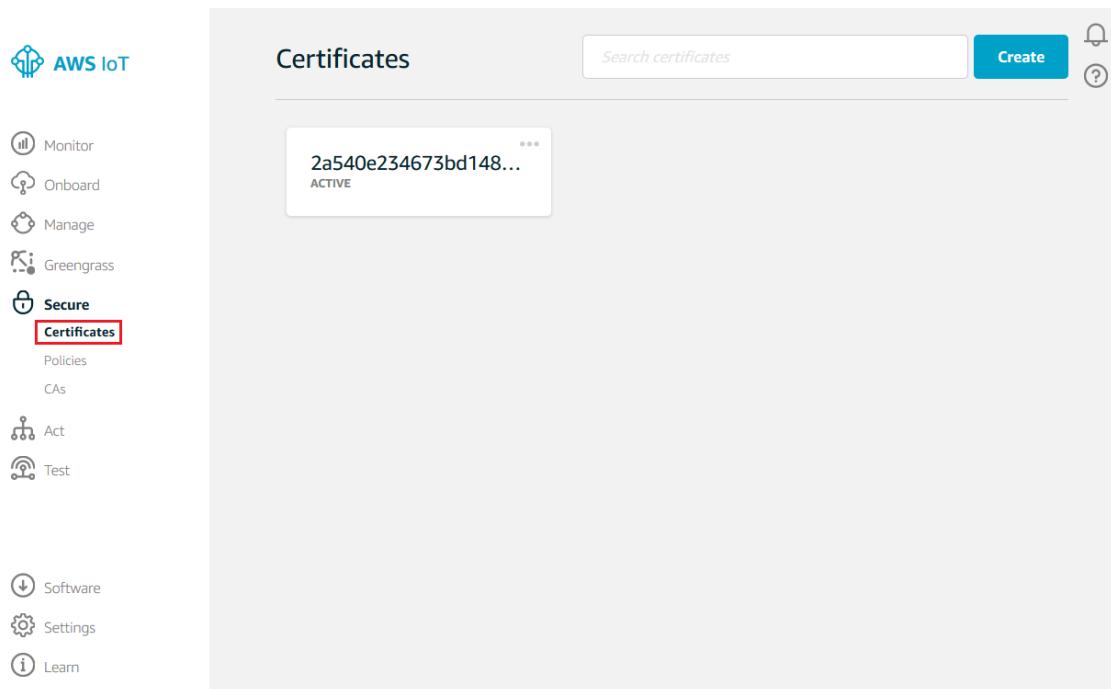
At the bottom left, there is a "Add statement" button. At the bottom right, there is a large blue "Create" button.

Per ulteriori informazioni, consulta [Gestione di policy AWS IoT](#).

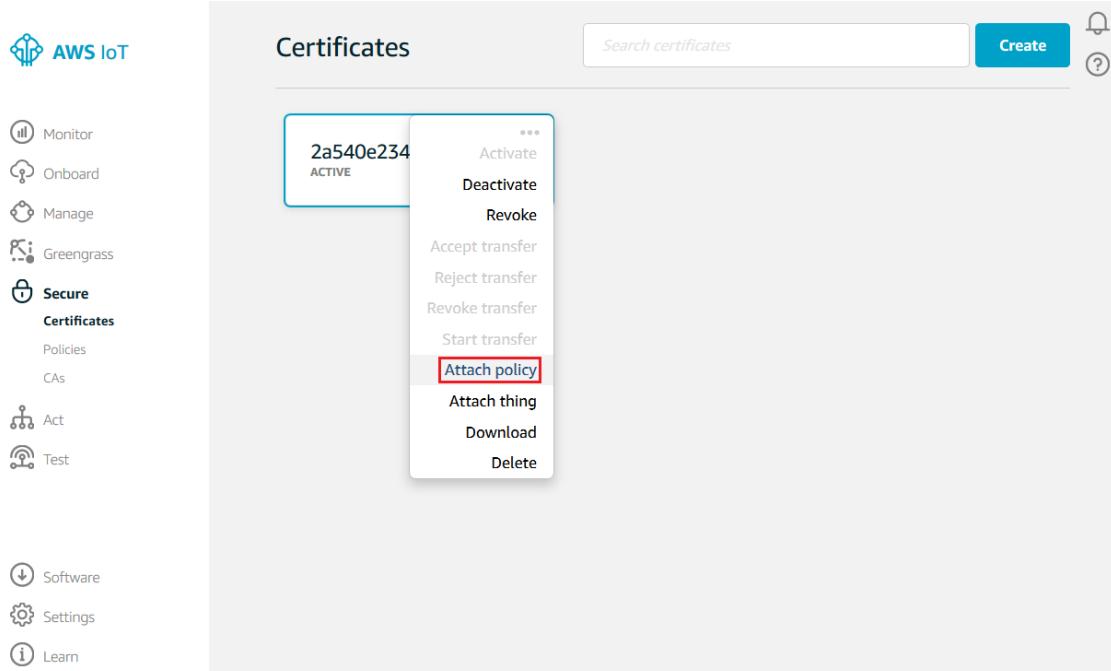
Collegamento di una policy AWS IoT a un certificato del dispositivo

Dopo avere creato una policy, è necessario collegarla al certificato del dispositivo. Collegando una policy AWS IoT a un certificato, concedi al dispositivo le autorizzazioni specificate nella policy.

1. Nel riquadro di navigazione a sinistra scegli Secure (Sicurezza) e quindi Certificates (Certificati).



2. Nella casella per il certificato creato scegli ... per aprire un menu a discesa e quindi scegli Attach policy (Collega policy).



3. Nella finestra di dialogo Attach policies to certificate(s) (Collega policy ai certificati) seleziona la casella di controllo accanto alla policy creata nella fase precedente e quindi scegli Attach (Collega).

Attach policies to certificate(s)

Policies will be attached to the following certificate(s):
09eb9ae91d6f9bdf423d4b491aa50fdbd925c2fefb56f63dab8435ecfc08b18a

Choose one or more policies

Search policies

MylotPolicy [View](#)

1 policy selected [Cancel](#) [Attach](#)

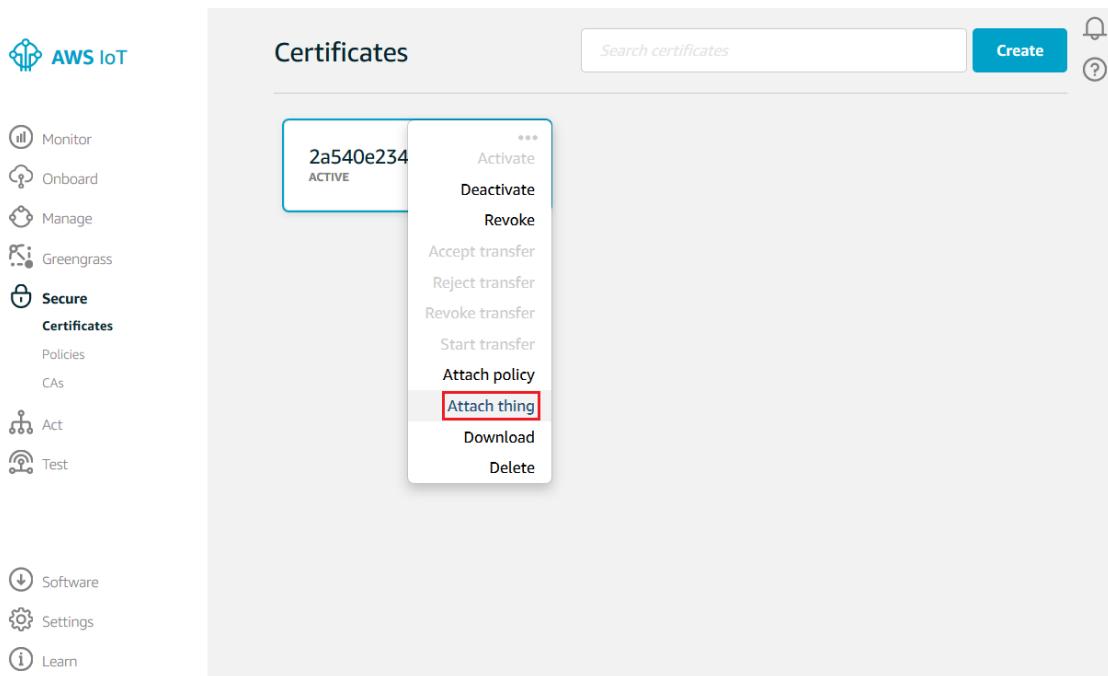


Collegamento di un certificato a un oggetto

Un dispositivo deve avere un certificato, una chiave privata e un certificato CA root per l'autenticazione con AWS IoT. È consigliabile anche collegare il certificato del dispositivo all'oggetto IoT che rappresenta il dispositivo in AWS IoT. In questo modo, puoi creare policy AWS IoT per concedere le autorizzazioni in base ai certificati collegati agli oggetti. Per ulteriori informazioni, consulta [Variabili delle policy di oggetto \(p. 203\)](#).

Per collegare un certificato all'oggetto che rappresenta il dispositivo nel registro:

1. Nella casella per il certificato creato scegli ... per aprire un menu a discesa e quindi scegli Attach thing (Collega oggetto).



2. Nella finestra di dialogo Attach things to certificate(s) (Collega oggetti ai certificati) seleziona la casella di controllo accanto all'oggetto registrato e quindi scegli Attach (Collega).

Attach things to certificate(s)

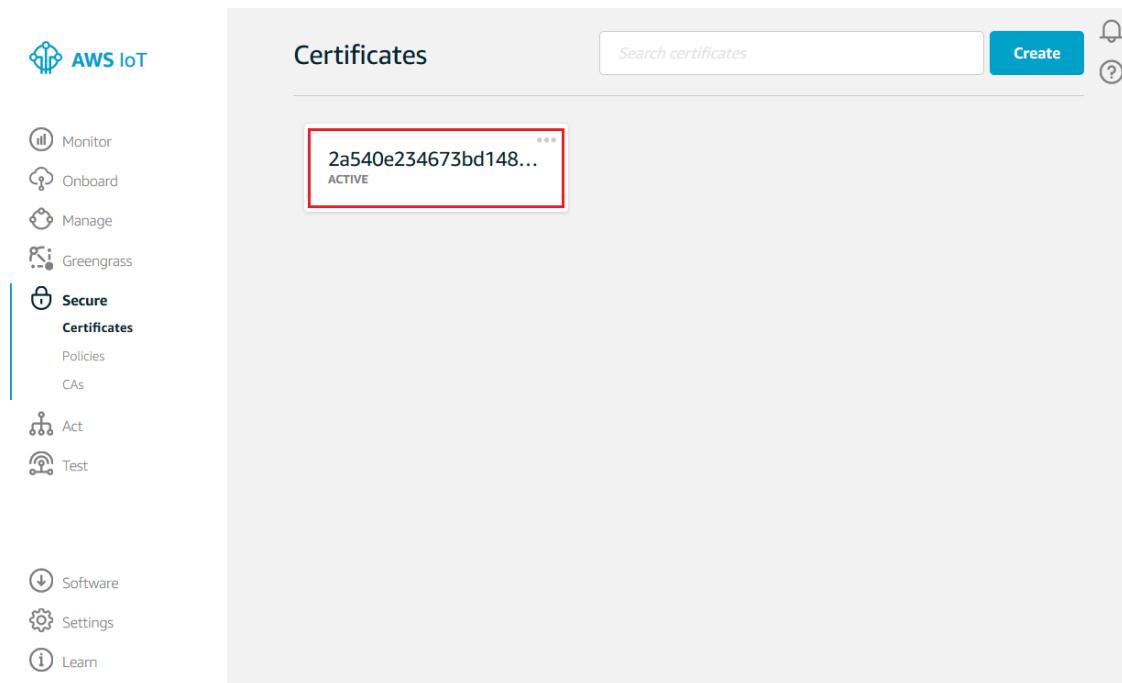
Things will be attached to the following certificate(s):

09eb9ae91d6f9bdf423d4b491aa50fdbd925c2fefb56f63dab8435ecfc08b18a

Choose one or more things

This is a modal dialog box titled "Attach things to certificate(s)". It contains a search bar labeled "Search things" and a list of selected items. One item, "MyiotThing", is listed with a checked checkbox. At the bottom right of the dialog, there are buttons for "Cancel" and "Attach".

3. Per verificare che l'oggetto sia collegato, seleziona la casella che rappresenta il certificato.



4. Nel riquadro di navigazione a sinistra della pagina Details (Dettagli) per il certificato scegli Things (Oggetti).

CERTIFICATE
09eb9ae91d6f9bdf423d4b491aa50fdbd925c2fefb56f63dab8435ecfc08b18a
ACTIVE

Actions ▾

Details Things

Policies MyIotThing

Things Non-compliance

5. Per verificare che la policy sia collegata, nel riquadro di navigazione a sinistra della pagina Details (Dettagli) per il certificato scegli Policies (Policy).

CERTIFICATE
09eb9ae91d6f9bdf423d4b491aa50fdbd925c2fefb56f63dab8435ecfc08b18a
ACTIVE

Actions ▾

Details Policies

Policies MyIotPolicy

Things Non-compliance

Configurazione del dispositivo

In tutti i dispositivi devono essere installati un certificato del dispositivo, una chiave privata e un certificato CA root per poter comunicare con AWS IoT. Consulta la documentazione del dispositivo per connetterlo e copiare il certificato del dispositivo, la chiave privata e il certificato dell'autorità di certificazione root nel dispositivo.

Se non disponi di un dispositivo IoT, puoi utilizzare il client MQTT, gli SDK del dispositivo AWS IoT o AWS CLI. Per maggiori informazioni, vedi la sezione [AWS IoTTutorial SDK \(p. 89\)](#). I tutorial utilizzano un Raspberry Pi, ma possono essere facilmente adattati per l'utilizzo con altri tipi di computer.

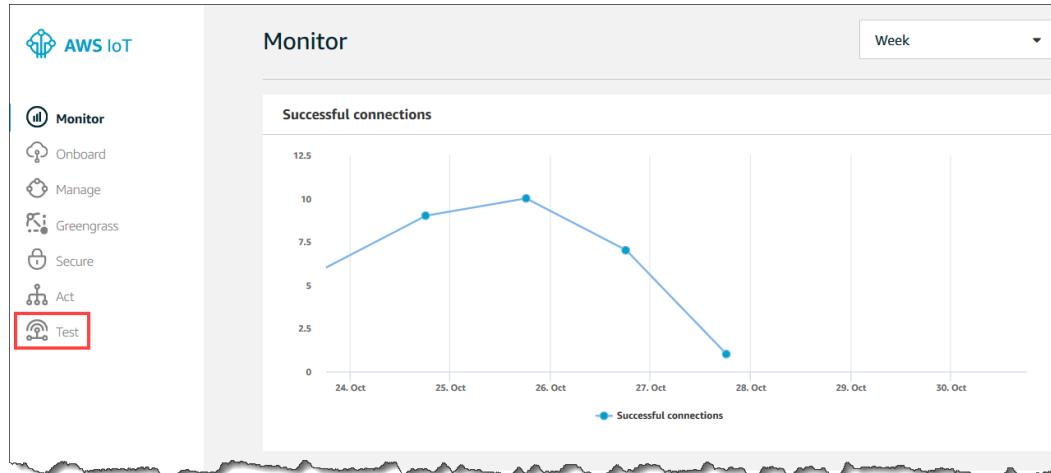
Visualizzazione di messaggi MQTT del dispositivo con il client MQTT AWS IoT

Puoi usare il client MQTT AWS IoT per comprendere meglio i messaggi MQTT inviati da un dispositivo.

I dispositivi pubblicano i messaggi MQTT negli argomenti. Puoi usare il client MQTT AWS IoT per sottoscrivere questi argomenti per visualizzare i messaggi.

Per visualizzare i messaggi MQTT:

1. Nel riquadro di navigazione a sinistra della [console AWS IoT](#) scegli Test.



2. Effettua la sottoscrizione all'argomento in cui l'oggetto IoT pubblica. Proseguendo con l'esempio, nel campo Subscription topic (Argomento sottoscrizione) in Subscribe to a topic (Sottoscrizione a un argomento), digita **my/topic** e quindi scegli **Subscribe to topic** (Effettua sottoscrizione all'argomento).

AWS IoT Guida per gli sviluppatori Visualizzazione di messaggi MQTT del dispositivo con il client MQTT AWS IoT

The screenshot shows the AWS IoT MQTT client interface. On the left, a sidebar menu includes options like Monitor, Onboard, Manage, Greengrass, Secure, Defend, Act, and Test. The 'Test' option is currently selected. The main area is titled 'MQTT client' and shows a 'Connected as iotconsole-1549405147548-4' status. A blue header bar at the top of the main area says 'Subscriptions'. Below it, there are two buttons: 'Subscribe to a topic' and 'Publish to a topic'. The 'Subscribe to a topic' section contains a 'Subscription topic' input field with 'my/topic' and a 'Subscribe to topic' button. It also includes a 'Max message capture' input field set to '100'. Under 'Quality of Service', the '0 - This client will not acknowledge to the Device Gateway that messages are received' radio button is selected. In the 'MQTT payload display' section, the 'Auto-format JSON payloads (improves readability)' radio button is selected. At the bottom of the interface, there are three small circular icons.

La scelta dell'opzione **Subscribe to topic** (Effettua sottoscrizione all'argomento) nella fase precedente fa sì che l'argomento **my/topic** venga visualizzato nella colonna Subscriptions (Sottoscrizioni).

This screenshot shows the same AWS IoT MQTT client interface, but the 'Publish' tab is now active. The main area is titled 'MQTT client' and shows a 'Connected as iotconsole-1549405147548-4' status. The 'Subscriptions' section still shows 'my/topic'. The 'Publish' section has a 'Specify a topic and a message to publish with a QoS of 0.' label and a 'Publish to topic' button. Below this, a code editor window displays the following JSON message:

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

Per emulare un oggetto IoT che invia un messaggio

- Nella pagina del client MQTT, nel campo **Specify a topic and a message to publish** (Specifica un argomento e un messaggio da pubblicare) della sezione **Publish** (Pubblicare), digitare ...**my/topic**.

Note

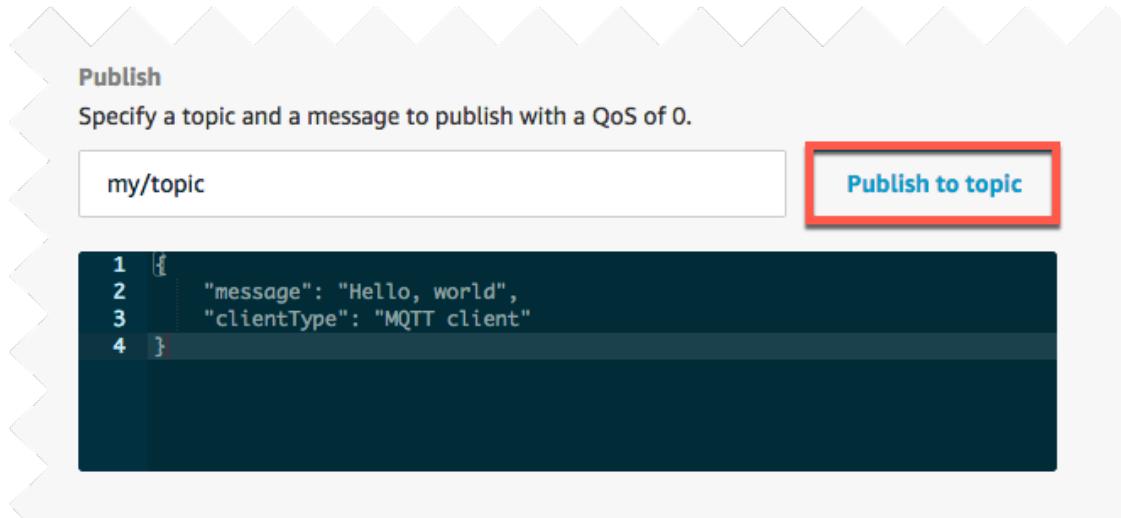
Non è consigliabile utilizzare informazioni di identificazione personale nei nomi degli argomenti.

Nella sezione relativa al payload del messaggio digita il codice JSON seguente:

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

}

Scegliere Publish to topic (Pubblica nell'argomento). Il messaggio dovrebbe venire visualizzato nel client MQTT AWS IoT. Scegliere my/topic nella colonna Subscription (Sottoscrizione) per visualizzare il messaggio.



Configurazione e test delle regole

Il motore di regole AWS IoT è in ascolto dei messaggi MQTT in ingresso che corrispondono a una regola. Quando viene ricevuto un messaggio con una corrispondenza, la regola esegue una determinata operazione con i dati contenuti nel messaggio MQTT, ad esempio la scrittura di dati in un bucket Amazon S3, la chiamata di una funzione Lambda o l'invio di un messaggio a un argomento Amazon SNS. In questa fase creerai e configurerai una regola per inviare i dati ricevuti da un dispositivo a un argomento Amazon SNS. Nello specifico, eseguirai le operazioni seguenti:

- Creazione di un argomento Amazon SNS.
- Sottoscrizione dell'argomento Amazon SNS usando un numero di telefono cellulare.
- Creazione di una regola che invia un messaggio all'argomento Amazon SNS quando viene ricevuto un messaggio dal dispositivo.
- Test della regola mediante il client MQTT.

Creazione di un argomento SNS

Puoi usare la console Amazon SNS per creare un argomento Amazon SNS.

Note

Amazon SNS non è disponibile in tutte le regioni AWS.

1. Aprire la [console Amazon SNS](#).
2. Nel riquadro a sinistra scegli Topics (Argomenti).

The screenshot shows the AWS SNS dashboard. On the left, there's a sidebar with links: SNS dashboard, Topics (which is selected and highlighted in orange), Applications, Subscriptions, and Text messaging (SMS). The main area has a header "SNS dashboard". Under "Common actions", there are five items: "Create topic" (with a description: Create a communication channel to send messages and subscribe to notifications), "Create platform application" (with a description: Create a platform application for mobile devices), "Create subscription" (with a description: Subscribe an endpoint to a topic to receive messages published to that topic), "Publish message" (with a description: Publish a message to a topic or as a direct publish to a platform endpoint), and "Publish text message (SMS)" (with a description: Publish a text message to a phone number). To the right, under "Resources", it says "You are using the following Amazon SNS resources in the us-west-2 region:" followed by a table with four rows: Topic (0), Subscriptions (0), Applications (0), and Endpoints (0). Below that is a "More info" section with links: Getting started, Documentation, API reference, Forums, and Service health.

3. Scegli Create new topic (Crea nuovo argomento).

The screenshot shows the "Topics" page. The sidebar on the left is identical to the previous dashboard. The main area has a header "Topics". Below it are three buttons: "Publish to topic", "Create new topic" (which is highlighted with a red box), and "Actions ▾". There's also a "Filter" input field. A table lists one topic: "My_SNS_Topic" with ARN "arn:aws:sns:us-west-2::My_SNS_Topic". At the bottom, it says "Total Items: 1" and "Selected Items: 0".

4. Digita un nome di argomento e un nome visualizzato e quindi scegli Create topic (Crea argomento).

The screenshot shows the "Create new topic" dialog. It has two input fields: "Topic name" containing "MylotSNSTopic" and "Display name" containing "SNS Topic". Below the fields is a large empty text area. At the bottom right are two buttons: "Cancel" and "Create topic" (which is highlighted with a red box).

Note

Non è consigliabile utilizzare informazioni di identificazione personale nei nomi degli argomenti Amazon SNS.

5. Prendi nota dell'ARN per l'argomento appena creato.

The screenshot shows the AWS SNS Topics page. On the left, there's a sidebar with links: SNS dashboard, Topics (which is selected and highlighted in orange), Applications, Subscriptions, and Text messaging (SMS). The main area has a title 'Topics' and three buttons: 'Publish to topic', 'Create new topic', and 'Actions'. Below these are 'Filter' and 'Name' columns. Two topics are listed:

| Name | ARN |
|--------------|-------------------------------------|
| My_SNS_Topic | arn:aws:sns:us-west-2::My_SNS_Topic |
| MyIoTNSTopic | arn:aws:sns:us-west-2::MyIoTNSTopic |

Sottoscrizione di un argomento Amazon SNS

Per ricevere messaggi SMS sul telefono cellulare, sottoscrivi l'argomento Amazon SNS.

1. Nella console Amazon SNS seleziona la casella di controllo accanto all'argomento appena creato. Dal menu Actions (Operazioni) scegli Subscribe to topic (Sottoscrivvi argomento).

The screenshot shows the same AWS SNS Topics page as before. A context menu is open over the 'MyIoTNSTopic' row. The menu items are: 'Edit topic display name', 'Subscribe to topic' (which is highlighted with a red box), 'Confirm a subscription', 'Edit topic policy', 'Edit topic delivery policy', 'Delivery status', and 'Delete topics'.

2. In Create subscription (Crea sottoscrizione) scegli SMS nell'elenco a discesa Protocol (Protocollo).

Nel campo Endpoint digita il numero di telefono di un cellulare abilitato per gli SMS e quindi scegli Create subscription (Crea sottoscrizione).

Note

Immetti il numero di telefono usando solo numeri e trattini.

Create subscription

| | |
|-----------|---|
| Topic ARN | arn:aws:sns:us-west-2:█████████████████████:MyIotSNSTopic |
| Protocol | SMS |
| Endpoint | 1-206-555-0100 |

Cancel **Create subscription**

La console Amazon SNS visualizzerà il seguente messaggio, ma è possibile che non venga ricevuto un messaggio di conferma.

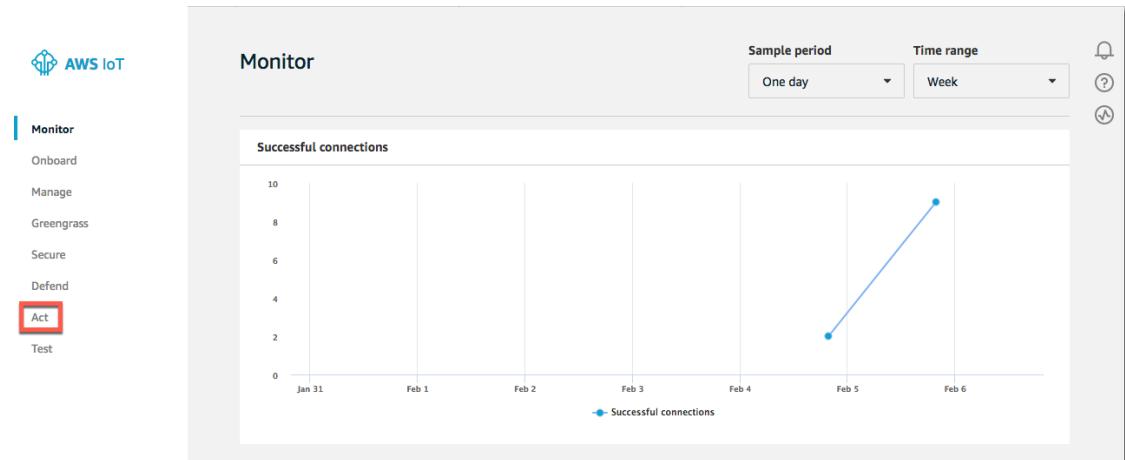
A confirmation message will be sent to the subscribed endpoint.
Once the subscription has been confirmed, the endpoint will receive notifications from this topic.

Creazione di una regola

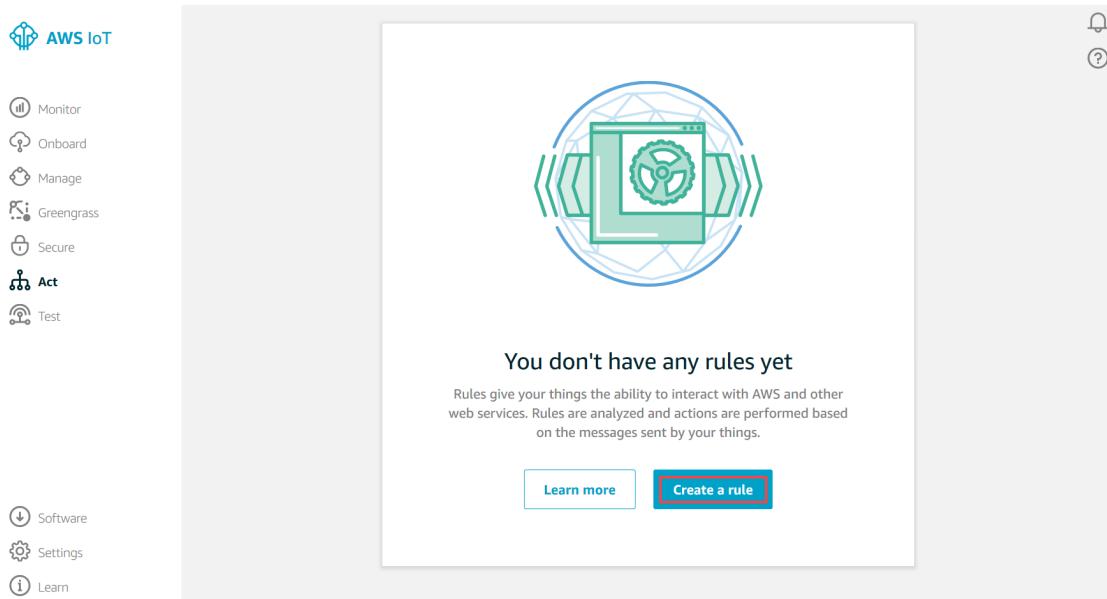
Le regole AWS IoT sono costituite da un filtro di argomenti, un'operazione della regola e, nella maggior parte dei casi, un ruolo IAM. I messaggi pubblicati negli argomenti che soddisfano il filtro di argomenti attivano la regola. L'operazione della regola definisce l'operazione da eseguire quando la regola viene attivata. Il ruolo IAM contiene una o più policy IAM che determinano i servizi AWS cui può accedere la regola. È possibile creare più regole in ascolto su un singolo argomento. Analogamente, è possibile creare una singola regola che viene attivata da più argomenti. Il motore di regole AWS IoT elabora continuamente i messaggi pubblicati negli argomenti che soddisfano il filtro di argomenti definito nelle regole.

In questo esempio creerai una regola che usa Amazon SNS per inviare una notifica SMS a un numero di telefono cellulare.

- Nel riquadro di navigazione a sinistra della console AWS IoT scegli Esecuzione azioni.



- Nella pagina Act (Esegui) scegli Create a rule (Crea una regola).



3. Nella pagina Create a rule (Crea una regola) digita un nome per la regola nel campo Name (Nome).

Note

Non è consigliabile utilizzare informazioni di identificazione personale nel nome delle regole.

Nel campo Description (Descrizione) digita una descrizione per la regola.

Create a rule

Create a rule to evaluate messages sent by your things and specify what to do when a message is received (for example, write data to a DynamoDB table or invoke a Lambda function).

Name
MyIotRule

Description
A rule for [AWS IoT Getting Started](#)

4. Scorrere fino a Rule query statement (Istruzione query regola). Scegli la versione più recente nell'elenco a discesa Using SQL version (Versione SQL in uso). Nel campo Rule query statement (Istruzione query regola) immettere **SELECT * FROM 'my/topic'**.

SELECT * specifica che vuoi inviare l'intero messaggio MQTT che ha attivato la regola. **FROM 'my/topic'** è il filtro di argomenti. Il motore di regole usa il filtro di argomenti per determinare le regole da attivare quando viene ricevuto un messaggio MQTT.

Rule query statement

Indicate the source of the messages you want to process with this rule.

Using SQL version

2016-03-23

Rule query statement

SELECT <Attribute> FROM <Topic Filter> WHERE <Condition>. For example: SELECT temperature FROM 'iot/topic' WHERE temperature > 50. To learn more, see [AWS IoT SQL Reference](#).

```
1 SELECT * FROM 'my/topic'
```

5. In Set one or more actions (Imposta una o più operazioni) scegli Add action (Aggiungi operazione).

Set one or more actions

Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. (*.required)

Add action

6. Nella pagina Select an action (Seleziona un'operazione) seleziona Send a message as an SNS push notification (Invia un messaggio come notifica push SNS) e quindi scegli Configure action (Configura operazione).

Select an action

Select an action.



Insert a message into a DynamoDB table
DYNAMODB



Split message into multiple columns of a DynamoDB table (DynamoDBv2)
DYNAMODBV2



Send a message to a Lambda function
LAMBDA



Send a message as an SNS push notification
SNS



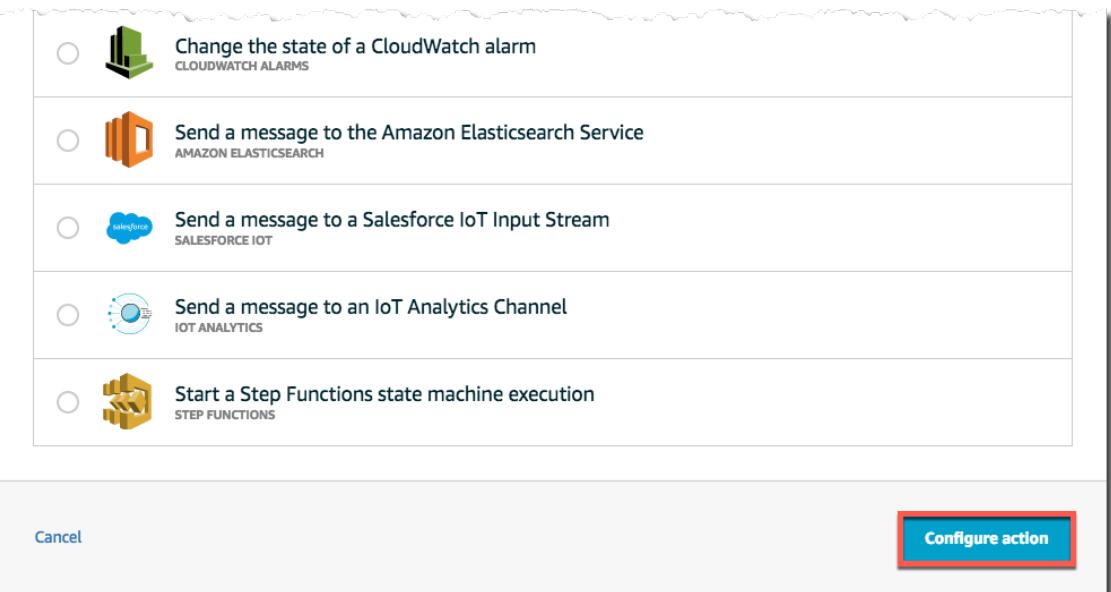
Send a message to an SQS queue
SQS



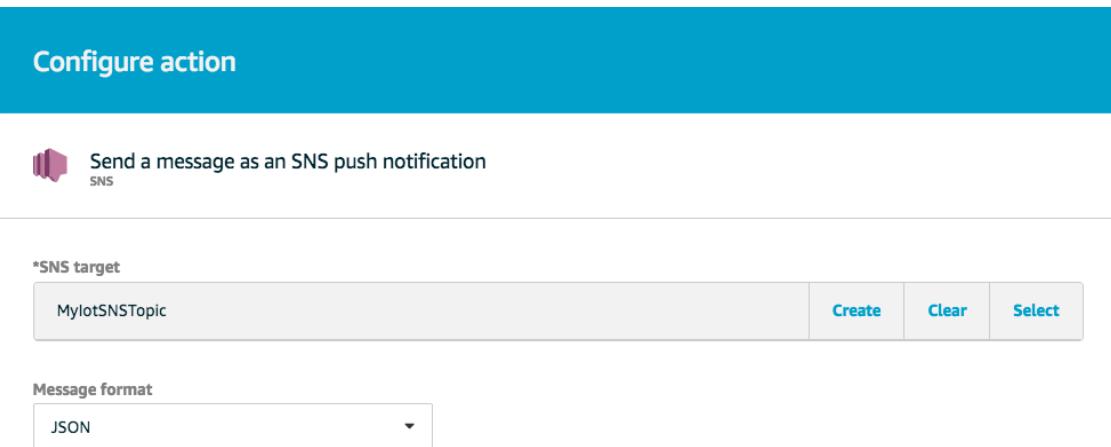
Send a message to an Amazon Kinesis Stream
AMAZON KINESIS



Republish a message to an AWS IoT topic
AWS IOT REPUBLISH



7. Nella pagina Configure action (Configura operazione), in SNS target (Destinazione SNS), scegli Select (Seleziona) per espandere l'elenco a discesa degli argomenti SNS. Quindi, scegli Select (Seleziona) accanto all'argomento Amazon SNS creato in precedenza. In Message format (Formato messaggio) seleziona JSON.



8. Assegna ora l'autorizzazione AWS IoT per la pubblicazione nell'argomento Amazon SNS per conto tuo quando viene attivata la regola. Scegli Create a new role (Crea un nuovo ruolo). Immetti un nome per il nuovo ruolo nel campo IAM role name (Nome ruolo IAM). Dopo avere immesso il nome, scegli Create a new role (Crea un nuovo ruolo).

Configure action

 Send a message as an SNS push notification
SNS

*SNS target

| | | | |
|---------------|------------------------|-----------------------|------------------------|
| MyiotSNSTopic | Create | Clear | Select |
|---------------|------------------------|-----------------------|------------------------|

Message format

| |
|------|
| JSON |
|------|

Choose or create a role to grant AWS IoT access to perform this action.

*IAM role name

| | | |
|---------------|-----------------------------|--|
| Choose a role | Update role | Create a new role |
|---------------|-----------------------------|--|

[Cancel](#) [Add action](#)

9. In IAM role name (Nome ruolo IAM), scegli Update role (Aggiorna ruolo) per applicare le autorizzazioni al nuovo ruolo creato, seleziona il nuovo ruolo creato e scegli Add action (Aggiungi operazione).

Configure action

 Send a message as an SNS push notification
SNS

*SNS target
MyiotSNSTopic [Create](#) [Clear](#) [Select](#)

Message format
JSON

Choose or create a role to grant AWS IoT access to perform this action.

*IAM role name
MyiotRuleRole [Update role](#) [Create a new role](#)

[Cancel](#) Add action

10. Nella pagina Create a Rule (Crea una regola) scegli Create rule (Crea regola).

Set one or more actions

Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. (*.required)

 Send a message as an SNS push notification
MyIoTTopic Remove Edit ▾

Add action

Error action

Optionally set an action that will be executed when something goes wrong with processing your rule.

Add action

Tags

Apply tags to your resources to help organize and identify them. A tag consists of a case-sensitive key-value pair. [Learn more](#) about tagging your AWS resources.

| Tag name | Value | Clear |
|---------------------------------------|--|--------------|
| Provide a tag name, e.g. Manufacturer | Provide a tag value, e.g. Acme-Corporation | Clear |

Add another

Cancel **Create rule**

Per ulteriori informazioni sulla creazione di regole, consulta la pagina relativa alle [regole AWS IoT](#).

Test della regola Amazon SNS

Puoi testare il ruolo utilizzando il client MQTT AWS IoT:

1. Nel riquadro di navigazione a sinistra della [console AWS IoT](#) scegli Test.
2. Nella sezione Pubblicare della pagina del client MQTT digita ... o l'argomento usato nella regola nel campo Specify a topic and a message to publish (Specifica un argomento e un messaggio da pubblicare) **my/topic**. Nella sezione relativa al payload del messaggio digita il codice JSON seguente:

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

3. Scegliere Publish to topic (Pubblica nell'argomento). Riceverai un messaggio Amazon SNS sul tuo telefono cellulare.

Complimenti! Hai creato e configurato una regola per inviare i dati ricevuti da un dispositivo a un argomento Amazon SNS.

Fasi successive

Per ulteriori informazioni sulle regole AWS IoT, consulta [Tutorial sulle regole AWS IoT \(p. 50\)](#) e [Regole AWS IoT \(p. 254\)](#).

Creazione e monitoraggio di un processo AWS IoT

I processi AWS IoT permettono di distribuire e monitorare attività di gestione nel parco istanze di dispositivi. Puoi usare processi per inviare operazioni remote a uno o più dispositivi contemporaneamente, controllare la distribuzione di processi nei dispositivi e monitorare lo stato di esecuzione dei processi attuale e precedente per ogni dispositivo.

Questo argomento mostra come creare e distribuire un processo di esempio in un dispositivo. Vengono descritte le operazioni necessarie per creare un processo e monitorarne gli eventi in un dispositivo configurato per comunicare con AWS IoT. Queste istruzioni presuppongono l'uso di Raspberry Pi, ma possono essere adattate per altri dispositivi basati su Linux.

Ecco alcuni possibili scenari per l'uso di processi:

- Aggiornamento di firmware, software o file del dispositivo, ad esempio dei certificati di sicurezza.
- Esecuzione di attività amministrative, come il riavvio dei dispositivi o l'esecuzione di operazioni di diagnostica.
- Ripristino delle impostazioni di fabbrica o di altri stati noti corretti dei dispositivi.

Connessione del dispositivo ad AWS IoT

Eseguire la procedura seguente per connettere un dispositivo Raspberry Pi ad AWS IoT.

1. Completa il tutorial [Connessione del componente Raspberry Pi](#). Al termine, avrai un oggetto AWS IoT registrato nell'account AWS denominato MyRaspberryPi. Avrai anche certificati di sicurezza completamente configurati nel dispositivo.
2. Completa il tutorial [Uso dell'SDK AWS IoT per dispositivi per JavaScript](#). Al termine, il dispositivo sarà connesso ad AWS IoT e potrai eseguire il codice di esempio fornito con l'SDK di dispositivo AWS IoT per JavaScript.

Il dispositivo è ora pronto per usare processi AWS IoT.

Esecuzione del processo di esempio

L'SDK di dispositivo AWS IoT per JavaScript include un esempio denominato `jobs-example.js`. Questo esempio è in grado di ricevere messaggi dalla [console AWS IoT](#) per verificare la connettività con la piattaforma AWS IoT. Può anche ricevere ed elaborare esecuzioni di processi che hanno origine dal servizio AWS IoT Jobs.

Puoi eseguire questo esempio usando il comando seguente. Usa l'endpoint REST del dispositivo Raspberry Pi come valore del parametro `-H`.

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

Se hai creato un file di configurazione che contiene il nome dell'oggetto e l'endpoint host (endpoint REST del dispositivo), puoi usare il comando seguente.

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

Creazione di un documento del processo

Un documento del processo è un documento JSON che fornisce tutte le informazioni necessarie al dispositivo per l'esecuzione di un processo. L'SDK di dispositivo AWS IoT per JavaScript usa una proprietà denominata `operation` per instradare documenti dei processi a gestori specifici. Il programma `jobs-example.js` include un gestore di esempio per un'operazione denominata `customJob`. Creeremo ora un documento di un processo denominato `example-job.json` per questo gestore. Il file `example-job.json` deve contenere l'oggetto JSON seguente.

```
{  
    "operation": "customJob",  
    "otherInfo": "someValue"  
}
```

Per ulteriori documenti di processi di esempio, consulta la documentazione per l'esempio [jobs-agent.js](#).

Creazione di un processo

Puoi ora creare un processo per la distribuzione del documento del processo in tutti i dispositivi specificati. Per creare un processo, puoi usare la console AWS IoT, l'SDK AWS IoT o l'interfaccia a riga di comando di AWS IoT.

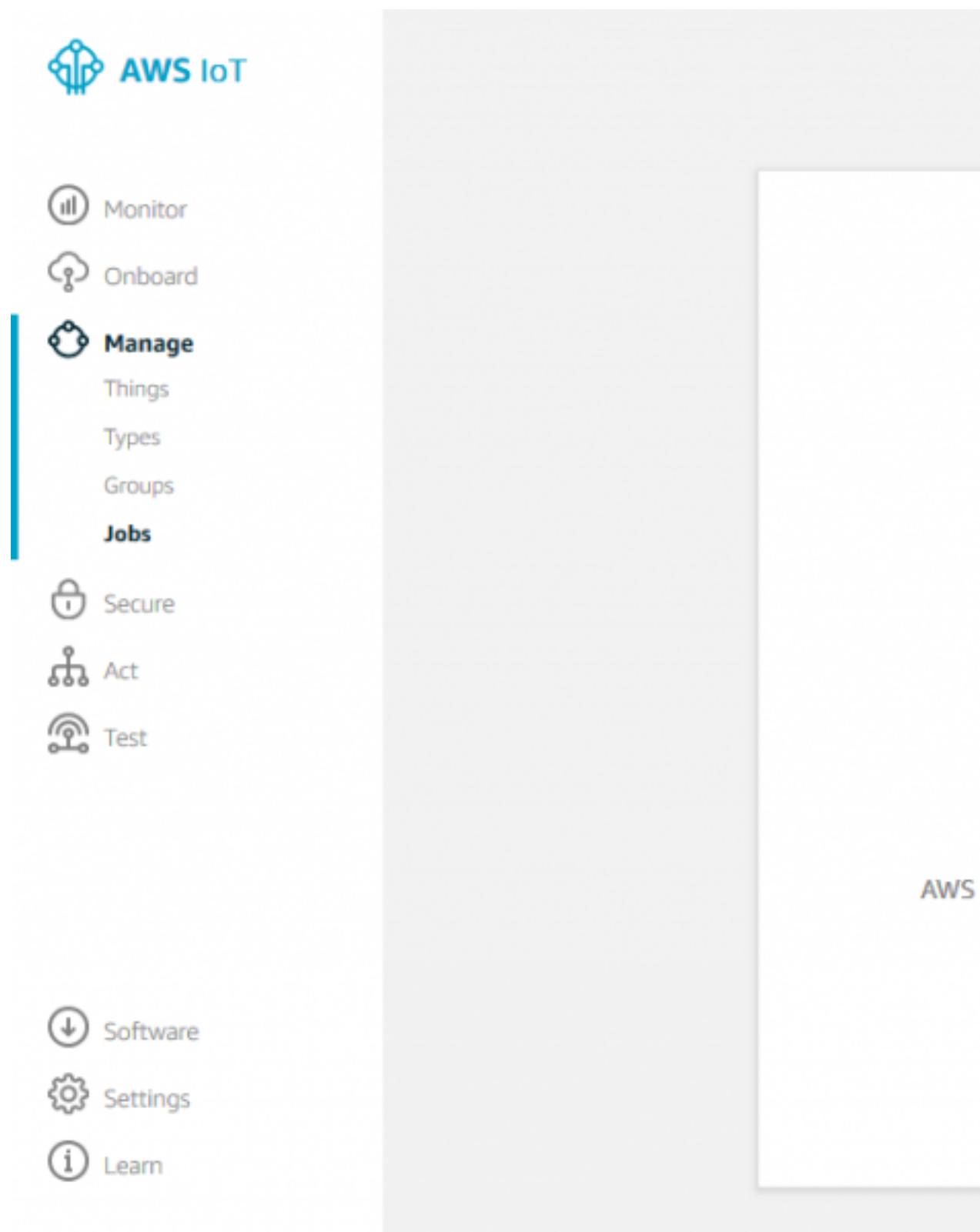
L'esempio seguente mostra come creare un processo usando l'[interfaccia a riga di comando di AWS IoT](#).

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

Se archivi il documento del processo in Amazon Simple Storage Service, usa il parametro `-document-source` invece del parametro `-document` per specificare l'URL Amazon S3 per il documento del processo.

Se preferisci usare la console AWS IoT, completa questa procedura per creare un processo:

1. Carica il documento del processo in un bucket Amazon S3. Per informazioni sul caricamento di documenti in Amazon S3, consulta [Come caricare file e cartelle in un bucket S3](#) nella Guida per l'utente della console Amazon Simple Storage Service.
2. Nella console AWS IoT scegli Gestione e quindi Processi.
3. Scegli Create a job (Crea un processo).



4. Nella pagina Seleziona un processo scegli Crea processo personalizzato.

The screenshot shows a mobile application interface for creating a job in AWS IoT Device Management. At the top, there is a large blue header bar with the text "CREATE JOB" and "Select a job". Below this, there are four main sections, each represented by a card:

- Select a job**: A brief description explaining what jobs are.
- Create a custom job**: A description of sending a request to acquire an executable job file from a device.
- Create an Amazon FreeRTOS Over-the-air (OTA) update job**: A description of sending a firmware image securely over-the-air to FreeRTOS-based devices.
- Create a Greengrass Core update job**: A description of creating a snapshot job to update Greengrass Core or OTA agent version.

5. Nella pagina Creazione di un processo immetti un ID processo univoco.

Note

Non è consigliabile utilizzare informazioni di identificazione personale nell'ID processo.

In Selezione i dispositivi da aggiornare seleziona il dispositivo che hai connesso ad AWS IoT.

The screenshot shows the 'CREATE JOB' screen in the AWS IoT console. At the top, there is a back arrow icon and the text 'CREATE JOB'. Below this, the heading 'Create a job' is displayed. The first section, 'Job ID', contains a text input field with the value 'example-job-01', which is highlighted with a red border. The next section, 'Description', has an empty text input field. Below these, the heading 'Select devices to update' is shown, followed by the instruction 'Browse and select the devices you want to include in this job.' A summary message indicates '1 thing(s) and 0 thing group(s) selected.' The 'Things' tab is active, showing a search bar and a list item 'MyRaspberryPi' with a checked checkbox, also highlighted with a red border.

CREATE JOB

Create a job

Job ID

example-job-01

Description

Select devices to update

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

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

Things Thing Groups Summary

Search

MyRaspberryPi

6. Scorri verso il basso la sezione Aggiunta di un file di processo e scegli il documento del processo che hai caricato in Amazon S3. In Tipo di processo seleziona Il processo sarà completo dopo la distribuzione nei dispositivi/gruppi selezionati (snapshot). L'altra opzione, Continuerà a essere distribuito in tutti i dispositivi aggiunti ai gruppi selezionati (continuo), è per la distribuzione di un processo in gruppi di dispositivi man mano che a ogni gruppo vengono aggiunti dispositivi. Lascia invariata l'impostazione Configurazione rollout esecuzioni processi. Scegliere Create (Crea).

Add a job file

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

`example-job.json`

Pre-sign resource URLs

For an extra layer of security, you can pre-sign URLs that refer to resources in your job file.

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

Job type

A job can run on the devices and/or groups selected, or remain open until completed.

Your job will complete after deploying to the selected devices

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

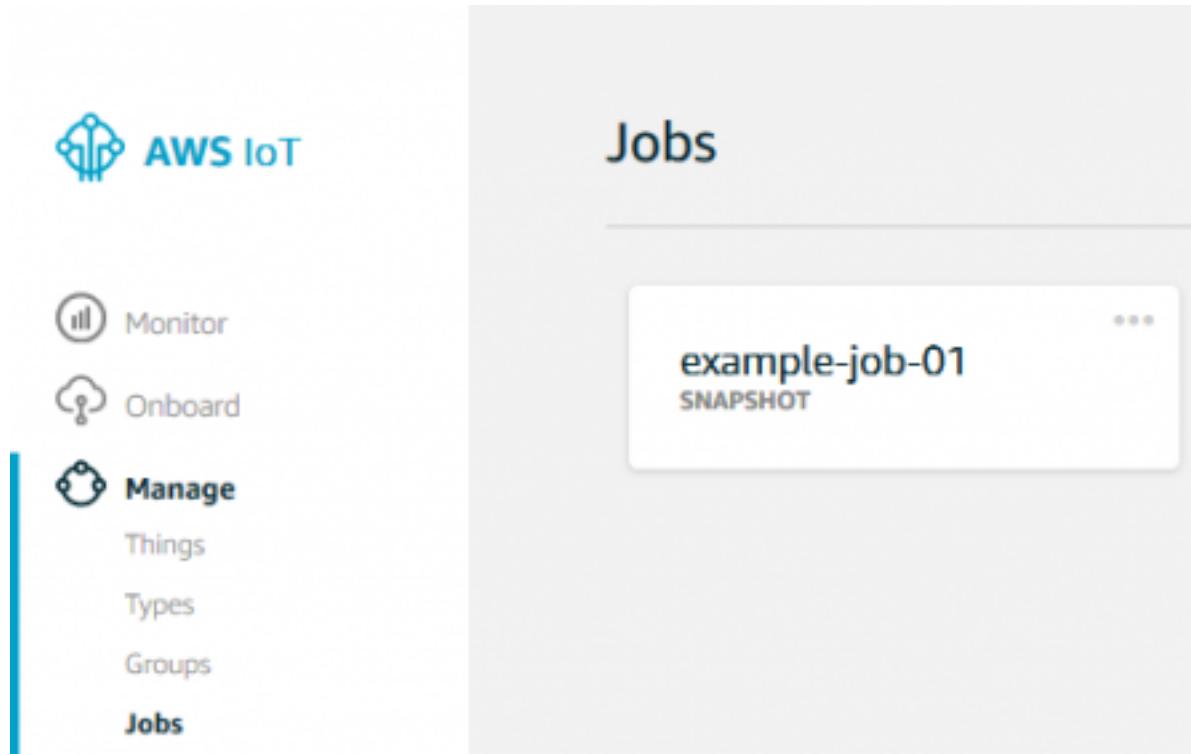
Job executions rollout configuration

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

Maximum per minute (1-1000)

1000

7. Il nuovo processo verrà visualizzato nella pagina Processi.



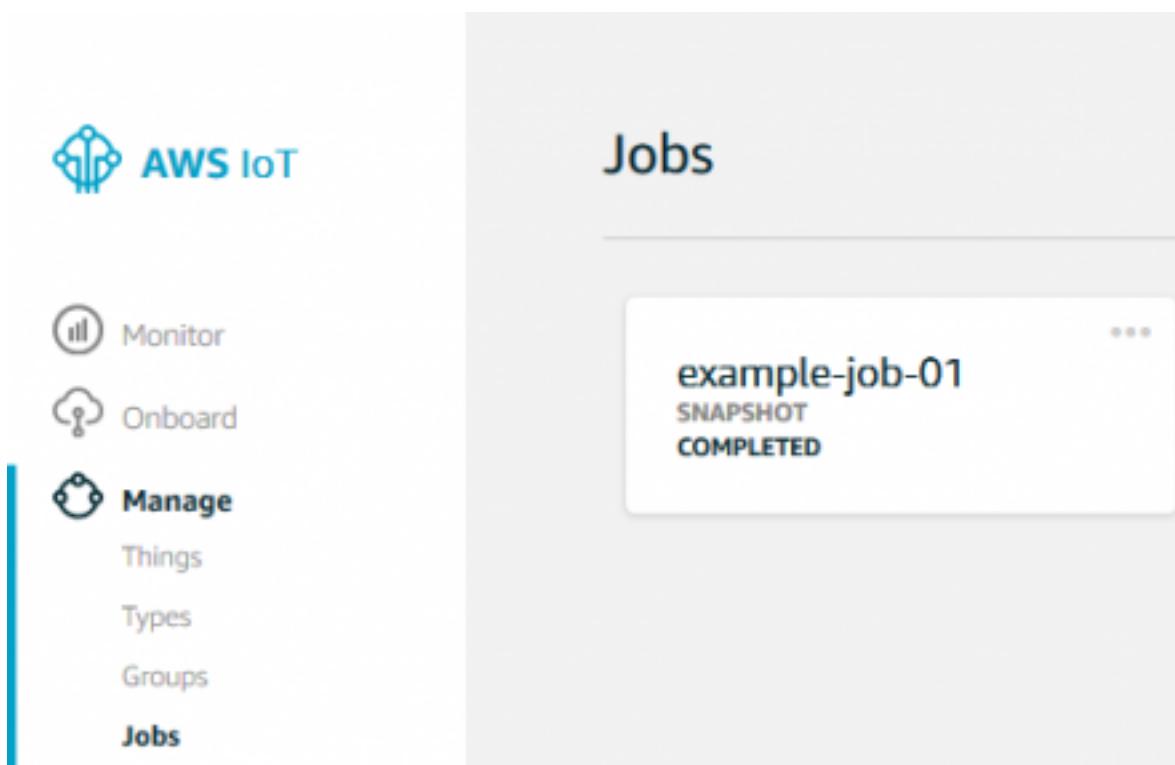
Per ulteriori informazioni sulla creazione e la distribuzione di processi, consulta la [documentazione di AWS IoT Jobs](#).

Esecuzione del processo in un dispositivo

Al termine della creazione del processo, il servizio Jobs invia una notifica che segnala la presenza di un processo in sospeso nel dispositivo. Il dispositivo ottiene i dettagli del processo e il documento del processo tramite l'API [NextJobExecutionChanged](#). L'esempio `jobs-example.js` che hai già eseguito esegue il processo nel dispositivo. Quando il processo è completo, l'esempio ne pubblica lo stato completato usando l'API [UpdateJobExecution](#). Quando esegui l'esempio nel dispositivo, viene restituito l'output seguente.

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

Aggiornando la pagina Processi, potrai notare che il processo è stato completato con successo.



Monitoraggio dello stato del processo con eventi di processo e di esecuzione di processi

Puoi usare eventi Job e JobExecution per monitorare lo stato del processo.

Si tratta di un utile metodo per comunicare a utenti, amministratori di sistema o altri membri del sistema che un processo è completo o che lo stato di esecuzione del processo è cambiato. Ad esempio, puoi comunicare a un utente un aggiornamento firmware in un dispositivo o informare un amministratore di sistema riguardo a un problema nel parco istanze di dispositivi che deve essere esaminato e risolto.

Gli eventi di processo per il processo in questo esempio vengono pubblicati negli argomenti seguenti quando il processo viene completato o annullato.

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

Gli eventi di esecuzione di processi per il processo in questo esempio vengono inviati agli argomenti seguenti quando l'esecuzione del processo raggiunge uno dei possibili stati finali.

```
$aws/events/jobExecution/example-job-01/succeeded  
$aws/events/jobExecution/example-job-01/failed  
$aws/events/jobExecution/example-job-01/rejected  
$aws/events/jobExecution/example-job-01/canceled  
$aws/events/jobExecution/example-job-01/removed
```

Quando l'esecuzione del processo viene completata con successo, AWS IoT pubblica un evento [JobExecution](#) di operazione riuscita. Puoi visualizzare questo evento passando alla pagina Test in AWS IoT e sottoscrivendo l'argomento `$aws/events/jobExecution/example-job-01/succeeded` nel client MQTT.

The screenshot shows two side-by-side interfaces. On the left is the AWS IoT Test interface, which has a sidebar with icons for Monitor, Onboard, Manage, Greengrass, Secure, Act, and Test. The Test icon is highlighted with a red border. On the right is an MQTT client interface titled 'MQTT client'. It features a 'Subscriptions' section with a blue header, a 'Subscribe to a topic' button, and a 'Publish to a topic' button. A red box highlights the topic path '\$aws/events/jobExecution/example-job-01/succeeded' in the 'Subscriptions' section. Below the MQTT client interface, there is some partially visible text: 'Subscribe', 'Devices p receive th', 'Subscribe', and 'Max mess 100'.

Quando l'esecuzione del processo per il dispositivo viene completata con successo, viene visualizzato il messaggio seguente.

Publish

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

```
$aws/events/jobExecution/example-job-01/succeeded
```

```
1  [
2    "message": "Hello from AWS IoT console"
3  ]
```

\$aws/events/jobExecution/example-job-01/...

Dec 19, 2017

```
{
  "eventType": "JOB_EXECUTION",
  "eventId": "af479061-a800-4d1f-a557-bbcd71243f7e",
  "timestamp": "1513709703",
  "operation": "succeeded",
  "jobId": "example-job-01",
  "thingArn": "arn:aws:iot:us-east-1:xxxxxxxxxxxx:thing",
  "status": "SUCCEEDED",
  "statusDetails": {
    "key": "value"
  }
}
```

AWS IoT pubblica anche un evento job di operazione completata. Puoi visualizzare questo evento sottoscrivendo l'argomento \$aws/events/job/example-job-01/completed nel client MQTT.

Publish

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

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

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

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

Dec 19, 2017

```
{
  "eventType": "JOB",
  "eventId": "a1817d74-0fld-42b3-b03f-accfc90af41e",
  "timestamp": "1513709645",
  "operation": "completed",
  "jobId": "example-job-01",
  "status": "COMPLETED",
  "targetSelection": "SNAPSHOT",
  "targets": [
    "arn:aws:iot:us-east-1:[REDACTED]:thing/MyRaspbe"
  ],
  "description": "Job example-job-01 for Thing MyRaspb",
  "completedAt": "1513709645105",
  "createdAt": "1513709615488",
  "lastUpdatedAt": "1513709645105",
  "jobProgressDetails": {
    "numberOfCanceledThings": 0,
    "numberOfRejectedThings": 0,
    "numberOfFailedThings": 0,
    "numberOfRemovedThings": 0,
    "numberOfSucceededThings": 1
  }
}
```

Tutorial sulle regole AWS IoT

I tutorial seguenti mostrano come creare e verificare regole AWS IoT. Prima di iniziare, assicurati di completare il [Tutorial sulle nozioni di base su AWS IoT \(p. 5\)](#), in cui viene mostrato come creare un account AWS e registrare un dispositivo in AWS IoT, i prerequisiti per questi tipi di tutorial.

Lo scenario in questo tutorial è una serra con file di piante. Ogni pianta dispone di un sensore di umidità. In un intervallo predeterminato, il sensore di umidità invia i suoi dati a AWS IoT. Il motore di regole AWS IoT riceve questi dati e li scrive in una tabella DynamoDB. Viene creata una regola per scrivere i dati in DynamoDB e i sensori vengono emulati utilizzando il client MQTT AWS IoT.

Una regola AWS IoT è costituita da un'istruzione SQL SELECT, un filtro di argomenti e un'operazione. I dispositivi inviano informazioni a AWS IoT pubblicando messaggi in argomenti MQTT. L'istruzione SQL SELECT ti permette di estrarre dati da un messaggio MQTT in ingresso. Il filtro di argomenti di una regola AWS IoT specifica uno o più argomenti MQTT. La regola viene attivata quando viene ricevuto un messaggio MQTT in un argomento che corrisponde al filtro di argomenti. Le operazioni delle regole ti permettono di recuperare le informazioni estratte da un messaggio MQTT e di inviarle a un altro servizio AWS. Le operazioni delle regole sono definite per servizi AWS come Amazon DynamoDB, AWS Lambda, Amazon SNS e Amazon S3. Usando una regola Lambda, puoi richiamare altri servizi AWS o Web di terze parti. Per un elenco completo delle operazioni delle regole, consulta [Operazioni delle regole AWS IoT \(p. 261\)](#).

In questi tutorial si pressuppone l'uso del client MQTT AWS IoT e di `my/greenhouse` come filtro di argomenti nelle regole.

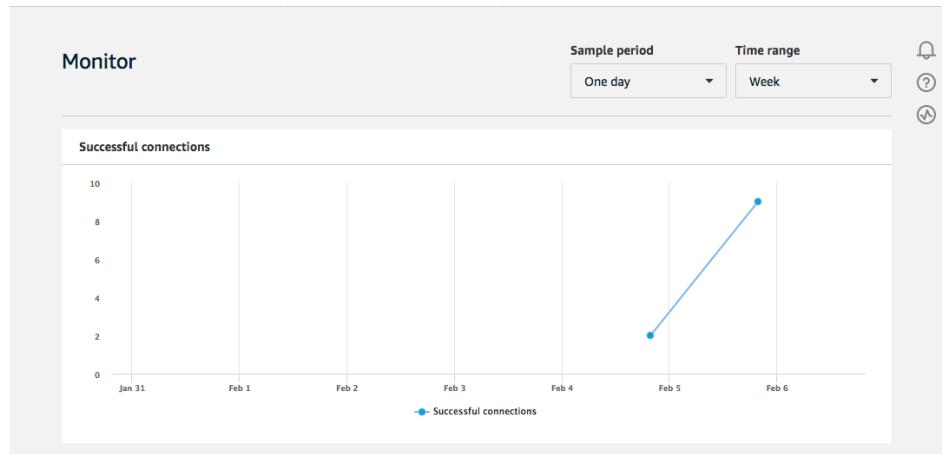
Puoi anche usare il tuo dispositivo, ma devi saper identificare l'argomento MQTT in cui il dispositivo esegue la pubblicazione per poterlo specificare come filtro di argomenti nella regola. Per ulteriori informazioni, consulta la sezione relativa alle [regole AWS IoT \(p. 254\)](#).

Creazione di una regola Amazon DynamoDB

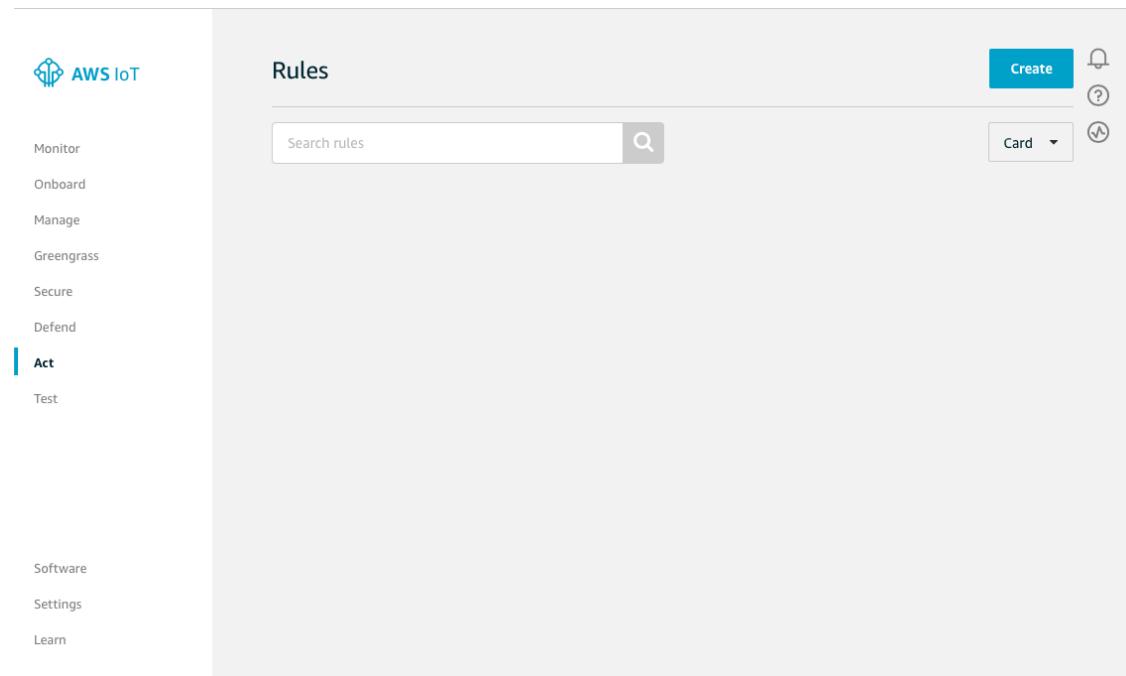
Le regole DynamoDB permettono di recuperare informazioni da un messaggio MQTT in ingresso e di scriverle in una tabella DynamoDB.

Per creare una regola DynamoDB

- Nella console [AWS IoT](#), nel riquadro di navigazione, scegliere Agisci.



- Nella pagina Rules (Regole) scegli Create (Crea).



3. Nella pagina Create a rule (Crea una regola), immettere un nome e una descrizione per la regola.

Note

Non è consigliabile utilizzare informazioni personali identificabili nei nomi e nelle descrizioni delle regole.

Create a rule

Create a rule to evaluate messages sent by your things and specify what to do when a message is received (for example, write data to a DynamoDB table or invoke a Lambda function).

Name

Description

4. In Rule query statement (Istruzione query regola), scegliere la versione più recente dall'elenco Using SQL version (Uso della versione SQL). In Rule query statement (Istruzione query regola), immettere:

```
SELECT * FROM 'my/greenhouse'
```

("SELECT *" specifica che si desidera inviare l'intero messaggio MQTT che ha attivato la regola.
"FROM 'my/greenhouse'" indica al motore di regole di attivare questa regola quando viene ricevuto un messaggio il cui argomento corrisponde al filtro argomenti. Selezionare Aggiungi operazione.

Rule query statement

Indicate the source of the messages you want to process with this rule.

Using SQL version

2016-03-23 ▾

Rule query statement

SELECT <Attribute> FROM <Topic Filter> WHERE <Condition>. For example: SELECT temperature FROM 'iot/topic' WHERE temperature > 50. To learn more, see [AWS IoT SQL Reference](#).

```
1 SELECT * FROM 'my/greenhouse'
```

Set one or more actions

Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. (*.required)

Add action

5. Nella pagina Select an action (Seleziona un'operazione), scegliere Insert a message into a DynamoDB table (Inserisci un messaggio in una tabella DynamoDB), quindi Configure action (Configura operazione).

Select an action

Select an action.

-  Insert a message into a DynamoDB table
DYNAMODB
-  Split message into multiple columns of a DynamoDB table (DynamoDBv2)
DYNAMODBV2
-  Send a message to a Lambda function
LAMBDA
-  Send a message as an SNS push notification
SNS
-  Send a message to an SQS queue
SQS
-  Send a message to an Amazon Kinesis Stream
AMAZON KINESIS
-  Republish a message to an AWS IoT topic
AWS IOT REPUBLISH
-  Store a message in an Amazon S3 bucket
S3
-  Send a message to an Amazon Kinesis Firehose stream
AMAZON KINESIS FIREHOSE
-  Send message data to CloudWatch
CLOUDWATCH METRICS
-  Change the state of a CloudWatch alarm
CLOUDWATCH ALARMS
-  Send a message to the Amazon Elasticsearch Service
AMAZON ELASTICSEARCH
-  Send a message to a Salesforce IoT Input Stream
SALESFORCE IOT
-  Send a message to an IoT Analytics Channel
IOT ANALYTICS
-  Start a Step Functions state machine execution
STEP FUNCTIONS

[Cancel](#) Configure action

6. Nella pagina Configure action (Configura operazione), scegli Create a new resource (Crea una nuova risorsa).

Configure action

 Insert a message into a DynamoDB table
DYNAMODB

The table must contain Partition and Sort keys.

*Table name
Choose a resource ▾  **Create a new resource**

*Partition key
Required field does not exist

*Partition key type
Required field does not exist

*Partition key value

Sort key
Optional field does not exist

Sort key type
Optional field does not exist

Sort key value

Write message data to this column

Operation 

Choose or create a role to grant AWS IoT access to perform this action.

No role selected 

Cancel 

7. Nella pagina Amazon DynamoDB scegli Create table (Crea tabella).

The screenshot shows the Amazon DynamoDB homepage. At the top center is the AWS logo and the text "Amazon DynamoDB". Below it is a brief description: "Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. Its flexible data model and reliable performance make it a great fit for mobile, web, gaming, ad-tech, IoT, and many other applications." Below the description is a large blue "Create table" button. Underneath the button is a link to "Getting started guide".

Below the main heading are three main sections:

- Create tables**: Represented by an icon of three cylinders with a plus sign. Below the icon is the text "Create tables".
- Add and query items**: Represented by an icon of a document with a magnifying glass. Below the icon is the text "Add and query items".
- Monitor and manage tables**: Represented by an icon of a monitor displaying a graph with a checkmark. Below the icon is the text "Monitor and manage tables".

At the bottom of the page, there are links: "More about DynamoDB throughput", "DynamoDB API reference", and "Monitoring tables".

In the footer, there is a link to "DynamoDB documentation & support" and a link to "Getting started guide | FAQ | Developer guide | Forums | Report an issue".

- Nella pagina Create DynamoDB table (Crea tabella DynamoDB), immettere un nome nel campo Table name (Nome tabella). In Chiave di partizione, immettere **Row**. Selezionare Aggiungi chiave di ordinamento e quindi immettere **PositionInRow** nel campo Chiave di ordinamento. Row rappresenta una fila di piante in una serra. PositionInRow rappresenta la posizione di una pianta nella fila. Scegliere String (Stringa) per la partizione e le chiavi di ordinamento, quindi selezionare Create (Crea). Saranno necessari alcuni secondi per creare la tabella DynamoDB. Chiudi la scheda del browser in cui è aperta la console Amazon DynamoDB. Se non si chiude la scheda, la tabella DynamoDB non viene visualizzata nell'elenco Table name (Nome tabella) nella pagina Configure action (Configura operazione) della console AWS IoT.

The screenshot shows the "Create DynamoDB table" wizard. The first step is "Table settings". It includes fields for "Table name*" (set to "GreenhouseTable") and "Primary key*". The primary key is set to "Partition key" with "Row" as the value. A checkbox "Add sort key" is checked, and "PositionInRow" is selected as the sort key. Below the table settings, there is a section titled "Table settings" with a note: "Default settings provide the fastest way to get started with your table. You can modify these default settings now or after your table has been created." A checkbox "Use default settings" is checked. To the right of the checkbox is a list of default settings:

- No secondary indexes.
- Provisioned capacity set to 5 reads and 5 writes.
- Basic alarms with 80% upper threshold using SNS topic "dynamodb*".
- Encryption at Rest with DEFAULT encryption type **NEW!**

Below the table settings, there is a note in a box: "You do not have the required role to enable Auto Scaling by default. Please refer to documentation."

At the bottom of the page, there is a note: "Additional charges may apply if you exceed the AWS Free Tier levels for CloudWatch or Simple Notification Service. Advanced alarm settings are available in the CloudWatch management console." There are "Cancel" and "Create" buttons at the bottom right.

9. Nella pagina Configure action (Configura operazione), scegliere la nuova tabella nell'elenco Table name (Nome tabella). In Partition key value (Valore della chiave di partizione), immettere `#{row}`. Questo indica alla regola di recuperare il valore dell'attributo `row` dal messaggio MQTT e di scriverlo nella colonna Row (Riga) della tabella DynamoDB. In Sort key value (Valore della chiave di ordinamento), immettere `#{pos}`. In questo modo, il valore dell'attributo `pos` viene scritto nella colonna PositionInRow. Lascia vuoto il campo Write message data to this column (Scrivi i dati del messaggio in questa colonna). Per impostazione predefinita, l'intero messaggio viene scritto in una colonna della tabella denominata Payload. Scegliere Create a new role (Crea un nuovo ruolo).

Configure action

Insert a message into a DynamoDB table

The table must contain Partition and Sort keys.

*Table name

GreenhouseTable

| | | |
|----------------|---------------------|----------------------|
| *Partition key | *Partition key type | *Partition key value |
| Row | STRING | #{row} |
| Sort key | Sort key type | Sort key value |
| PositionInRow | STRING | #{pos} |

Write message data to this column

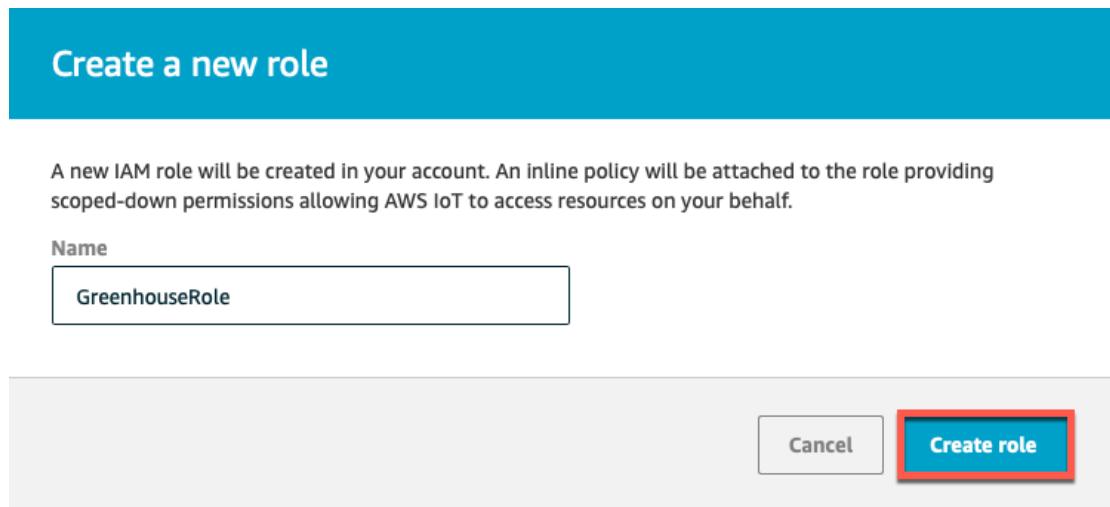
Operation [?](#)

Choose or create a role to grant AWS IoT access to perform this action.

No role selected

Cancel

10. In Create a new role (Crea un nuovo ruolo), immettere un nome univoco in Name (Nome), quindi scegliere Create role (Crea ruolo).



11. Selezionare Add action (Aggiungi operazione).

Configure action

Insert a message into a DynamoDB table
DYNAMODB

The table must contain Partition and Sort keys.

*Table name
GreenhouseTable

*Partition key
Row *Partition key type STRING *Partition key value \${row}

Sort key
PositionInRow Sort key type STRING Sort key value \${pos}

Write message data to this column

Operation

Choose or create a role to grant AWS IoT access to perform this action.
GreenhouseRole Policy Attached ✓

12. Scegliere Create rule (Crea regola) per creare la regola.

Create a rule

Create a rule to evaluate messages sent by your things and specify what to do when a message is received (for example, write data to a DynamoDB table or invoke a Lambda function).

Name

GreenhouseRule

Description

A DynamoDB rule for a greenhouse

Rule query statement

Indicate the source of the messages you want to process with this rule.

Using SQL version

2016-03-23

Rule query statement

SELECT <Attribute> FROM <Topic Filter> WHERE <Condition>. For example: SELECT temperature FROM 'iot/topic' WHERE temperature > 50. To learn more, see [AWS IoT SQL Reference](#).

```
1 SELECT * FROM 'my/greenhouse'
```

Set one or more actions

Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. (*.required)



Insert a message into a DynamoDB table
GreenhouseTable

Remove Edit ▾

Add action

Error action

Optionally set an action that will be executed when something goes wrong with processing your rule.

Add action

Tags

Apply tags to your resources to help organize and identify them. A tag consists of a case-sensitive key-value pair. [Learn more](#) about tagging your AWS resources.

Tag name

Provide a tag name, e.g. Manufacturer

Value

Provide a tag value, e.g. Acme-Corporation

Clear

Add another

Test di una regola Amazon DynamoDB

1. Per testare la regola, aprire la console AWS IoT e scegliere Test (Test) dal riquadro di navigazione.
2. Scegliere Publish to a topic (Pubblica in un argomento). Nella sezione Publish (Pubblica), immettere **my/greenhouse** come l'argomento. Nell'area dei messaggi, immettere il seguente JSON:

```
{  
    "row" : "0",  
    "pos" : "0",  
    "moisture" : "75"  
}
```

The screenshot shows the AWS IoT MQTT client interface. On the left, there's a sidebar with 'Subscriptions' and two buttons: 'Subscribe to a topic' and 'Publish to a topic'. The 'Publish to a topic' button is highlighted with a red box. The main area has a header 'Connected as iotconsole-' with a dropdown arrow. Below it, there are sections for 'Subscription topic' (with a required field 'Specify a topic to subscribe to, e.g. myTopic/1' and a 'Subscribe to topic' button), 'Max message capture' (set to 100), 'Quality of Service' (radio button selected for level 0), and 'MQTT payload display' (radio button selected for 'Auto-format JSON payloads (improves readability)'). In the bottom section, there's a 'Publish' area with a 'topic' input field containing 'my/greenhouse' and a 'Publish to topic' button (also highlighted with a red box). Below the input field is a code editor showing the JSON message from the previous step.

Tornare alla console DynamoDB e scegliere Tables (Tabelle).

The screenshot shows the AWS DynamoDB console. On the left, a sidebar menu has 'Tables' highlighted with a red box. The main content area is titled 'Create table' and contains a brief description of Amazon DynamoDB. Below this is a 'Recent alerts' section stating 'No CloudWatch alarms have been triggered.' and a link to 'View all in CloudWatch'. A section titled 'Total capacity for US West (Oregon)' shows provisioning details: Provisioned read capacity 5, Reserved read capacity 0; Provisioned write capacity 5, Reserved write capacity 0. Under 'Service health', there is a table with one row: 'Amazon DynamoDB (Oregon)' status 'Service is operating normally' with a green checkmark icon. A link 'View complete service health details' is also present.

Selezionare la GreenhouseTable e quindi scegliere la scheda Items (Elementi). I dati vengono visualizzati nella scheda Items (Elementi).

The screenshot shows the 'Items' tab for the 'GreenhouseTable' table. The table has one item listed: 'Row' 0, 'PositionInRow' 1, 'payload' { "moisture" : { "S" : "75" }, "pos" : { "S" : "1" }, "row" : { "S" : "0" } }. The 'Scan' dropdown is set to 'Scan' and the search bar contains 'Scan: [Table] GreenhouseTable: Row, PositionInRow'.

Creazione di una regola AWS Lambda

Puoi definire una regola che richiama una funzione Lambda, trasferendo i dati dal messaggio MQTT che ha attivato la regola. In questo modo è possibile estrarre i dati del messaggio in ingresso e quindi chiamare un altro servizio AWS o di terze parti. In questo tutorial si presuppone che sia stato completato il [tutorial Nozioni di base su AWS IoT \(p. 5\)](#), nel quale si crea un argomento Amazon SNS a cui si effettua la sottoscrizione. Verrà creata una funzione Lambda per la pubblicazione di un messaggio nell'argomento Amazon SNS creato nel [Tutorial sulle nozioni di base su AWS IoT \(p. 5\)](#). Verrà inoltre creata una regola Lambda che chiama la funzione Lambda, trasferendo alcuni dati dal messaggio MQTT che ha attivato la regola.

In questo tutorial, verrà utilizzato il client MQTT AWS IoT per inviare un messaggio che attiva la regola.

Creare una funzione Lambda

- Nella [console AWS Lambda](#) scegliere Crea funzione.

The screenshot shows the AWS Lambda Functions page. On the left, there's a sidebar with 'AWS Lambda' at the top, followed by 'Dashboard', 'Applications', 'Functions' (which is highlighted in orange), and 'Layers'. The main area is titled 'Functions (1)'. It has a search bar with 'Filter by tags and attributes or search by keyword'. Below the search bar is a table with columns: Function name, Description, Runtime, Code size, and Last modified. A single row is shown: 'myIoTLambdaFunction' with the description 'A starter AWS Lambda function.', runtime 'Node.js 8.10', code size '330 bytes', and last modified '3 days ago'. At the top right of the main area is a red 'Create function' button.

2. Nella pagina Crea funzione scegliere Use a blueprint (Usa un piano). Nel campo del filtro Blueprints (Piani), immetti **hello-world** e quindi premi Enter (Invio). Scegliere il piano hello-world-python, quindi scegliere Configure (Configura).

The screenshot shows the 'Create function' wizard. The title is 'Create function' with an 'Info' link. Below it says 'Choose one of the following options to create your function.' There are three radio button options: 'Author from scratch' (with a note 'Start with a simple Hello World example.' and an icon of a computer monitor with a gear), 'Use a blueprint' (selected, with a note 'Build a Lambda application from sample code and configuration presets for common use cases.' and an icon of two checkmarks), and 'Browse serverless app repository' (with a note 'Deploy a sample Lambda application from the AWS Serverless Application Repository.' and an icon of a cloud and a database). Below this is a section titled 'Blueprints' with an 'Info' link. It has a search bar with 'Add filter' and a keyword input field containing 'Keyword : hello-world'. Below the search bar are several blueprint cards: 'greengrass-hello-world' (note: Deploy this lambda to a Greengrass core where it will send a hello world message to a topic, tags: python · greengrass · iot · hello world), 'hello-world' (note: A starter AWS Lambda function, tags: nodejs), 'hello-world-python' (selected, note: A starter AWS Lambda function, tags: python2.7), 'hello-world-python3' (note: A starter AWS Lambda function, tags: python3.6), and 'greengrass-hello-world-nodejs' (note: Deploy this lambda to a Greengrass core where it will send a hello world message to a topic, tags: nodejs6.10 · greengrass · iot · hello world). At the bottom right are 'Cancel' and 'Configure' buttons, with 'Configure' being highlighted in red.

3. In Basic information (Informazioni di base) immettere un nome per la funzione.

Note

Non è consigliabile utilizzare informazioni personali identificabili nei nomi e nelle descrizioni delle regole.

Basic information [Info](#)

Function name

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.

4. In Execution role (Ruolo di esecuzione) scegliere Create new role from AWS policy templates (Crea nuovo ruolo dai modelli di policy AWS). In Nome ruolo immettere un nome per il ruolo. In Policy templates (Modelli di policy) scegliere Amazon SNS publish policy (Policy di pubblicazione Amazon SNS). Fare clic all'esterno del menu a discesa per chiuderlo.

VPN Connection Monitor permissions
CloudWatch EC2

Amazon SQS poller permissions
SQS

AWS IoT Button permissions
SNS

Amazon Rekognition no data permissions
Rekognition

Amazon Rekognition read-only permissions
Rekognition

Amazon Rekognition write-only permissions
Rekognition

AWS Config Rules permissions
Config S3

AWS Batch access permissions
Batch

Amazon SNS publish policy
SNS

Basic Lambda@Edge permissions (for CloudFront trigger)
CloudWatch Logs

AWS KMS decryption permissions
KMS

5. Selezionare Create function (Crea funzione).

Basic information Info

Function name

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).
 ▾

ⓘ Role creation might take a few minutes. The new role will be scoped to the current function. To use it with other functions, you can modify it in the IAM console.

Role name
Enter a name for your new role.

Use only letters, numbers, hyphens, or underscores with no spaces.

Policy templates Info
Choose one or more policy templates.
 SNS

Lambda function code
Code is preconfigured by the chosen blueprint. You can configure it after you create the function.

Runtime
Python 2.7

```
1 from __future__ import print_function
2
3 import json
4
5 print('Loading function')
6
7
8 def lambda_handler(event, context):
9     #print("Received event: " + json.dumps(event, indent=2))
10    print("value1 = " + event['key1'])
11    print("value2 = " + event['key2'])
12    print("value3 = " + event['key3'])
13    return event['key1'] # Echo back the first key value
14    #raise Exception('Something went wrong')
15
```

* These fields are required.

6. Nella console Lambda scegliere il nome della funzione Lambda. Vengono visualizzate le informazioni sulla funzione Lambda. Scorrere fino alla sezione Function code (Codice funzione) e sostituire il codice esistente con il seguente:

```
from __future__ import print_function

import json
import boto3

print('Loading function')

def lambda_handler(event, context):

    # Parse the JSON message
    eventText = json.dumps(event)

    # Print the parsed JSON message to the console; you can view this text in the Monitoring tab in the Lambda console or in the CloudWatch Logs console
    print('Received event: ', eventText)

    # Create an SNS client
    sns = boto3.client('sns')

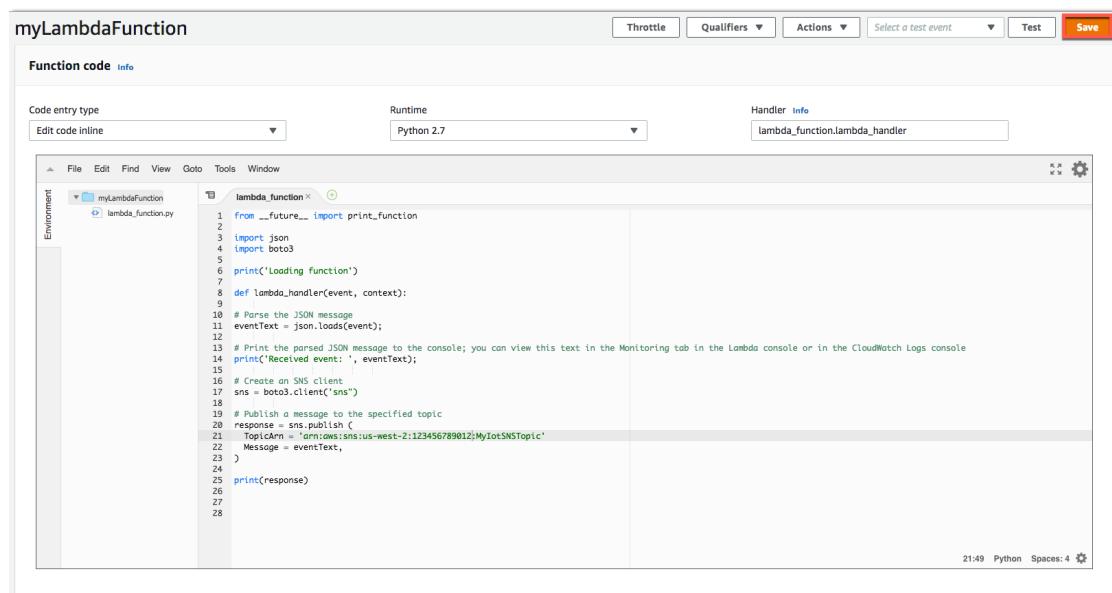
    # Publish a message to the specified topic
    response = sns.publish (
        TopicArn = 'arn:aws:iam::123456789012:role/service-role/myLambdaFunctionRole',
        Message = eventText
    )

    print(response)
```

Note

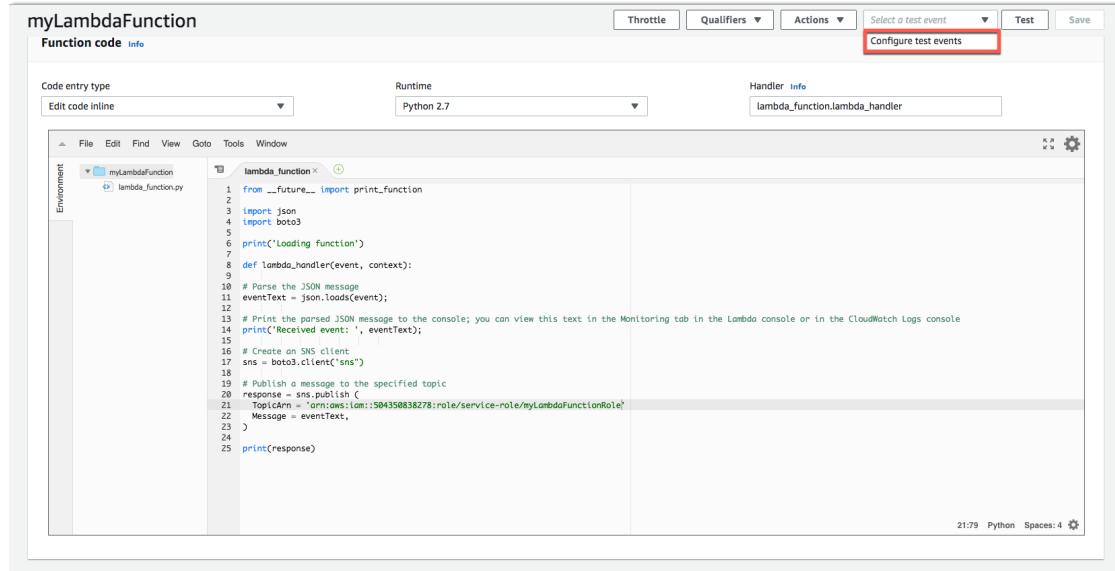
Sostituisci il valore di TopicArn con l'ARN dell'argomento Amazon SNS creato in precedenza.

Selezione Salva.



Test della funzione Lambda

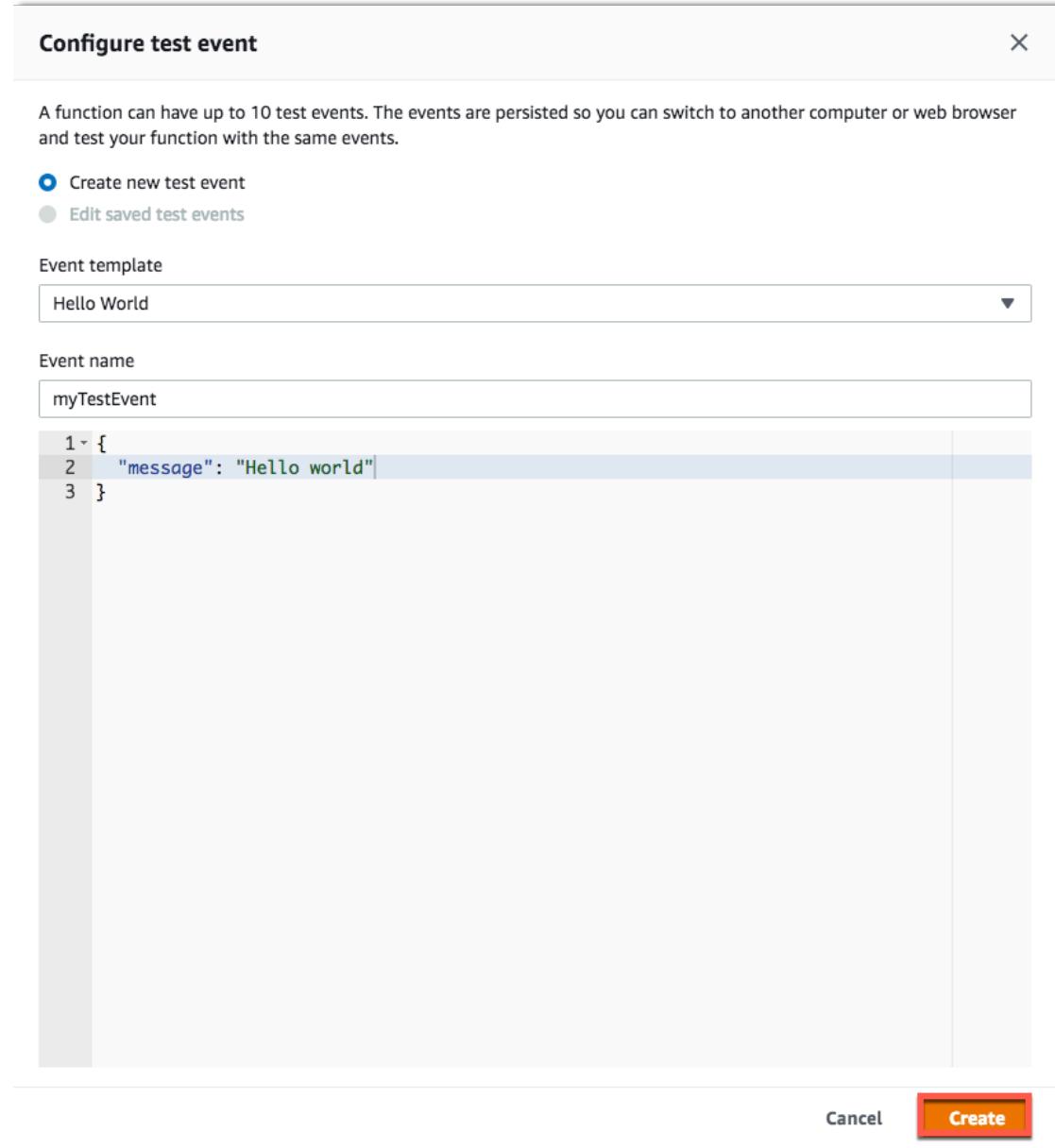
1. In alto a destra nella pagina dei dettagli della funzione Lambda, da Select a test event (Seleziona un evento di test), scegliere Configure test events (Configurazione di eventi di test).



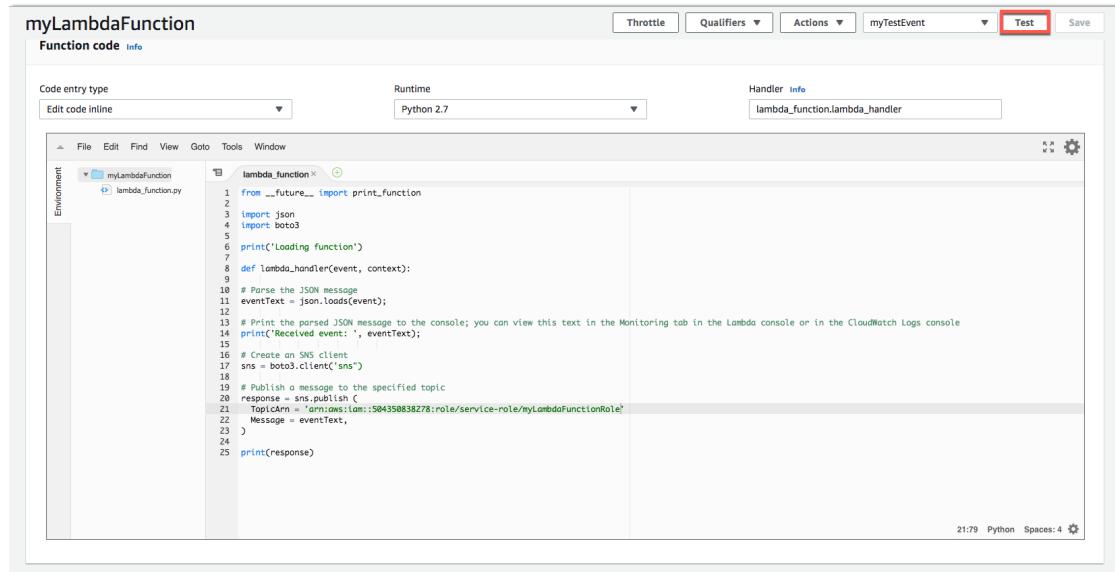
2. In Configure test events (Configurazione di eventi di test) immettere un nome per l'evento di test e sostituire il messaggio JSON con il seguente:

```
{
    "message" : "Hello, world"
}
```

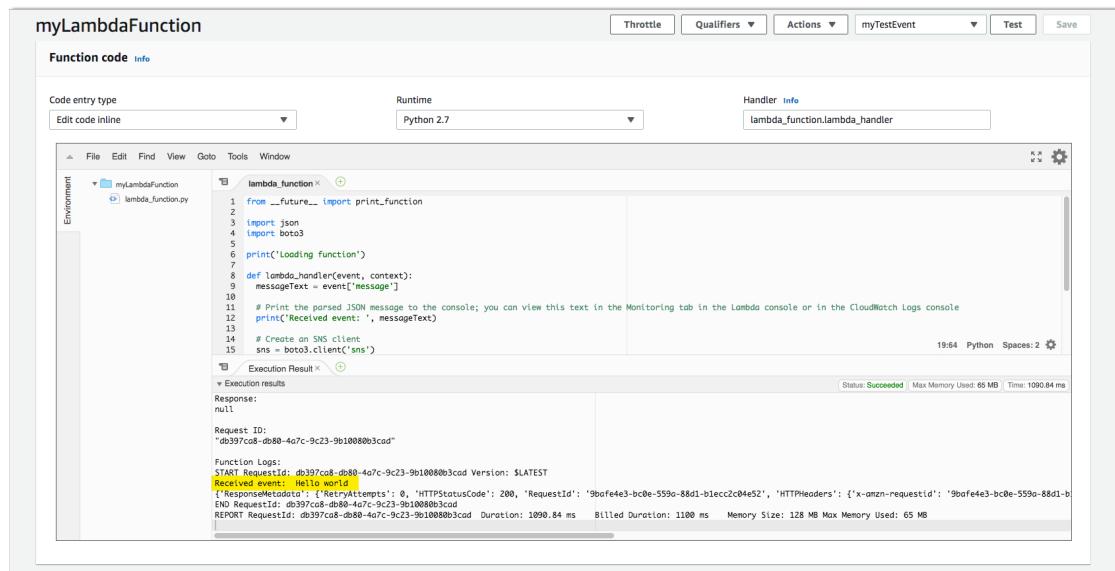
Scegliere Crea.



3. In alto a destra nella pagina dei dettagli della funzione Lambda scegliere Test per testare la funzione Lambda con il messaggio specificato nell'evento di test.



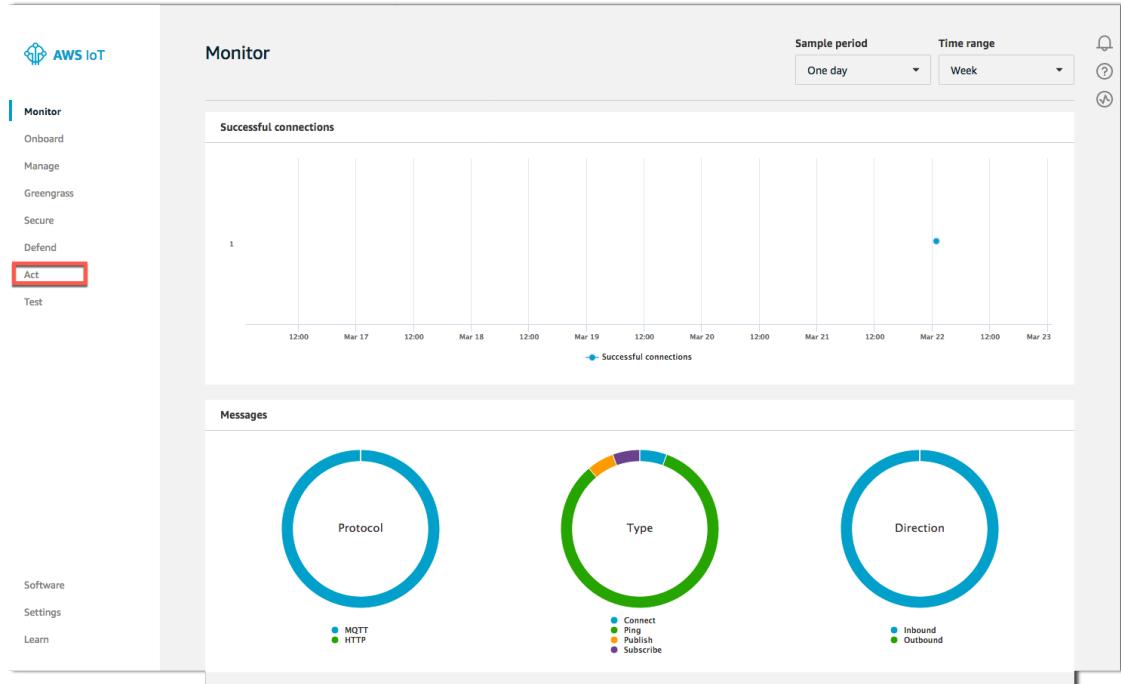
- Con il codice di funzione Lambda, nella scheda Execution result (Risultato esecuzione), è possibile vedere l'output della funzione Lambda.



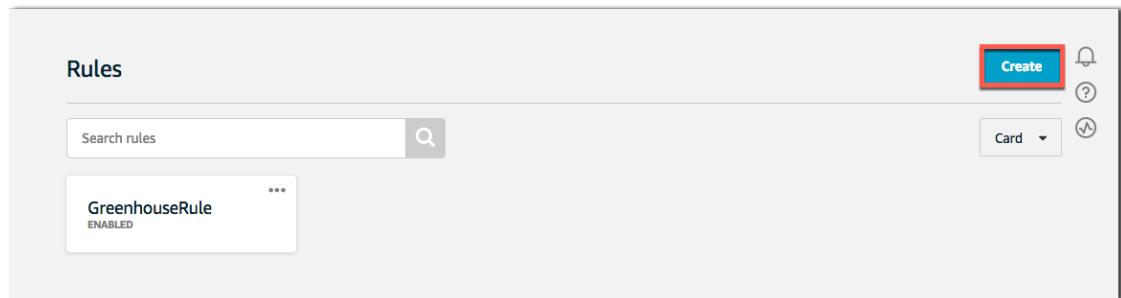
Creare una regola Lambda

Questa sezione fornisce i passaggi per la creazione di una regola con un'operazione Lambda e un'operazione di errore. L'operazione Lambda chiama la funzione Lambda. Se si verifica un errore quando si chiama la funzione Lambda, l'operazione di errore pubblica un messaggio nell'argomento MQTT `lambda/error`. Questa caratteristica risulta utile quando si esegue il test della regola.

- Andare alla console AWS IoT e, dal riquadro di navigazione, scegliere Esecuzione azioni.



2. Scegliere Crea per creare una regola AWS IoT.



3. Nella pagina Crea una regola immettere un nome per la regola.

The screenshot shows the "Create a rule" wizard. Step 1: Configure basic settings. It includes fields for Name (containing "myLambdaRule") and Description (empty). The instructions below the form state: "Create a rule to evaluate messages sent by your things and specify what to do when a message is received (for example, write data to a DynamoDB table or invoke a Lambda function)."

4. In Istruzione query regola immettere la query seguente:

```
SELECT * FROM "my/lambda/topic"
```

Rule query statement

Indicate the source of the messages you want to process with this rule.

Using SQL version

2016-03-23 ▾

Rule query statement

SELECT <Attribute> FROM <Topic Filter> WHERE <Condition>. For example: SELECT temperature FROM 'iot/topic' WHERE temperature > 50. To learn more, see [AWS IoT SQL Reference](#).

```
1 SELECT * FROM "my/lambda/topic"
```

5. In Set one or more actions (Imposta una o più operazioni) scegli Add action (Aggiungi operazione).

Set one or more actions

Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. (*.required)

Add action

6. In Seleziona un'operazione scegliere Send a message to a Lambda function (Invia un messaggio a una funzione Lambda), quindi scegliere Configura operazione.

Select an action

Select an action.

-  Insert a message into a DynamoDB table
DYNAMODB
-  Split message into multiple columns of a DynamoDB table (DynamoDBv2)
DYNAMODBV2
-  Send a message to a Lambda function
LAMBDA
-  Send a message as an SNS push notification
SNS
-  Send a message to an SQS queue
SQS
-  Send a message to an Amazon Kinesis Stream
AMAZON KINESIS
-  Republish a message to an AWS IoT topic
AWS IOT REPUBLISH
-  Store a message in an Amazon S3 bucket
S3
-  Send a message to an Amazon Kinesis Firehose stream
AMAZON KINESIS FIREHOSE
-  Send message data to CloudWatch
CLOUDWATCH METRICS
-  Change the state of a CloudWatch alarm
CLOUDWATCH ALARMS
-  Send a message to the Amazon Elasticsearch Service
AMAZON ELASTICSEARCH
-  Send a message to a Salesforce IoT Input Stream
SALESFORCE IOT
-  Send a message to an IoT Analytics Channel
IOT ANALYTICS
-  Start a Step Functions state machine execution
STEP FUNCTIONS

[Cancel](#) Configure action

7. In Configura operazione scegliere Seleziona.

Configure action

 Send a message to a Lambda function
LAMBDA

We'll set [the permissions](#) on the Lambda function for you. [Create a new Lambda function](#)

*Function name

No lambda function selected Select

[Cancel](#) Add action

8. Scegliere la funzione Lambda.

Configure action

 Send a message to a Lambda function
LAMBDA

We'll set [the permissions](#) on the Lambda function for you. [Create a new Lambda function](#)

*Function name

| | | |
|--|--|-----------------------|
| No lambda function selected | Refresh | Close |
| <input type="text" value="Search for lambda functions"/> | | |
| myLambdaFunction | Select | |
| Cancel Add action | | |

9. Scegliere Aggiungi operazione.

Configure action

 Send a message to a Lambda function
LAMBDA

We'll set [the permissions](#) on the Lambda function for you. [Create a new Lambda function](#)

*Function name [Clear](#) [Select](#)

[Cancel](#) Add action

10. Nella pagina Crea una regola, in Operazione in caso di errore, scegliere Aggiungi operazione.

Error action

Optionally set an action that will be executed when something goes wrong with processing your rule.

Add action

11. Nella pagina Imposta un'operazione come operazione di errore scegliere Republish a message to an AWS IoT topic (Ripubblica un messaggio in un argomento AWS IoT), quindi scegliere Configura operazione.

Set an action as error action

Set an action as error action.

-  Insert a message into a DynamoDB table
DYNAMODB
-  Split message into multiple columns of a DynamoDB table (DynamoDBv2)
DYNAMODBV2
-  Send a message to a Lambda function
LAMBDA
-  Send a message as an SNS push notification
SNS
-  Send a message to an SQS queue
SQS
-  Send a message to an Amazon Kinesis Stream
AMAZON KINESIS
-  Republish a message to an AWS IoT topic
AWS IOT REPUBLISH
-  Store a message in an Amazon S3 bucket
S3
-  Send a message to an Amazon Kinesis Firehose stream
AMAZON KINESIS FIREHOSE
-  Send message data to CloudWatch
CLOUDWATCH METRICS
-  Change the state of a CloudWatch alarm
CLOUDWATCH ALARMS
-  Send a message to the Amazon Elasticsearch Service
AMAZON ELASTICSEARCH
-  Send a message to a Salesforce IoT Input Stream
SALESFORCE IOT
-  Send a message to an IoT Analytics Channel
IOT ANALYTICS
-  Start a Step Functions state machine execution
STEP FUNCTIONS

[Cancel](#) Configure action

12. Nella pagina Configura operazione, in Argomento, immettere `lambda/error`.

Configure action

 Republish a message to an AWS IoT topic
AWS IOT REPUBLISH

This action will republish the message to another AWS IoT topic.

*Topic [?](#)

Choose or create a role to grant AWS IoT access to perform this action.

No role selected [Create Role](#) [Select](#)

[Cancel](#) [Add action](#)

13. In Choose or create a role to grant AWS IoT access to perform this action (Scegli o crea un ruolo per concedere ad AWS IoT l'accesso per eseguire questa operazione) scegliere Crea ruolo.

Configure action

 Republish a message to an AWS IoT topic
AWS IOT REPUBLISH

This action will republish the message to another AWS IoT topic.

*Topic [?](#)

Choose or create a role to grant AWS IoT access to perform this action.

No role selected [Create Role](#) [Select](#)

[Cancel](#) [Add action](#)

14. In Crea un nuovo ruolo immettere un nome per il ruolo e scegliere Crea ruolo.

Create a new role

A new IAM role will be created in your account. An inline policy will be attached to the role providing scoped-down permissions allowing AWS IoT to access resources on your behalf.

Name

15. In Configura operazione scegliere Aggiungi operazione.

Configure action

 Republish a message to an AWS IoT topic
AWS IOT REPUBLISH

This action will republish the message to another AWS IoT topic.

*Topic [?](#)

Choose or create a role to grant AWS IoT access to perform this action.

| | | | |
|-------------------------|-------------------|--|---------------------------------------|
| myLambdaErrorActionRole | Policy Attached ✓ | <input type="button" value="Create Role"/> | <input type="button" value="Select"/> |
|-------------------------|-------------------|--|---------------------------------------|

16. In Crea una regola scegliere Crea regola.

Create a rule

Create a rule to evaluate messages sent by your things and specify what to do when a message is received (for example, write data to a DynamoDB table or invoke a Lambda function).

Name

Description

Rule query statement

Indicate the source of the messages you want to process with this rule.

Using SQL version

Rule query statement

SELECT <Attribute> FROM <Topic Filter> WHERE <Condition>. For example: SELECT temperature FROM 'iot/topic' WHERE temperature > 50. To learn more, see [AWS IoT SQL Reference](#).

```
1 SELECT * FROM "my/lambda/topic"
```

Set one or more actions

Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. (*.required)



Send a message to a Lambda function
myLambdaFunction

[Remove](#) [Edit](#)

[Add action](#)

Error action

Optionally set an action that will be executed when something goes wrong with processing your rule.



Republish a message to an AWS IoT topic
lambda/error

[Remove](#) [Edit](#)

Tags

Apply tags to your resources to help organize and identify them. A tag consists of a case-sensitive key-value pair. [Learn more](#) about tagging your AWS resources.

Tag name

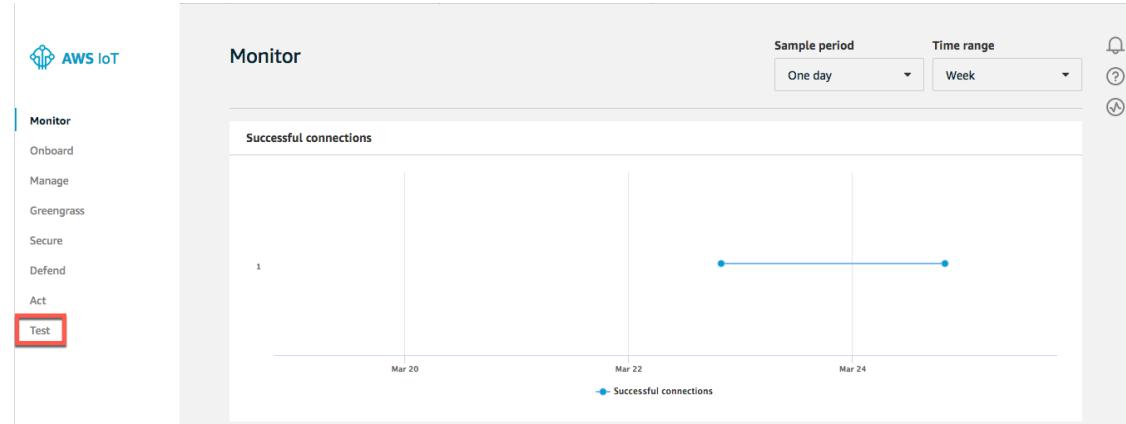
Value

[Clear](#)

[Add another](#)

Test della regola Lambda

- Per testare la regola Lambda, apri la console AWS IoT e scegli Test (Test) dal riquadro di navigazione.

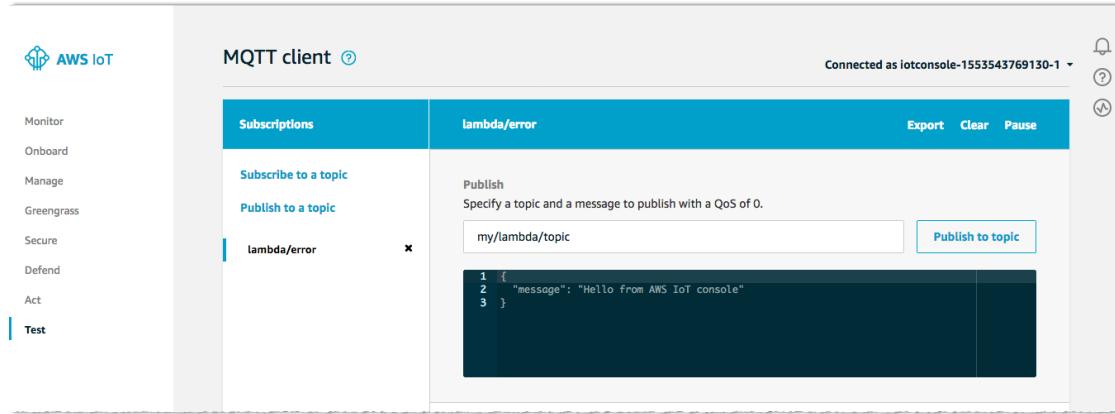


- Nel client MQTT, in Argomento sottoscrizione, immettere `lambda/error`, quindi scegliere Effettua sottoscrizione all'argomento.

The screenshot shows the AWS IoT Subscriptions interface. On the left, a sidebar lists 'Subscriptions', 'Subscribe to a topic', and 'Publish to a topic'. The 'Subscribe to a topic' section is active. It contains a 'Subscription topic' input field containing 'lambda/error', a 'Subscribe to topic' button (which is highlighted with a red box), a 'Max message capture' input field set to '100', and a 'Quality of Service' section with two radio buttons: '0 - This client will not acknowledge to the Device Gateway that messages are received' (selected) and '1 - This client will acknowledge to the Device Gateway that messages are received'. Below these are 'MQTT payload display' settings with three radio buttons: 'Auto-format JSON payloads (improves readability)' (selected), 'Display payloads as strings (more accurate)', and 'Display raw payloads (in hexadecimal)'. The right side of the interface is divided into two sections: 'Publish' (with a note to specify a topic and message to publish with QoS 0) and a code editor window containing a JSON message:

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

- In Pubblica immettere `my/lambda/topic` e quindi scegliere Pubblica nell'argomento per pubblicare il messaggio JSON di default.



La pubblicazione di questo messaggio dovrebbe attivare la regola e chiamare la funzione Lambda. La funzione Lambda esegue il push di un messaggio Amazon SNS a un numero di telefono sottoscritto all'argomento Amazon SNS. Se non si riceve un messaggio di testo, controllare nel client MQTT se sono stati pubblicati messaggi in `lambda/error`.

Risoluzione dei problemi relativi alle regole Lambda

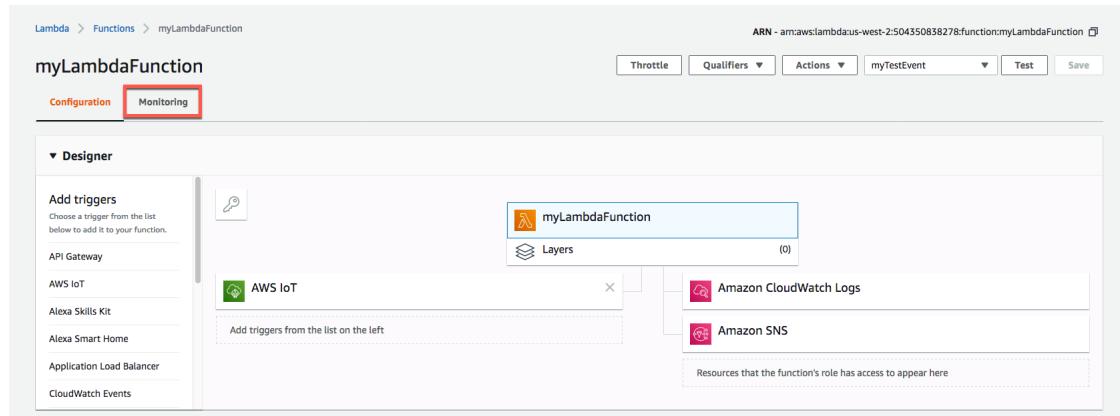
Se viene chiamata la funzione Lambda ma non si riceve un messaggio di testo, verificare che il numero di telefono sia sottoscritto all'argomento Amazon SNS. Se il numero di telefono è sottoscritto, controllare i log CloudWatch per la funzione Lambda. AWS Lambda scrive i log in CloudWatch, il che consente di visualizzare l'output dalla funzione Lambda.

Per visualizzare CloudWatch Logs

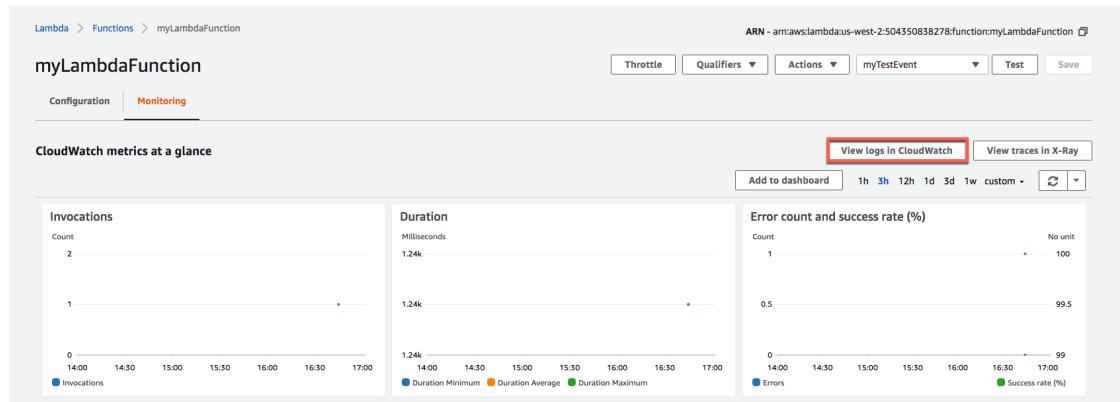
- Nella console Lambda scegliere Funzioni dal riquadro di navigazione.

- Scegliere la funzione Lambda.

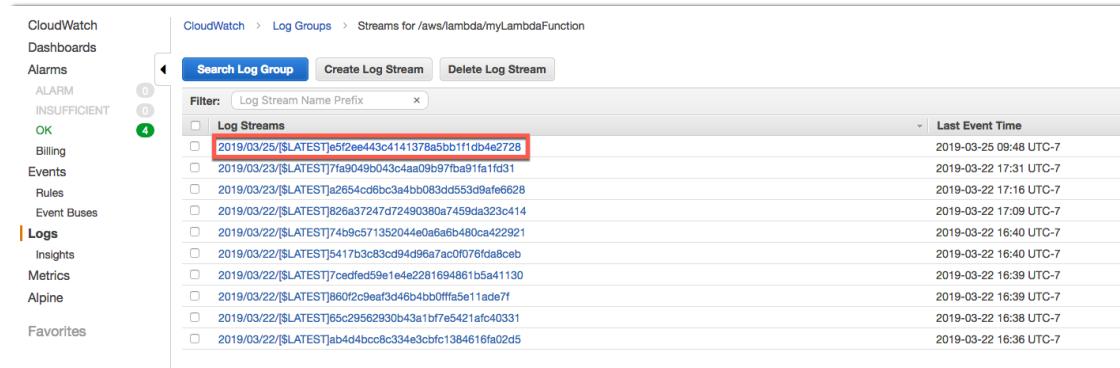
- Nella pagina dei dettagli della funzione Lambda scegliere la scheda Monitoraggio.



- Scegliere View logs in CloudWatch (Visualizza log in CloudWatch).



- Scegliere il flusso di log più recente.



- Il flusso di log mostra i log scritti dalla funzione Lambda.



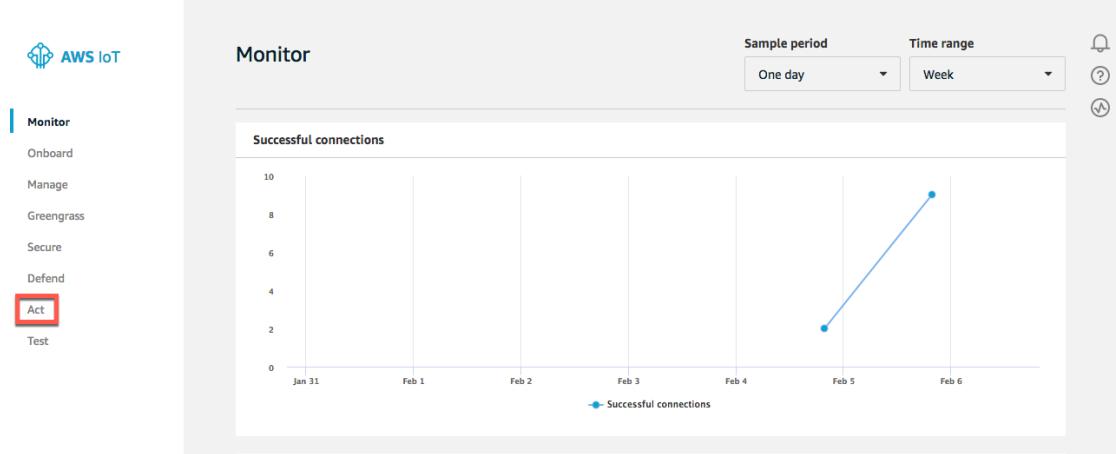
Creazione di una regola Amazon SNS

Puoi definire una regola per l'invio dei dati del messaggio a un argomento Amazon SNS.

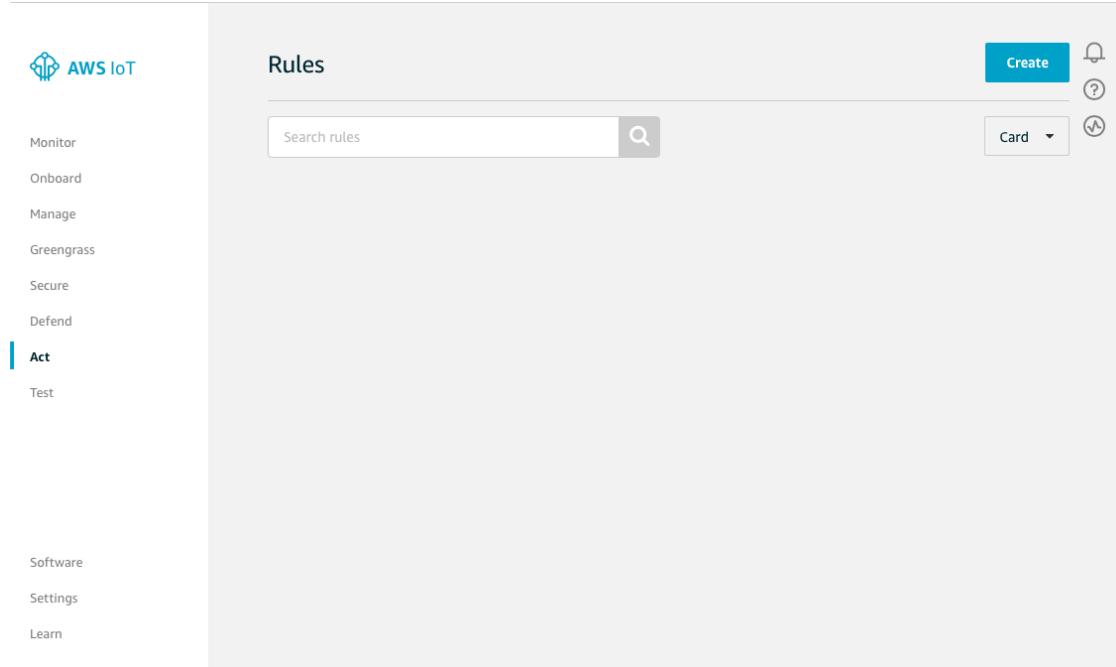
In questo tutorial potrai creare una regola per l'invio del nome dell'oggetto AWS IoT che ha attivato la regola a tutti i sottoscrittori di un argomento Amazon SNS.

Per creare una regola con un'operazione SNS

- Nella console [AWS IoT](#), nel riquadro di navigazione, scegliere Agisci.



- Nella pagina Rules (Regole) scegli Create (Crea).



- Immetti un nome e una breve descrizione della regola.

Note

Non è consigliabile utilizzare informazioni di identificazione personale nei nomi e nelle descrizioni delle regole.

Create a rule

Create a rule to evaluate messages sent by your things and specify what to do when a message is received (for example, write data to a DynamoDB table or invoke a Lambda function).

Name
MySNSRule

Description
A more complex SNS rule

- Nell'editor Rule query statement (Istruzione query regola), immetti quanto segue:

```
SELECT *, topic(3) as thing FROM '$aws/things/+shadow/update/accepted'
```

(Il filtro di argomenti successivo a "FROM" specifica gli argomenti che attivano l'operazione della regola, quando un messaggio viene pubblicato in uno di essi. Il simbolo dell'addizione (+) usato nel filtro di argomenti è un carattere jolly che corrisponde a qualsiasi nome di oggetto. L'attributo "topic(3)" successivo a "SELECT" aggiunge il nome dell'oggetto, ovvero il terzo campo dell'argomento, al contenuto del messaggio).

Rule query statement
Indicate the source of the messages you want to process with this rule.

Using SQL version
2016-03-23

Rule query statement
SELECT <Attribute> FROM <Topic Filter> WHERE <Condition>. For example: SELECT temperature FROM 'iot/topic' WHERE temperature > 50. To learn more, see [AWS IoT SQL Reference](#).

```
1 SELECT *, topic(3) as thing FROM '$aws/things/+shadow/update/accepted'
```

- In Set one or more actions (Imposta una o più operazioni) scegli Add action (Aggiungi operazione).

Set one or more actions
Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. (*.required)

Add action

- Nella pagina Select an action (Seleziona un'operazione), scegliere Send a message as an SNS push notification (Invia un messaggio come notifica push SNS), quindi scegliere Configure action (Configura operazione).

Select an action

Select an action.

-  Insert a message into a DynamoDB table
DYNAMODB
-  Split message into multiple columns of a DynamoDB table (DynamoDBv2)
DYNAMODBV2
-  Send a message to a Lambda function
LAMBDA
-  Send a message as an SNS push notification
SNS
-  Send a message to an SQS queue
SQS
-  Send a message to an Amazon Kinesis Stream
AMAZON KINESIS
-  Republish a message to an AWS IoT topic
AWS IOT REPUBLISH
-  Store a message in an Amazon S3 bucket
S3
-  Send a message to an Amazon Kinesis Firehose stream
AMAZON KINESIS FIREHOSE
-  Send message data to CloudWatch
CLOUDWATCH METRICS
-  Change the state of a CloudWatch alarm
CLOUDWATCH ALARMS
-  Send a message to the Amazon Elasticsearch Service
AMAZON ELASTICSEARCH
-  Send a message to a Salesforce IoT Input Stream
SALESFORCE IOT
-  Send a message to IoT Analytics
IOT ANALYTICS
-  Start a Step Functions state machine execution
STEP FUNCTIONS

[Cancel](#) Configure action

7. Nella pagina Configure action (Configura operazione), scegliere Create (Crea) per SNS target (Destinazione SNS).

Configure action

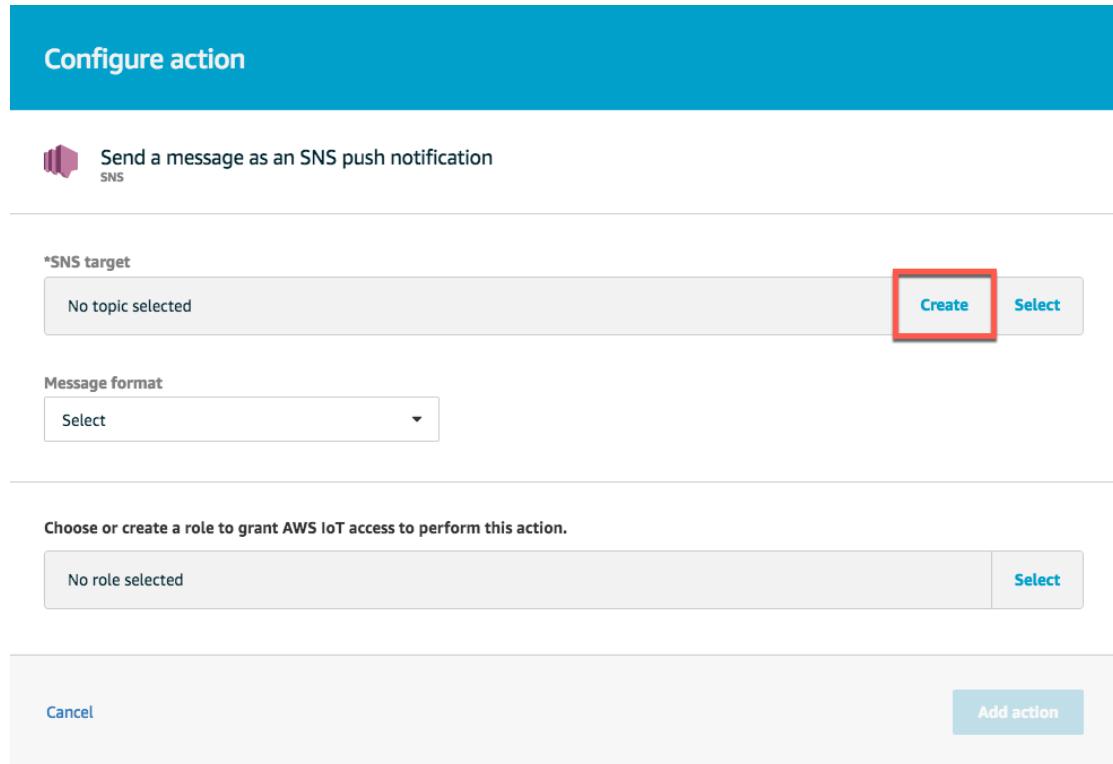
 Send a message as an SNS push notification
SNS

*SNS target
No topic selected Create Select

Message format
Select ▾

Choose or create a role to grant AWS IoT access to perform this action.
No role selected Select

Cancel Add action

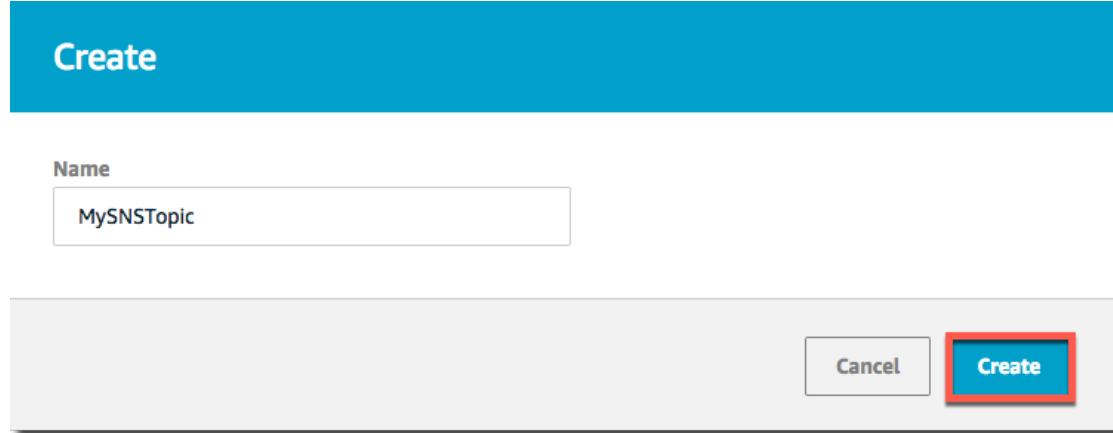


8. Immetti un nome argomento nella finestra di dialogo visualizzata e quindi scegli Create (Crea).

Create

Name
MySNSTopic

Cancel Create



9. Nella pagina Configure action (Configura operazione), scegliere l'argomento SNS appena creato per SNS target (Destinazione SNS). Per Message format (Formato messaggio), scegliere RAW. In Choose or create a role to grant AWS IoT access to perform this action (Scegli o crea un ruolo per concedere ad AWS IoT l'accesso per eseguire questa operazione), scegli Create Role (Crea ruolo).

Configure action

 Send a message as an SNS push notification
SNS

*SNS target

| | | | |
|------------|------------------------|-----------------------|------------------------|
| MySNSTopic | Create | Clear | Select |
|------------|------------------------|-----------------------|------------------------|

Message format

| |
|-----|
| RAW |
|-----|

Choose or create a role to grant AWS IoT access to perform this action.

| | | |
|------------------|-----------------------------|------------------------|
| No role selected | Create Role | Select |
|------------------|-----------------------------|------------------------|

[Cancel](#) [Add action](#)

10. Immetti un nome del ruolo, quindi scegli Create role (Crea ruolo).

Create a new role

A new IAM role will be created in your account. An inline policy will be attached to the role providing scoped-down permissions allowing AWS IoT to access resources on your behalf.

Name

| |
|-----------|
| MySNSRole |
|-----------|

[Cancel](#) [Create role](#)

11. In Configure action (Configura operazione), scegli Add action (Aggiungi operazione).

Configure action

 Send a message as an SNS push notification
SNS

*SNS target

| | | | |
|------------|------------------------|-----------------------|------------------------|
| MySNSTopic | Create | Clear | Select |
|------------|------------------------|-----------------------|------------------------|

Message format

| | |
|-----|---|
| RAW | ▼ |
|-----|---|

Choose or create a role to grant AWS IoT access to perform this action.

| | | | |
|-----------|-------------------|-----------------------------|------------------------|
| MySNSRole | Policy Attached ✓ | Create Role | Select |
|-----------|-------------------|-----------------------------|------------------------|

[Cancel](#) Add action

12. Scegli Create rule (Crea regola).

Create a rule

Create a rule to evaluate messages sent by your things and specify what to do when a message is received (for example, write data to a DynamoDB table or invoke a Lambda function).

Name
mySNSRule

Description

Rule query statement
Indicate the source of the messages you want to process with this rule.

Using SQL version
2016-03-23

Rule query statement
SELECT <Attribute> FROM <Topic Filter> WHERE <Condition>. For example: SELECT temperature FROM 'iot/topic' WHERE temperature > 50. To learn more, see [AWS IoT SQL Reference](#).

```
1 SELECT *, topic(3) as thing FROM '$aws/things/+shadow/update/accepted'
```

Set one or more actions
Select one or more actions to happen when the above rule is matched by an inbound message. Actions define additional activities that occur when messages arrive, like storing them in a database, invoking cloud functions, or sending notifications. (*.required)

 Send a message as an SNS push notification
MyIoTTopic Remove Edit >

Add action

Error action
Optionally set an action that will be executed when something goes wrong with processing your rule.

Add action

Tags
Apply tags to your resources to help organize and identify them. A tag consists of a case-sensitive key-value pair. [Learn more](#) about tagging your AWS resources.

Tag name
Provide a tag name, e.g. Manufacturer

Value
Provide a tag value, e.g. Acme-Corporation

Clear

Add another

87

Cancel **Create rule**

Per testare la regola, aggiungi una sottoscrizione all'argomento SNS creato e aggiorna la copia shadow di ogni oggetto AWS IoT.

Puoi usare la console AWS IoT per trovare un oggetto, aprirne la pagina dei dettagli e modificare la copia shadow del dispositivo. Quando il servizio Device Shadow riceve la notifica della modifica, pubblica un messaggio in `$aws/things/MySNSThing/shadow/update/accepted`. La regola viene attivata e tutti i sottoscrittori dell'argomento SNS ricevono un messaggio contenente il nome dell'oggetto.

AWS IoTTutorial SDK

Gli SDK (Software Development Kit) di dispositivo AWS IoT ti aiutano a connettere i dispositivi a AWS IoT rapidamente e in tutta semplicità. Gli SDK di dispositivo AWS IoT includono librerie open source, guide per sviluppatori con esempi e guide alla portabilità, con cui puoi creare soluzioni o prodotti IoT innovativi sulle piattaforme hardware che preferisci.

Important

Prima di leggere questo tutorial, leggere [Nozioni di base su AWS IoT \(p. 5\)](#).

Questi tutorial forniscono istruzioni dettagliate per connettere il tuo Raspberry Pi a [Broker di messaggi per AWS IoT \(p. 239\)](#) utilizzando SDK di dispositivo AWS IoT per Embedded C e SDK di dispositivo AWS IoT per JavaScript. Dopo avere seguito le istruzioni, potrai connetterti alla piattaforma AWS IoT ed eseguire le applicazioni di esempio incluse con il kit SDK Device per AWS IoT.

Indice

- [Prerequisiti \(p. 89\)](#)
- [Creazione di un oggetto AWS IoT per Raspberry Pi \(p. 89\)](#)
- [Uso dell'SDK AWS IoT per Embedded C \(p. 104\)](#)
- [Uso dell'SDK di dispositivo AWS IoT per JavaScript \(p. 107\)](#)

Prerequisiti

Questo tutorial richiede quanto segue:

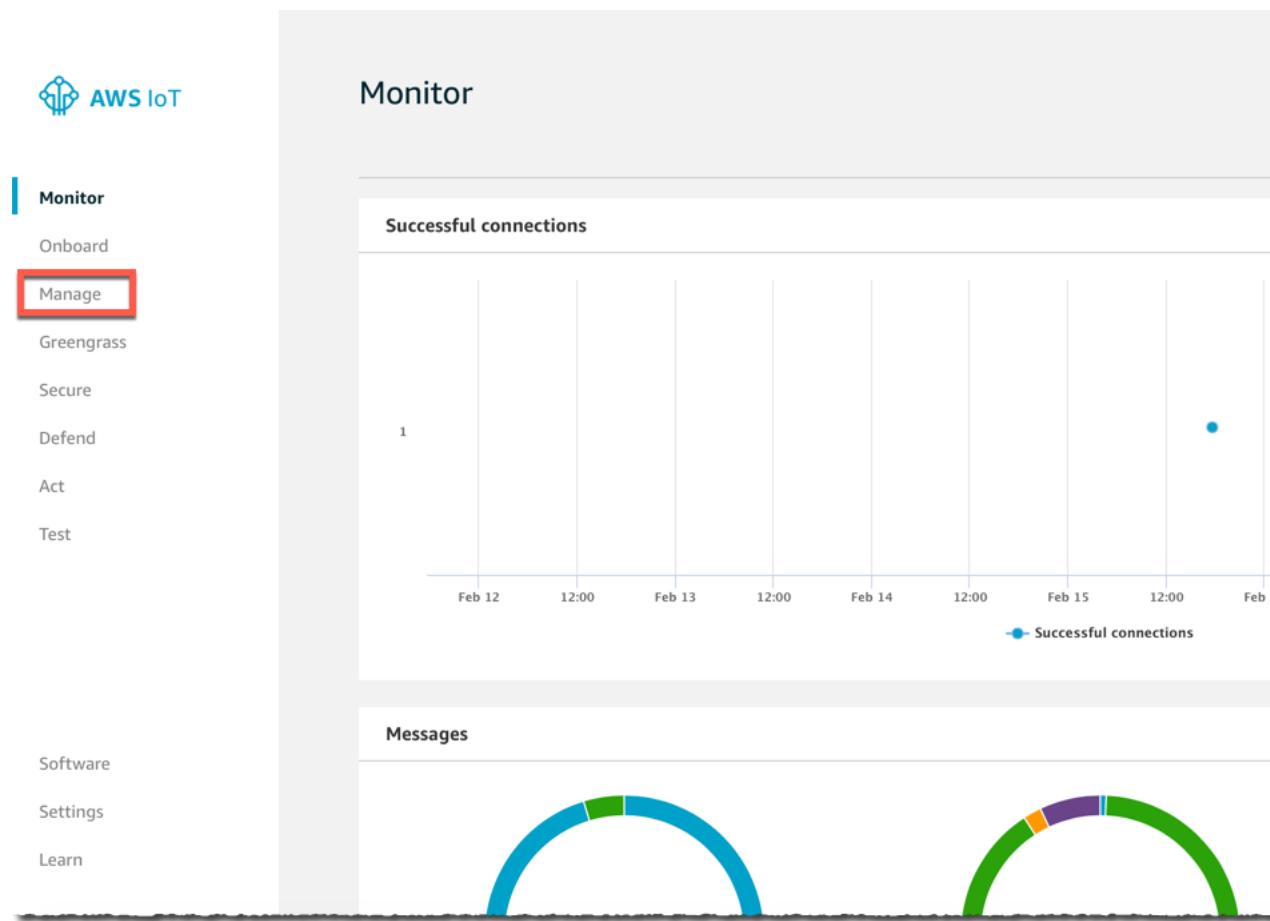
- [Raspberry Pi 2 modello B](#) o successivo.
- Sistema operativo [Raspbian Wheezy](#) o successivo.
- Browser Web [Chromium](#) o [Iceweasel](#).
- Raspberry Pi deve essere connesso a Internet utilizzando una connessione Wi-Fi o ethernet.
- Un account AWS. Se non disponi già di un account AWS, puoi ottenerne uno gratuitamente accedendo al [Centro risorse per le nozioni di base su Amazon AWS](#).

Creazione di un oggetto AWS IoT per Raspberry Pi

Un oggetto rappresenta un dispositivo il cui stato o i cui dati sono archiviati nel cloud AWS. Lo stato o i dati del dispositivo sono archiviati in un documento JSON noto come shadow del dispositivo. La copia shadow viene utilizzata per archiviare e recuperare informazioni sullo stato. Il [servizio Device Shadow](#) conserva una copia shadow per ogni dispositivo connesso a AWS IoT.

Creare un oggetto AWS IoT

1. Sul Raspberry Pi, aprire un browser Web e accedere alla [console AWS IoT](#). Potrebbe essere richiesto di effettuare l'accesso.
2. Nella [console AWS IoT](#), viene visualizzata la pagina Monitor (Monitora). Nel riquadro di navigazione, selezionare Manage (Gestisci).



3. Scegliere Create (Crea).

The screenshot shows the AWS IoT Things management interface. On the left, a sidebar menu lists various categories: Monitor, Onboard, Manage (with 'Things' selected), Types, Thing Groups, Billing Groups, Jobs, Greengrass, Secure, Defend, Act, Test, Software, Settings, and Learn. The main area is titled 'Things' and contains a search bar with the placeholder 'Search things' and a magnifying glass icon. Below the search bar is a button labeled 'Configure fleet indexing' with a help icon. A card displays the details for a single thing named 'MyTestThing', which is listed as 'NO TYPE'. There is also a three-dot ellipsis icon next to the thing name.

4. Nella pagina Creating AWS IoT things (Creazione di oggetti AWS IoT), scegli Create a single thing (Crea singolo oggetto).

Creating AWS IoT things

An IoT thing is a representation and record of your physical device in the cloud. Any physical device needs a thing record in order to work with AWS IoT. [Learn more.](#)

Register a single AWS IoT thing

Create a thing in your registry

Create a single thing

Bulk register many AWS IoT things

Create things in your registry for a large number of devices already using AWS IoT, or register devices so they are ready to connect to AWS IoT.

Create many things

[Cancel](#)

Create a single thing

5. Nella pagina Add your device to the device registry (Aggiungi il tuo dispositivo al registro dei dispositivi), immettere **MyRaspberryPi** come Name (Nome) del dispositivo. Lasciare i valori predefiniti di tutti gli altri campi, quindi scegliere Next (Avanti).

CREATE A THING

Add your device to the thing registry

This step creates an entry in the thing registry and a thing shadow for your device.

Name

Apply a type to this thing

Using a thing type simplifies device management by providing consistent registry data for things that share a type. Types provide things with a common set of attributes, which describe the identity and capabilities of your device, and a description.

Thing Type

No type selected

Create a type

Add this thing to a group

Adding your thing to a group allows you to manage devices remotely using jobs.

Thing Group

Groups /

Create group Change

Set searchable thing attributes (optional)

Enter a value for one or more of these attributes so that you can search for your things in the registry.

Attribute key

Value

Clear

Add another

Show thing shadow ▾

Cancel

Back

Next

- Nella pagina Add a certificate for your thing (Aggiungi un certificato per l'oggetto), scegliere Create certificate (Crea certificato). Questa operazione genera un certificato e una coppia di chiavi X.509.

CREATE A THING

Add a certificate for your thing

A certificate is used to authenticate your device's connection to AWS IoT.

One-click certificate creation (recommended)

This will generate a certificate, public key, and private key using AWS IoT's certificate authority.

[Create certificate](#)

Create with CSR

Upload your own certificate signing request (CSR) based on a private key you own.

[Create with CSR](#)

Use my certificate

Register your CA certificate and use your own certificates for one or many devices.

[Get started](#)

Skip certificate and create thing

You will need to add a certificate to your thing later before your device can connect to AWS IoT.

[Create thing without certificate](#)

7. Nella pagina Certificate created! (Certificato creato), scaricare le chiavi pubbliche e private, il certificato e l'autorità di certificazione (CA) della root. Salvarli sul Raspberry Pi. In seguito, verranno copiati in una directory diversa in seguito in questo tutorial. Scegliere Activate (Programma Activate) per attivare il certificato X.509, quindi scegliere Attach a policy (Collega una policy).

Certificate created!

Download these files and save them in a safe place. Certificates can be retrieved at any time, but the private and public keys cannot be retrieved after you close this page.

In order to connect a device, you need to download the following:

| | | |
|------------------------------|------------------------|--------------------------|
| A certificate for this thing | 0488f55a11.cert.pem | Download |
| A public key | 0488f55a11.public.key | Download |
| A private key | 0488f55a11.private.key | Download |

You also need to download a root CA for AWS IoT:

A root CA for AWS IoT [Download](#)

[Activate](#)

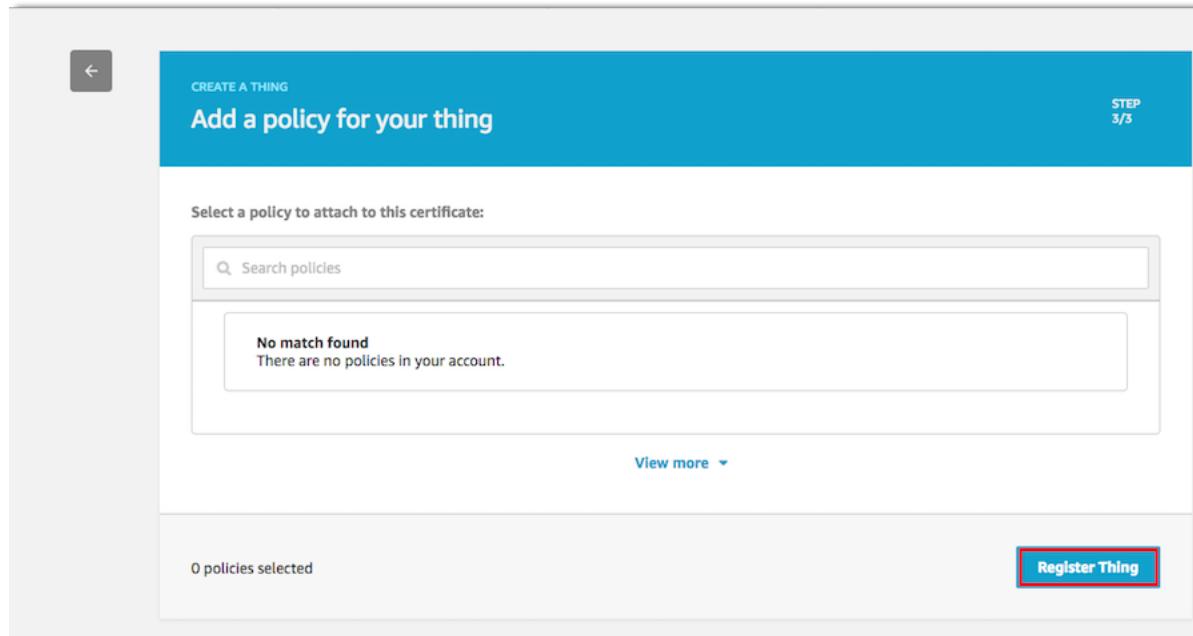
[Cancel](#)

[Done](#)

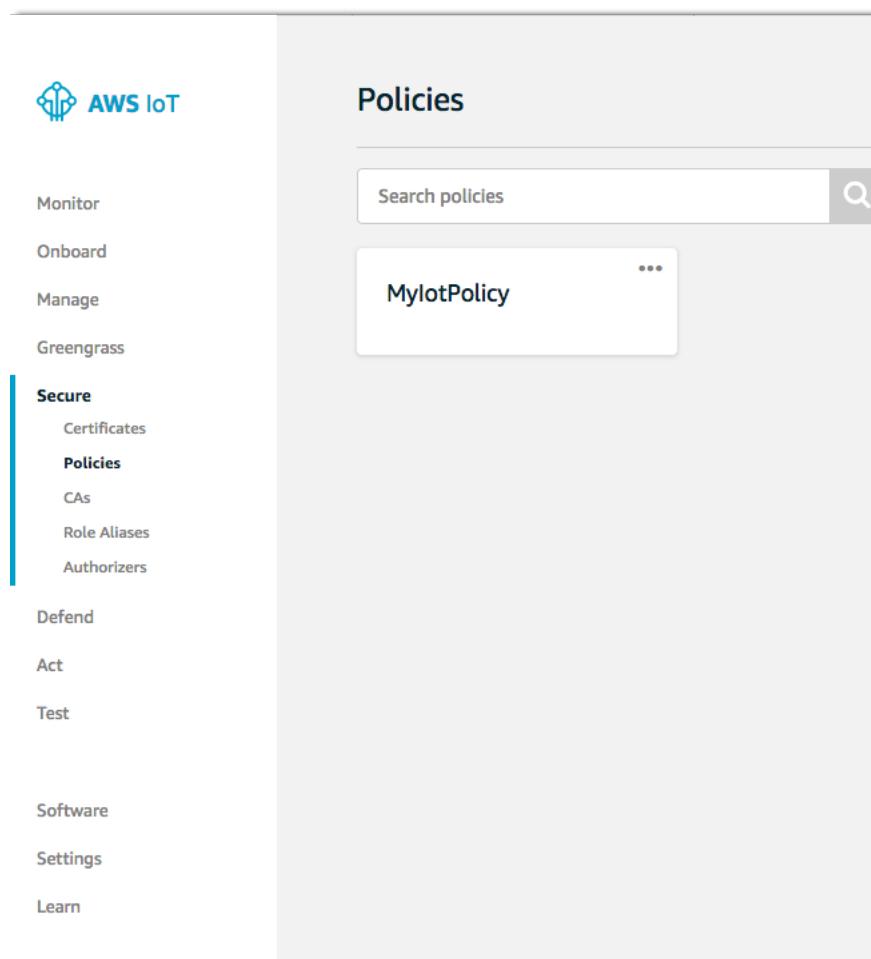
[Attach a policy](#)

8. Nella pagina Add a policy for your thing (Aggiungi una policy per l'oggetto), scegliere Register Thing (Registra l'oggetto).

Dopo avere registrato l'oggetto, è necessario creare e collegare una nuova policy al certificato.



9. Nella console AWS IoT del riquadro di navigazione, scegliere Secure (Sicurezza) e Policies (Policy). Nella pagina Policies (Policy), scegliere Create a policy (Crea una policy).



10. Nella pagina Create a policy (Crea una policy):

- Immettere un Name (Nome) per la policy. Per Action (Operazione),
- immettere **iot:***. In Resource ARN (ARN risorsa), immettere *****.
- In Effect (Effetto), scegliere Allow (Consenti), quindi scegliere Create (Crea).

Questa policy consente al componente Raspberry Pi di pubblicare messaggi in AWS IoT.

Important

Queste impostazioni sono eccessivamente permissive. In un ambiente di produzione restringere l'ambito delle autorizzazioni a quelle che sono richieste dal dispositivo. Per ulteriori informazioni, consulta [Autorizzazione \(p. 196\)](#).

The screenshot shows the 'Create a policy' page in the AWS IoT console. At the top, there is a blue header bar with the title 'Create a policy'. Below the header, a descriptive text explains what a policy is and provides a link to the 'AWS IoT Policies documentation page'. A 'Name' input field contains the value 'MyRaspberryPiPolicy'. The main section is titled 'Add statements' and includes a sub-instruction: 'Policy statements define the types of actions that can be performed by a resource.' To the right of this instruction is a link labeled 'Advanced mode'. The 'Add statements' section contains three fields: 'Action' (with the value 'iot:*'), 'Resource ARN' (with the value '*'), and 'Effect' (with the 'Allow' checkbox checked). There is also a 'Remove' button next to the effect section. Below these fields is a 'Create statement' button. At the bottom of the page is a large 'Create' button.

11. Nella console AWS IoT, scegliere Manage (Gestisci) e Things (Oggetti). Nella pagina Things (Oggetti), scegliere MyRaspberryPi.

The screenshot shows the AWS IoT Things interface. On the left, a sidebar menu lists various sections: Monitor, Onboard, Manage (with sub-options Things, Types, Thing Groups, Billing Groups, Jobs), Greengrass, Secure, Defend, Act, Test, Software, Settings, and Learn. The 'Manage Things' option is currently selected. The main content area is titled 'Things' and contains a search bar labeled 'Search things'. A single card is listed under the heading 'MyRaspberryPi' with the sub-label 'NO TYPE'. A red box highlights this card. In the top right corner of the main area, there is a 'Create' button and a 'Card' dropdown menu.

12. Nella pagina Details (Dettagli) dell'oggetto, nel riquadro di navigazione di sinistra, scegliere Interact (Interazione).

The screenshot shows the AWS IoT Thing details page for a thing named "MyRaspberryPi". The top navigation bar includes "THING", "MyRaspberryPi", "NO TYPE", and "Actions". On the left, a sidebar lists navigation options: Details (selected), Security, Thing Groups, Billing Groups, Shadow, Interact (highlighted with a red box), Activity, Jobs, Violations, and Defender metrics (with a "new" badge). The main content area shows the "Thing ARN" field with the value "arn:aws:iot:us-west-2:...:thing/MyRaspberryPi". Below it is the "Type" field, which is currently set to "No type".

13. Annota l'endpoint API REST. Queste informazioni saranno necessarie per connettersi a AWS IoT. Nel riquadro di navigazione, fare clic su Security (Sicurezza).

THING

MyRaspberryPi

NO TYPE

Actions

Details

Security

Thing Groups

Billing Groups

Shadow

Interact

Activity

Jobs

Violations

Defender metrics (new)

This thing already appears to be connected.

Connect a device

HTTPS

Update your Thing Shadow using this Rest API Endpoint. [Learn more](#)

`[REDACTED]-ats.iot.us-west-2.amazonaws.com`

MQTT

Use topics to enable applications and things to get, update, or delete the state information for a Thing (Thing Shadow)

[Learn more](#)

Update to this thing shadow

`$aws/things/MyRaspberryPi/shadow/update`

Update to this thing shadow was accepted

`$aws/things/MyRaspberryPi/shadow/update/accepted`

Update this thing shadow documents

`$aws/things/MyRaspberryPi/shadow/update/documents`

14. Scegliere il certificato creato in precedenza.

THING

MyRaspberryPi

NO TYPE

Actions

Details

Security

Thing Groups

Billing Groups

Shadow

Interact

Activity

Jobs

Violations

Defender metrics

Create certificate

View other options

511058e40bda25f70...

15. Nella pagina Details (Dettagli) del certificato, in Actions (Operazioni), scegliere Attach policy (Allega policy).

The screenshot shows the AWS IoT Certificate Details page. At the top, it displays the certificate's ARN: **511058e40bda25f705c2f16e29479bb59c1f7264ad8e4d89396004ef6899af24**. Below this, the status is listed as **ACTIVE**. On the right, a vertical **Actions** menu is open, showing options like **Activate**, **Deactivate**, **Revoke**, **Accept transfer**, **Reject transfer**, **Revoke transfer**, **Start transfer**, **Attach policy** (which is highlighted with a red box), **Attach thing**, **Download**, and **Delete**.

Certificate ARN
arn:aws:iot:us-west-2: [REDACTED]:cert/511058e40bda25f705c2f16e29479bb59c1f7264ad8e4d89396004ef6899af24

Details

Issuer
OU=Amazon Web Services O\=Amazon.com Inc. L\=Seattle ST\=Washington C\=US

Subject
CN=AWS IoT Certificate

Create date
Feb 22, 2019 3:01:24 PM -0800

Effective date
Feb 22, 2019 2:59:24 PM -0800

Expiration date
Dec 31, 2049 3:59:59 PM -0800

16. Nella pagina Attach policies to certificate(s) (Collega policy ai certificati), scegliere la policy creata, quindi Attach (Collega).

The dialog box is titled "Attach policies to certificate(s)". It contains the message: "Policies will be attached to the following certificate(s): **511058e40bda25f705c2f16e29479bb59c1f7264ad8e4d89396004ef6899af24**". Below this, there is a section titled "Choose one or more policies" with a search bar labeled "Search policies". A policy named "MylotPolicy" is selected, indicated by a checked checkbox. To the right of the checkbox is a "View" link. At the bottom of the dialog, there is a message "1 policy selected" next to a "Cancel" button and a prominent blue "Attach" button.

Uso dell'SDK AWS IoT per Embedded C

Configurazione dell'ambiente di runtime per l'SDK AWS IoT per Embedded C

Scarica l'SDK AWS IoT per Embedded C nel Raspberry Pi da [GitHub](#):

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

Verrà creata una directory denominata `aws-iot-device-sdk-embedded-C` nella directory corrente. Il percorso predefinito è la directory home dell'utente (`/home/pi`).

Scarica mbed TLS nel Raspberry Pi da [GitHub](#):

Note

Questo collegamento visualizza il ramo `development` potenzialmente instabile per impostazione predefinita. Non è consigliabile utilizzare il ramo `development`. Per ulteriori informazioni sui rami ufficialmente rilasciati, vedi [arm MBED](#).

Copia i contenuti della directory mbed TLS nella directory `aws-iot-device-sdk-embedded-C/external_libs/mbedtls`.

Configurazione delle app di esempio

L'SDK AWS IoT per Embedded C include applicazioni di esempio che puoi provare a usare. Per semplicità, eseguiremo l'applicazione `subscribe_publish_sample`, che consente di illustrare come connettersi al Broker di messaggi AWS IoT ed effettuare la sottoscrizione e la pubblicazione negli argomenti MQTT.

1. Segui le istruzioni in [Nozioni di base su AWS IoT \(p. 5\)](#) per creare un oggetto IoT, un certificato, una chiave privata e una policy IoT.
2. Copia il certificato, la chiave privata e il certificato CA root nella directory `aws-iot-device-sdk-embedded-C/certs`.

Note

I certificati CA root e dei dispositivi sono soggetti a scadenza o revoca. In questi casi, dovrai copiare nel dispositivo un nuovo certificato CA oppure una nuova chiave privata e un nuovo certificato del dispositivo.

3. Passa alla directory `aws-iot-device-sdk-embedded-C/samples/linux/subscribe_publish_sample`. Devi configurare l'endpoint AWS IoT personale, la chiave privata e il certificato. L'endpoint personale è l'endpoint API REST annotato prima. Se non ricordi l'endpoint e hai accesso a un computer in cui è installata l'AWS CLI, puoi usare il comando `aws iot describe-endpoint` per trovare l'URL dell'endpoint personale. In alternativa, passa alla console AWS IoT:
 - a. Scegli Register (Registra).
 - b. Scegliere Things (Oggetti).
 - c. Scegli l'oggetto che rappresenta il Raspberry Pi. Nella pagina Details (Dettagli) per l'oggetto nel riquadro di navigazione a sinistra scegli Interact (Interagisci).
 - d. Copia tutto, incluso ".com", da REST API endpoint (Endpoint API REST).

The screenshot shows the AWS IoT Thing configuration interface. At the top, it displays the Thing name 'MyRaspberryPi' and its type 'NO TYPE'. On the left, there's a sidebar with various tabs: Details, Security, Thing Groups, Billing Groups, Shadow, Interact (which is highlighted with a red box), Activity, Jobs, Violations, Defender metrics, and a 'new' button. The main area is titled 'Thing ARN' and shows the ARN: arn:aws:iot:us-west-2:...:thing/MyRaspberryPi. Below that is the 'Type' section, which has a search bar and the text 'No type'.

4. Apri il file `aws_iot_config.h` e nella sezione `//Get from console` aggiorna i valori per gli elementi seguenti:

`AWS_IOT_MQTT_HOST`

Endpoint personale.

`AWS_IOT_MY_THING_NAME`

Nome dell'oggetto.

`AWS_IOT_ROOT_CA_FILENAME`

Certificato CA root.

`AWS_IOT_CERTIFICATE_FILENAME`

Certificato.

`AWS_IOT_PRIVATE_KEY_FILENAME`

Chiave privata.

Ad esempio:

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

```
#define AWS_IOT_PRIVATE_KEY_FILENAME "4bbdc778b9-private.pem.key"  
// =====
```

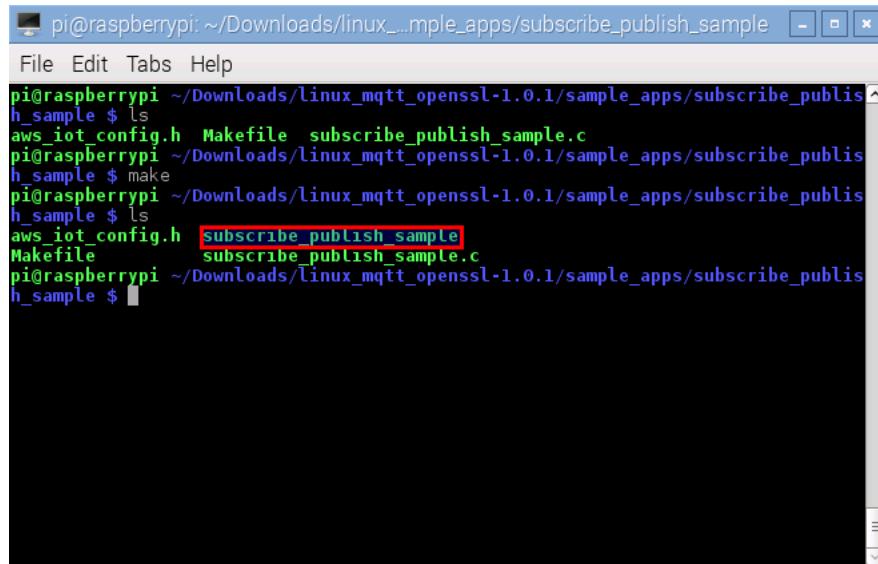
Esecuzione delle applicazioni di esempio

Esecuzione delle applicazioni di esempio SDK di dispositivo AWS IoT per Embedded C

1. Compila l'app `subscribe_publish_sample_app` usando il makefile incluso.

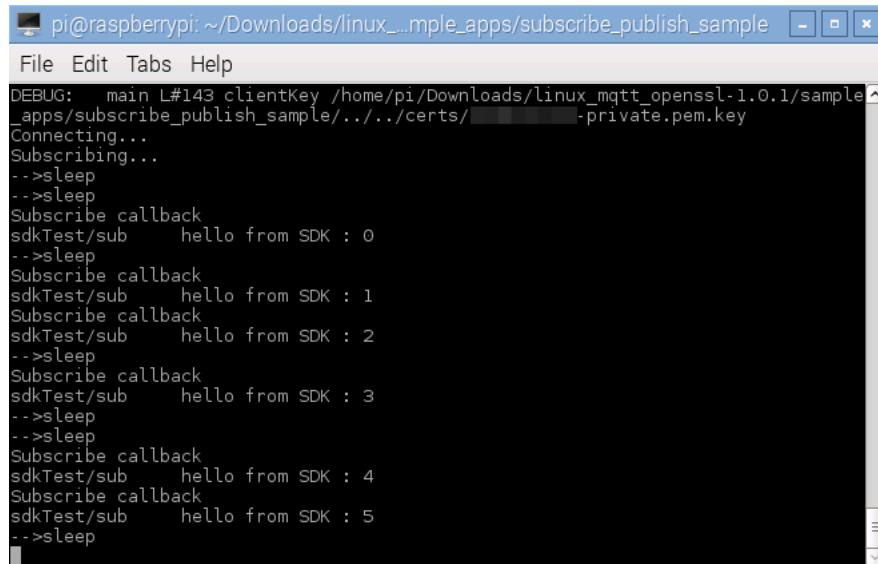
```
make -f Makefile
```

Verrà generato un file eseguibile.



```
pi@raspberrypi:~/Downloads/linux_mqtt_openssl-1.0.1/sample_apps/subscribe_publish_sample$ ls  
aws_iot_config.h Makefile subscribe_publish_sample.c  
pi@raspberrypi:~/Downloads/linux_mqtt_openssl-1.0.1/sample_apps/subscribe_publish_sample$ make  
pi@raspberrypi:~/Downloads/linux_mqtt_openssl-1.0.1/sample_apps/subscribe_publish_sample$ ls  
aws_iot_config.h subscribe_publish_sample  
Makefile subscribe_publish_sample.c  
pi@raspberrypi:~/Downloads/linux_mqtt_openssl-1.0.1/sample_apps/subscribe_publish_sample$
```

2. Esegui `subscribe_publish_sample_app`. Verrà visualizzato un output simile al seguente:



```
pi@raspberrypi:~/Downloads/linux_mqtt_openssl-1.0.1/sample_apps/subscribe_publish_sample$ ./subscribe_publish_sample  
DEBUG: main L#143 clientKey /home/pi/Downloads/linux_mqtt_openssl-1.0.1/sample_apps/subscribe_publish_sample/../../../../certs/-private.pem.key  
Connecting...  
Subscribing...  
-->sleep  
-->sleep  
Subscribe callback  
sdkTest/sub hello from SDK : 0  
-->sleep  
Subscribe callback  
sdkTest/sub hello from SDK : 1  
Subscribe callback  
sdkTest/sub hello from SDK : 2  
-->sleep  
Subscribe callback  
sdkTest/sub hello from SDK : 3  
-->sleep  
-->sleep  
Subscribe callback  
sdkTest/sub hello from SDK : 4  
Subscribe callback  
sdkTest/sub hello from SDK : 5  
-->sleep
```

Il componente Raspberry Pi è ora connesso ad AWS IoT tramite SDK di dispositivo AWS IoT per Embedded C.

Uso dell'SDK di dispositivo AWS IoT per JavaScript

Questa esercitazione mostra come installare Node.js, il programma di gestione del pacchetto npm, e il Device SDK per AWS IoT per JavaScript su un Raspberry Pi e come eseguire le applicazioni di esempio del dispositivo SDK.

Configurazione dell'ambiente di runtime per l'SDK di dispositivo AWS IoT per JavaScript

Per usare il Device SDK per AWS IoT per JavaScript, installare Node e il programma di gestione del pacchetto npm nel Raspberry Pi.

1. Per aggiungere il repository Node, apri un terminale ed esegui il comando seguente:

```
curl -sL https://deb.nodesource.com/setup_11.x | sudo -E bash -
```

2. Per installare Node ed npm, eseguire il comando seguente:

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

3. Per verificare l'installazione di Node ed npm, eseguire i comandi seguenti:

```
node -v
```

```
e
```

```
npm -v
```

Se da questi comandi viene visualizzato un numero di versione, l'installazione di Node ed npm è riuscita.

Installazione dell'SDK di dispositivo AWS IoT per JavaScript

Per installare il Device SDK per AWS IoT per JavaScript nel Raspberry Pi, creare una directory `~/deviceSDK` utilizzando il comando seguente:

```
mkdir deviceSDK
```

Utilizzare npm per installare l'SDK:

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

Al termine dell'installazione, dovresti notare una directory `node_modules` all'interno della directory `~/deviceSDK`.

Preparazione dell'esecuzione delle applicazioni di esempio

Seguire le istruzioni riportate in [Nozioni di base su AWS IoT \(p. 5\)](#) per registrare il Raspberry Pi con AWS IoT. In `aws-device-sdk-js` creare una directory `certs` e copiare i file di chiave privata, certificato e dell'autorità di certificazione root nella directory `certs`.

- Assegnare un nuovo nome alla chiave privata `node-private-key.pem`.
- Assegnare un nuovo nome al certificato `node-cert.pem`.

Per eseguire gli esempi del Device SDK per AWS IoT per JavaScript, sono necessarie le seguenti informazioni:

La regione AWS

È possibile trovare la regione in uso accedendo alla console AWS IoT e controllando l'URL. La regione viene visualizzata immediatamente dopo `https://` nell'URL. Ad esempio:

`https://us-west-2.console.aws.amazon.com/iot/home?region=us-west-2#/dashboard`

La regione AWS viene visualizzata anche dopo `?region=` nell'URL. Per ulteriori informazioni, consulta [Regioni ed endpoint AWS](#). Per informazioni sulle regioni specifiche di AWS IoT, consulta l'argomento relativo a [regioni ed endpoint AWS IoT](#).

Un ID client

Una stringa alfanumerica arbitraria utilizzata per identificare un dispositivo o un'applicazione che si connette a AWS IoT.

La chiave privata

Percorso completo della chiave privata sul Raspberry Pi. Si tratta della chiave generata al momento della registrazione del Raspberry Pi con AWS IoT.

Il certificato X.509 di AWS IoT

Percorso completo del certificato AWS IoT sul Raspberry Pi. Si tratta del certificato generato al momento della registrazione del Raspberry Pi con AWS IoT.

L'autorità di certificazione root del servizio STS Amazon

Percorso completo dell'autorità di certificazione root sul Raspberry Pi.

L'endpoint AWS IoT

È possibile trovare gli endpoint eseguendo il comando CLI `describe-endpoint`:

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

È possibile trovare gli endpoint anche accedendo alla console AWS IoT, scegliendo l'oggetto IoT per il Raspberry Pi e quindi scegliendo Interact (Interagisci). L'endpoint viene visualizzato in HTTPS e in Aggiorna lo shadow dispositivo con questo endpoint API Rest.

La porta su cui rimane in ascolto il broker di messaggi AWS IoT.

Questo è sempre 8883.

Nome dell'oggetto IoT

Si tratta del nome specificato al momento della registrazione del Raspberry Pi con AWS IoT.

Esecuzione delle applicazioni di esempio

Il Device SDK per AWS IoT per JavaScript include una serie di esempi nella directory `aws-iot-device-sdk-js/examples`. È consigliabile iniziare con `device-example.js`. Questo esempio viene eseguito in due modalità. In modalità 1 effettua la sottoscrizione all'argomento MQTT `topic_1` e pubblica un messaggio ogni 4 secondi in `topic_2`. In modalità 2 effettua la sottoscrizione a `topic_2` e pubblica un messaggio ogni 4 secondi in `topic_1`. È possibile eseguire due istanze di `device-example.js`, una in modalità 1 e una in modalità 2 e vedere i messaggi inviati e ricevuti.

Dalla directory `aws-iot-device-sdk-js/examples` eseguire il comando seguente per avviare un'istanza dell'esempio:

```
node device-example -k "../certs/node-private-key.pem" -c "../certs/node-cert.pem" -i "client-id-1" -H "<your-iot-endpoint>" -p 8883 -T "your-thing-name" --test-mode 1
```

Avviare un'altra istanza di `device-example.js` in esecuzione in modalità 2:

```
node device-example -k "../certs/node-private-key.pem" -c "../certs/node-cert.pem" -i "client-id-2" -H "<your-iot-endpoint>" -p 8883 -T "your-thing-name" --test-mode 2
```

Important

Assicurarsi di utilizzare ID client diversi per l'esecuzione delle due istanze di `device-example.js`. Due client (dispositivi o applicazioni) non possono connettersi a AWS IoT utilizzando lo stesso ID client. La connessione del primo client viene interrotta quando viene stabilita la connessione del secondo client.

Il nome dell'oggetto è importante solo quando si crea una policy specifica di un oggetto IoT. Nel tutorial Nozioni di base su AWS IoT non si crea una policy di questo tipo, pertanto è possibile utilizzare lo stesso nome oggetto per entrambe le istanze.

Il componente Raspberry Pi è ora connesso ad AWS IoT tramite l'SDK di dispositivo AWS IoT per JavaScript.

Se le istanze di esempio vengono eseguite correttamente, l'output dall'istanza in esecuzione in modalità 1 dovrebbe avere l'aspetto seguente:

```
substituting 250ms delay for true...  
connect  
message topic_1 {"mode1Process":1}  
message topic_1 {"mode1Process":2}  
message topic_1 {"mode1Process":3}  
message topic_1 {"mode1Process":4}  
...
```

L'output dall'istanza in esecuzione in modalità 2 dovrebbe avere l'aspetto seguente:

```
substituting 250ms delay for true...  
connect  
message topic_2 {"mode2Process":1}  
message topic_2 {"mode2Process":2}  
message topic_2 {"mode2Process":3}  
message topic_2 {"mode2Process":4}  
...
```

Se l'esempio non viene eseguito correttamente, provare ad aggiungere l'opzione `-d` quando si esegue l'esempio per visualizzare le informazioni di debug.

Tutorial AWS IoT aggiuntivi

I tutorial in questa sezione descrivono l'utilizzo congiunto di più servizi AWS IoT per ottenere una determinata attività. Questi tutorial illustrano soprattutto l'integrazione dei servizi piuttosto che approfondire le caratteristiche AWS IoT specifiche. I tutorial di questa sezione potrebbero essere correlati per dimostrare come sia possibile iniziare con soluzioni di base per poi evolverle e in che modo le tue esigenze cambiano o aumentano.

Ogni tutorial fornisce un elenco di prerequisiti, incluse eventuali esigenze di hardware specifiche. Laddove possibile, i tutorial forniranno alternative nel caso in cui tutto l'hardware necessario non fosse disponibile.

Esempio di irrigatura AWS IoT

Questo esempio pratico mostra come utilizzare AWS IoT per rilevare il livello di umidità corrente del terreno delle comuni piante d'appartamento in modo continuativo. Quando il livello di umidità diventa troppo basso, viene inviato un avviso via e-mail al possessore della pianta per ricordargli di innaffiarla.

Per ottenere la lettura dell'umidità effettiva si utilizzano componenti hardware, ad esempio un'unità **Raspberry Pi** e un kit di sensori dell'umidità del terreno, oltre a una comune pianta d'appartamento. Se non si hanno a disposizione l'hardware o la pianta, si possono simulare le letture dell'umidità del terreno generando letture casuali con il proprio computer di sviluppo. Questo esempio illustra entrambi gli approcci.

Indice

- [Modulo 1: Configurazione di AWS IoT e invio dei dati con il computer di sviluppo \(p. 111\)](#)
 - [Prerequisiti delle Fasi 1–5 \(p. 111\)](#)
 - [Fase 1: Creazione della policy AWS IoT \(p. 111\)](#)
 - [Fase 2: Creazione dell'oggetto \(p. 113\)](#)
 - [Fase 3: Invio e ricezione dei dati di test relativi all'oggetto \(p. 117\)](#)
 - [Fase 4: Configurazione di avvisi via e-mail per le letture di umidità basse \(p. 124\)](#)
 - [Fase 5: Simulazione di livelli di umidità casuali \(p. 129\)](#)
- [Modulo 2: Invio di dati con il Raspberry Pi \(p. 132\)](#)
 - [Prerequisiti delle Fasi 6–12 \(p. 132\)](#)
 - [Prerequisiti delle Fasi 6–12 \(p. 132\)](#)
 - [Fase 6: Preparazione della scheda microSDHC \(inizio\) \(p. 134\)](#)
 - [Fase 7: Download di Raspbian sulla scheda microSDHC \(p. 135\)](#)
 - [Fase 8: Preparazione della scheda microSDHC \(fine\) \(p. 137\)](#)
 - [Fase 9: Connessione a Raspberry Pi e configurazione di Raspbian \(p. 138\)](#)
 - [Fase 10: Configurazione del kit di sensori dell'umidità del terreno \(p. 142\)](#)
 - [Fase 11: Dati di acquisizione provenienti dal kit di sensori dell'umidità del terreno \(p. 148\)](#)
 - [Fase 12: Invio delle letture dei sensori dell'umidità del terreno a AWS IoT \(p. 149\)](#)
- [Pulizia \(p. 151\)](#)
- [Fasi successive \(p. 155\)](#)

Modulo 1: Configurazione di AWS IoT e invio dei dati con il computer di sviluppo

Nella prima parte di questa procedura guidata (fasi 1-5), configurerai AWS IoT affinché inizi a ricevere e archiviare le letture dell'umidità provenienti dal tuo computer di sviluppo, che fungerà da simulatore di dispositivo, o da un Raspberry Pi. Quindi, configurerai AWS IoT per l'invio di avvisi via e-mail basati su tali letture tramite Amazon Simple Notification Service (Amazon SNS).

Infine, utilizzerai il tuo computer di sviluppo per simulare letture dell'umidità del terreno generando dati casuali. Successivamente, inoltrerai le letture a AWS IoT. Se le letture diventano troppo basse, Amazon SNS invia automaticamente un avviso via e-mail.

Nel [Modulo 2 \(p. 132\)](#), potrai generare letture reali dell'umidità del terreno con un Raspberry Pi e inoltrarle a AWS IoT.

Prerequisiti delle Fasi 1–5

Per completare le prime cinque fasi di questo tutorial, hai bisogno di:

- Un account AWS
- Un utente amministratore IAM nell'account AWS. Potresti utilizzare l'utente root dell'account AWS anziché un utente amministratore IAM. Tuttavia, lo sconsigliamo.
- Un computer fisso o portatile di sviluppo che interagisca con la [console AWS IoT](#) da un browser Web e trasmetta letture simulate dell'umidità del terreno a AWS IoT. Il sistema operativo in esecuzione sul computer può essere Windows, macOS, Linux o Unix. Questo esempio è stato testato con un computer portatile con Windows 10 Enterprise Edition.

Fase 1: Creazione della policy AWS IoT

In questa fase, per consentire all'apparecchiatura Raspberry Pi (o al computer di sviluppo che lo simula) di eseguire operazioni AWS IoT, creerai una policy AWS IoT.

Per autenticare i dispositivi, AWS IoT utilizza certificati X.509. Le policy AWS IoT servono ad autorizzare i dispositivi a eseguire operazioni AWS IoT, ad esempio la sottoscrizione ad argomenti MQTT o la loro pubblicazione.

Se utilizzi l'hardware Raspberry Pi per questo esempio, esso presenterà il proprio certificato durante l'invio di messaggi a AWS IoT. Se invece utilizzi il tuo computer di sviluppo per simulare letture dell'umidità, sarà il computer a presentare il proprio certificato durante l'invio di messaggi a AWS IoT.

In un secondo momento, collegherai la policy al certificato del dispositivo.

1. Utilizzare il browser Web del sistema operativo per accedere alla Console di gestione AWS, all'indirizzo <https://aws.amazon.com>.

Note

Per la procedura guidata di esempio, consigliamo di accedere utilizzando le credenziali di [utente amministratore IAM](#) nel proprio account AWS.

2. Nella barra di navigazione AWS, scegliere la regione AWS in cui si desidera creare le risorse AWS IoT nel proprio account AWS. Questo esempio è stato testato con la regione US East (N. Virginia).
3. Apri la [console AWS IoT](#). Per eseguire questa operazione, selezionare Services (Servizi) sulla barra di navigazione di AWS. Nella casella Find a service by name or feature (Trova un servizio per nome o caratteristica), inserire **IoT Core** e premere Enter (Invio).

4. Nella console AWS IoT, se il pulsante Get started (Inizia) è visibile, premerlo.
5. Nel riquadro di navigazione del servizio, espandere Secure (Sicurezza), quindi selezionare Policies (Policy).

6.



7. Se viene visualizzata la finestra di dialogo You don't have any policies yet (Non hai ancora policy), selezionare Create a policy (Crea una policy). In caso contrario, scegliere Create (Crea).
8. Fornire un Name (Nome) che rappresenti la policy, ad esempio **PlantWateringPolicy**.

Note

Se si decide di usare un altro nome, ricordarsi di sostituire il nome in tutto l'esempio.

9. In Action (Operazione), immettere **iot:***.
10. Per Resource ARN (Risorsa ARN), sostituire il valore suggerito con un asterisco (*).
11. Per Effect (Effetto), scegliere Allow (Consenti).
12. Selezionare Create (Crea).

Create a policy

Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters). To learn more about IoT policies go to the [AWS IoT Policies documentation page](#).

Name

① PlantWateringPolicy

Add statements

Policy statements define the types of actions that can be performed by a resource.

Action

② iot:*

Resource ARN

③ *

Effect

④ Allow Deny

Remove

Add statement

⑤ Create

The screenshot shows the 'Create a policy' interface. Step 1 highlights the 'Name' field with the value 'PlantWateringPolicy'. Step 2 highlights the 'Action' dropdown with the value 'iot:*'. Step 3 highlights the 'Resource ARN' field with the value '*'. Step 4 highlights the 'Effect' checkbox which is checked 'Allow'. Step 5 highlights the 'Create' button at the bottom right.

Fase 2: Creazione dell'oggetto

In questa fase, creerai un oggetto in AWS IoT, che rappresenterà il Raspberry Pi (o il computer di sviluppo che simula un dispositivo).

I dispositivi connessi a AWS IoT sono rappresentati da oggetti nel registro AWS IoT. Il registro permette di tenere traccia di tutti i dispositivi connessi al tuo account AWS in AWS IoT.

1. Con la [console AWS IoT](#) aperta, nel riquadro di navigazione del servizio, selezionare Manage (Gestione).
2. Se è visibile la finestra di dialogo Introducing AWS IoT Device Management (Presentazione di AWS IoT Device Management), selezionare Show me later (Mostra più tardi), oppure premere Esc.
3. Nel riquadro di navigazione del servizio, con l'elemento Manage (Gestione) espanso, selezionare Things (Oggetti).



4. Se è visibile la finestra di dialogo You don't have any things yet (Non hai ancora oggetti), selezionare Register a thing (Registra un oggetto). In caso contrario, scegliere Create (Crea).
5. Nella pagina Creating AWS IoT things (Creazione di oggetti AWS IoT), per Register a single AWS IoT thing (Registrazione di un singolo oggetto AWS IoT), selezionare Create a single thing (Crea un oggetto singolo).

Creating AWS IoT things

An IoT thing is a representation and record of your physical device in the cloud. Any physical device needs a thing record in order to work with AWS IoT. [Learn more.](#)

Register a single AWS IoT thing
Create a thing in your registry

Bulk register many AWS IoT things
Create things in your registry for a large number of devices already using AWS IoT, or register devices so they are ready to connect to AWS IoT.

Create a single thing

Create many things

Cancel

Create a single thing



- Nella pagina Add your device to the device registry (Aggiungi il tuo dispositivo al registro dei dispositivi), fornire un Name (Nome), che rappresenterà il proprio Raspberry Pi (o il computer di sviluppo che simula un dispositivo), ad esempio MyRPi.

Note

Se si decide di usare un altro nome, ricordarsi di sostituire il nome in tutto l'esempio.

- Lasciare il resto della pagina invariato, quindi selezionare Next (Avanti).
- Nella pagina Add a certificate for your thing (Aggiungi un certificato per l'oggetto), scegliere Create certificate (Crea certificato).

CREATE A THING

Add a certificate for your thing

STEP 2/3

A certificate is used to authenticate your device's connection to AWS IoT.

One-click certificate creation (recommended)
This will generate a certificate, public key, and private key using AWS IoT's certificate authority.

Create with CSR
Upload your own certificate signing request (CSR) based on a private key you own.

Use my certificate
Register your CA certificate and use your own certificates for one or many devices.

Skip certificate and create thing
You will need to add a certificate to your thing later before your device can connect to AWS IoT.

Create certificate

Create with CSR

Get started

Create thing without certificate



9. Per A certificate for this thing (Un certificato per questo oggetto), selezionare Download (Scarica). Quindi, seguire le indicazioni del browser Web sullo schermo per salvare il file il cui nome finisce in `certificate.pem.crt.txt` sul proprio computer di sviluppo locale.

Note

Anche se la finestra di dialogo mostra un file che finisce in `cert.pem`, il file che è stato scaricato terminerà in `certificate.pem.crt.txt`.

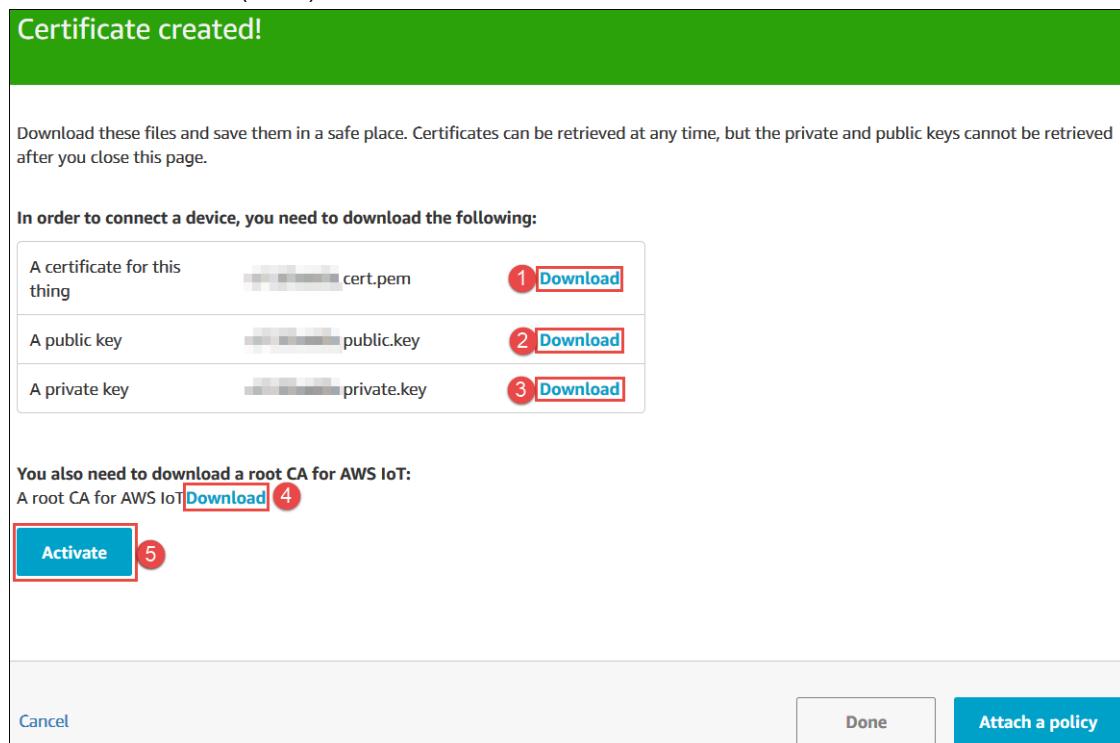
10. Ripetere la fase precedente in questa sezione per A public key (Una chiave pubblica), A private key (Una chiave privata) e A root CA for AWS IoT (Una CA root per IOT). Salvare i file che finiscono in `public.pem.key`, `private.pem.key` e `.pem`, rispettivamente, sul proprio computer di sviluppo.

Quando si sceglie il collegamento Download accanto a A root CA for AWS IoT (Una CA root per AWS IoT), viene visualizzata la sezione [Autenticazione del server \(p. 185\)](#) della Guida per sviluppatori AWS IoT. Qui, per ottenere la CA root per AWS IoT, fare clic sul collegamento Amazon Root CA 1 (CA root Amazon 1) in tale sezione, che consente di scaricare la chiave RSA a 2048 bit per l'endpoint di Amazon Trust Services.

Important

È possibile scaricare i file per A certificate for this thing (Un certificato per questo oggetto) e A root CA for AWS (Una CA root per AWS) in qualsiasi momento. Tuttavia, questa è l'unica opportunità per scaricare i file per A public key (Una chiave pubblica) e A private key for this thing (Una chiave privata per questo oggetto).

11. Selezionare Activate (Attiva).



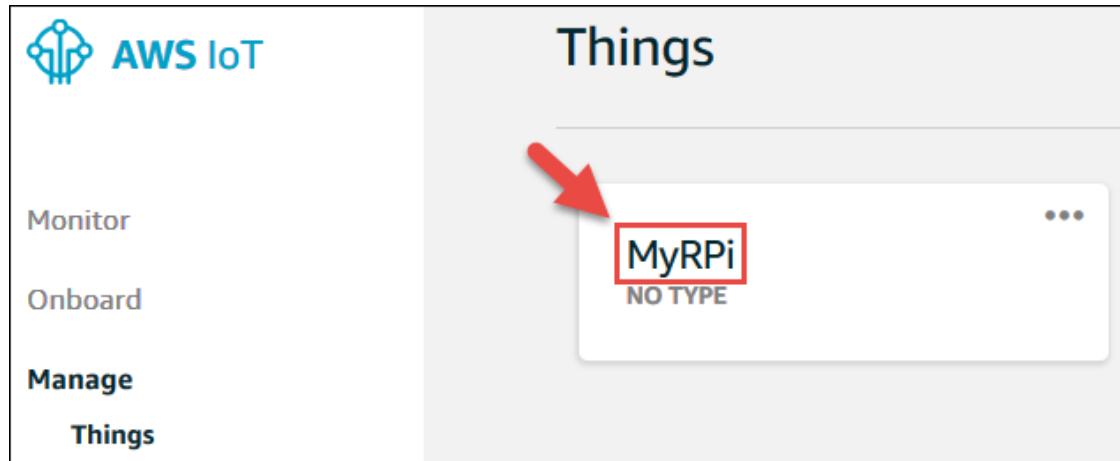
12. Scegliere Attach a policy (Collega policy).
13. Per Add a policy for your thing (Aggiungi una policy per il tuo oggetto), selezionare PlantWateringPolicy (0 policies selected (0 policy selezionate) si modificherà in 1 policy selected (1 policy selezionata)). Quindi, selezionare Register Thing (Registra l'oggetto).
14. Se viene visualizzata di nuovo la finestra di dialogo Introducing AWS IoT Device Management (Presentazione di ITDM), selezionare Show me later (Mostra più tardi), oppure premere Esc.

Fase 3: Invio e ricezione dei dati di test relativi all'oggetto

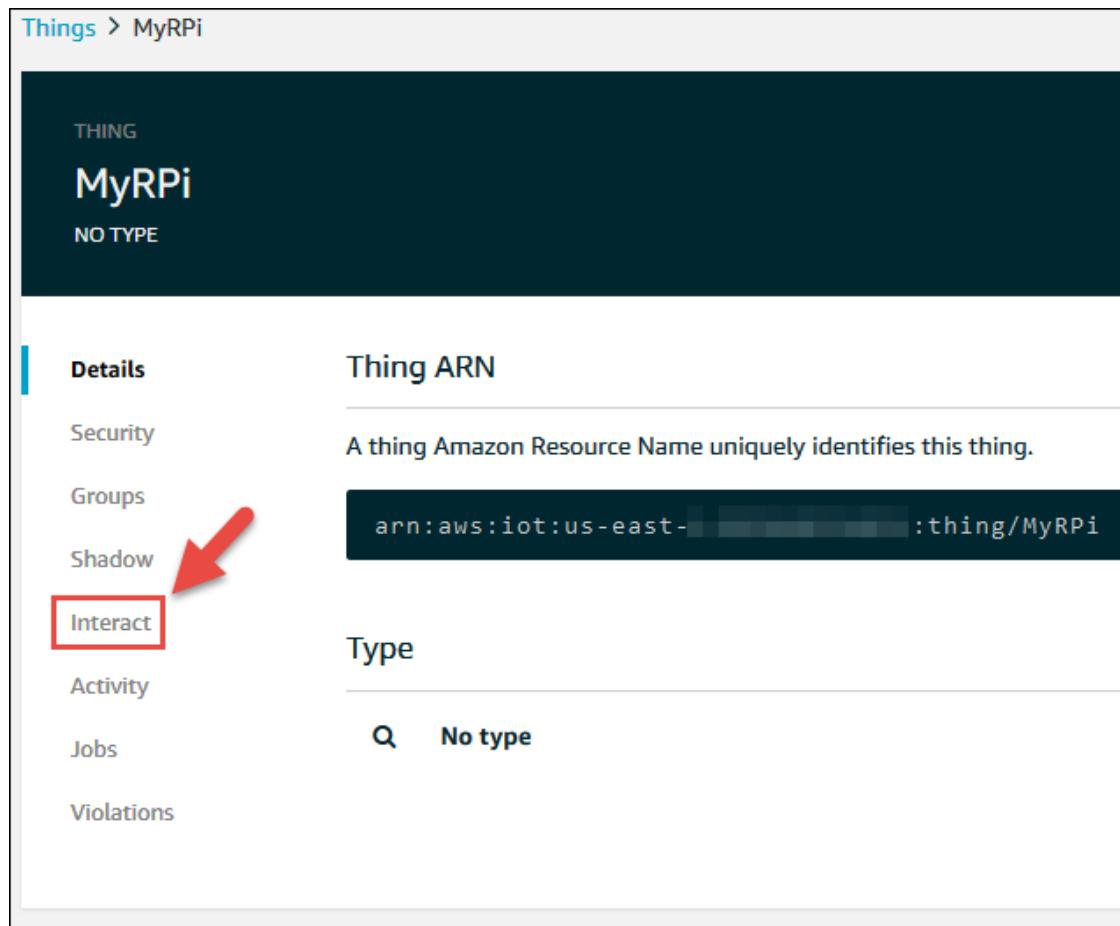
In questa fase, ti eserciterai a inviare dati di test alla shadow del dispositivo per il Raspberry Pi (o al computer di sviluppo che simula un dispositivo). In un secondo momento, potrai inviare dati reali provenienti dal kit di sensori dell'umidità del terreno tramite il Raspberry Pi alla relativa shadow oppure i dati simulati provenienti dal tuo computer di sviluppo alla relativa shadow.

La shadow di un dispositivo è un documento JSON archiviato in AWS IoT, che AWS IoT utilizza per salvare e recuperare informazioni sullo stato corrente di un dispositivo. Il [Servizio Device Shadow per AWS IoT \(p. 335\)](#) manterrà una shadow per ogni dispositivo che connetterai a AWS IoT. Puoi utilizzare la shadow per ottenere e impostare lo stato di un dispositivo, indipendentemente dal fatto che il dispositivo sia connesso a Internet o meno.

1. Nella [console AWS IoT](#), nella pagina Things (Oggetti), selezionare MyRPi.



2. Selezionare Interact (Interazione).



3. Per MQTT, annotare il valore per ciascuno dei seguenti argomenti MQTT, che consentono di impostare e recuperare gli aggiornamenti della shadow:
 - Aggiornamento di questo dispositivo shadow (ad esempio, \$aws/things/MyRPi/shadow/update)
 - Ottieni questo dispositivo shadow (ad esempio, \$aws/things/MyRPi/shadow/get)
 - Ottieni questo dispositivo shadow accettato (ad esempio, \$aws/things/MyRPi/shadow/get/accepted)

MyRPi

NO TYPE

Actions ▾

Details This thing already appears to be connected. Connect a device

Security

Groups

Shadow HTTPS

Update your Thing Shadow using this Rest API Endpoint. [Learn more](#)

Interact 1

Activity

Jobs MQTT

Violations

Use topics to enable applications and things to get, update, or delete the state information for a Thing (Thing Shadow)
[Learn more](#)

Update to this thing shadow 2 \$aws/things/MyRPi/shadow/update

Update to this thing shadow was accepted \$aws/things/MyRPi/shadow/update/accepted

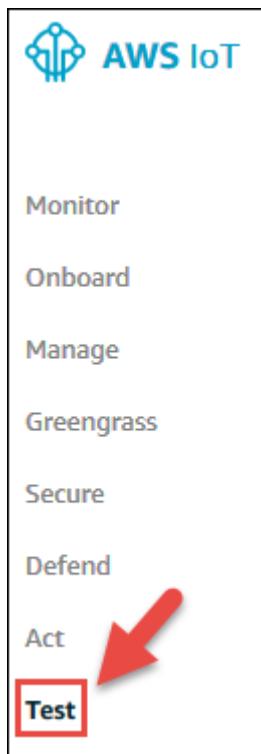
Update this thing shadow documents \$aws/things/MyRPi/shadow/update/documents

Update to this thing shadow was rejected \$aws/things/MyRPi/shadow/update/rejected

Get this thing shadow 3 \$aws/things/MyRPi/shadow/get

Get this thing shadow accepted 4 \$aws/things/MyRPi/shadow/get/accepted

4. Selezionare il pulsante Back (Indietro).
5. Se la finestra di dialogo Introducing AWS IoT Device Management (Presentazione della gestione dei dispositivi IoT) è visibile, selezionare Show me later (Mostra più tardi), oppure premere Esc.
6. Nel riquadro di navigazione del servizio, selezionare Test.



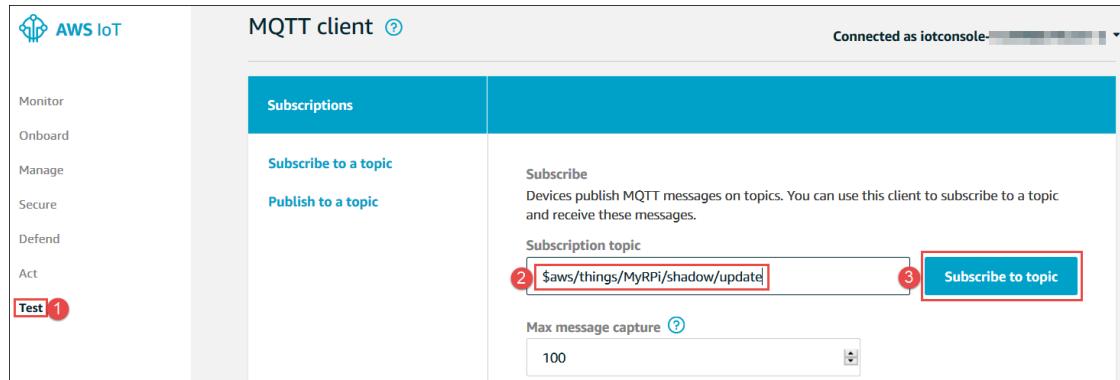
7. Per Subscription topic (Argomento sottoscrizione), inserire il valore dell'argomento MQTT annotato nello step 3 di questa procedura per Update to this thing shadow (Aggiorna alla shadow del dispositivo) (ad esempio, `$aws/things/MyRPi/shadow/update`), quindi selezionare Subscribe to topic (Effettua sottoscrizione all'argomento).

The screenshot shows the AWS IoT MQTT client interface. On the left, there is a sidebar with the same menu items as the main page. The main area is titled 'MQTT client' and shows a 'Connected as iotconsole...' status. Below this, there are two tabs: 'Subscriptions' (selected) and 'Publish to a topic'. Under 'Subscriptions', there is a 'Subscribe to a topic' section. It contains a text input field with the value '\$aws/things/MyRPi/shadow/update' (marked with a red box labeled 2) and a blue 'Subscribe to topic' button (marked with a red box labeled 3). Below the input field, there is a 'Max message capture' dropdown set to 100.

Important

Se all'oggetto è stato assegnato un nome diverso da MyRPi, ricordarsi di sostituire il nome MyRPi dell'oggetto nel nome dell'argomento MQTT menzionato in precedenza e negli altri nomi di argomenti MQTT della Fase 3. In caso contrario, non saranno visibili le attività relative all'argomento MQTT a cui è stata effettuata la sottoscrizione.

8. Selezionare Subscribe to a topic (Sottoscrizione a un argomento).



9. Ripetere gli step 7 e 8 di questa procedura per i valori dell'argomento MQTT annotato per Get this device shadow (Ottieni questa shadow del dispositivo) (ad esempio, **\$aws/things/MyRPi/shadow/get**) e Get this device shadow accepted (Richiesta di ottenere questa shadow oggetto accettata) (ad esempio, **\$aws/things/MyRPi/shadow/get/accepted**).
10. Ora, inoltrare i dati di alcuni test alla shadow. Per eseguire questa operazione, nel riquadro di navigazione del client MQTT, scegliere il valore dell'argomento MQTT per Update to thisdevice shadow (Aggiorna a questa shadow oggetto) (ad esempio, **\$aws/things/MyRPi/shadow/update**). Potrebbe essere necessario tenere fermo il puntatore del mouse sui valori troncati di un argomento per visualizzare il valore completo.
11. Nell'area di payload del messaggio, sostituire il payload corrente con il seguente:

```
{  
  "state": {  
    "desired": {  
      "welcome": null  
    },  
    "reported": {  
      "welcome": null,  
      "moisture": "low"  
    }  
  }  
}
```

Il payload precedente rimuove il valore di benvenuto predefinito per la shadow e aggiunge un valore di umidità con il valore `low` alla shadow.

12. Scegliere Publish to topic (Pubblica nell'argomento).

The screenshot shows the AWS IoT MQTT client interface. At the top, it says "Connected as iotconsole-1540416119545-0". The main area has a header "Subscriptions" and a single entry "\$aws/things/MyRPi/shadow/update". Below this is a "Publish" section with the instruction "Specify a topic and a message to publish with a QoS of 0." A text input field contains the topic "\$aws/things/MyRPi/shadow/update". To the right of the input field is a red box labeled "3" and a button labeled "Publish to topic". Below the input field is a code editor window containing a JSON payload:

```

1 {
2   "state": {
3     "desired": {
4       "welcome": null
5     },
6     "reported": {
7       "welcome": null,
8       "moisture": "low"
}

```

Two red circles are overlaid on the code editor: one labeled "1" pointing to the opening brace {}, and another labeled "2" pointing to the "moisture" key.

13. Per ottenere tali dati dalla shadow, selezionare il valore dell'argomento MQTT per Get this thing shadow (Ottieni questa shadow oggetto) (ad esempio, **\$aws/things/MyRPi/shadow/get**).
14. Nell'area di payload del messaggio, sostituire il payload corrente con il seguente:

```
{ }
```

Qui si utilizzano parentesi graffe vuote perché l'argomento MQTT Get this thing shadow (Ottieni questo shadow oggetto) accetta solo un payload vuoto.

15. Scegliere Publish to topic (Pubblica nell'argomento).

The screenshot shows the AWS IoT MQTT client interface. At the top, it says "Connected as iotconsole-1540416119545-0". The main area has a header "Subscriptions" and a single entry "\$aws/things/MyRPi/shadow/get". Below this is a "Publish" section with the instruction "Specify a topic and a message to publish with a QoS of 0." A text input field contains the topic "\$aws/things/MyRPi/shadow/get". To the right of the input field is a red box labeled "3" and a button labeled "Publish to topic". Below the input field is a code editor window containing a JSON payload:

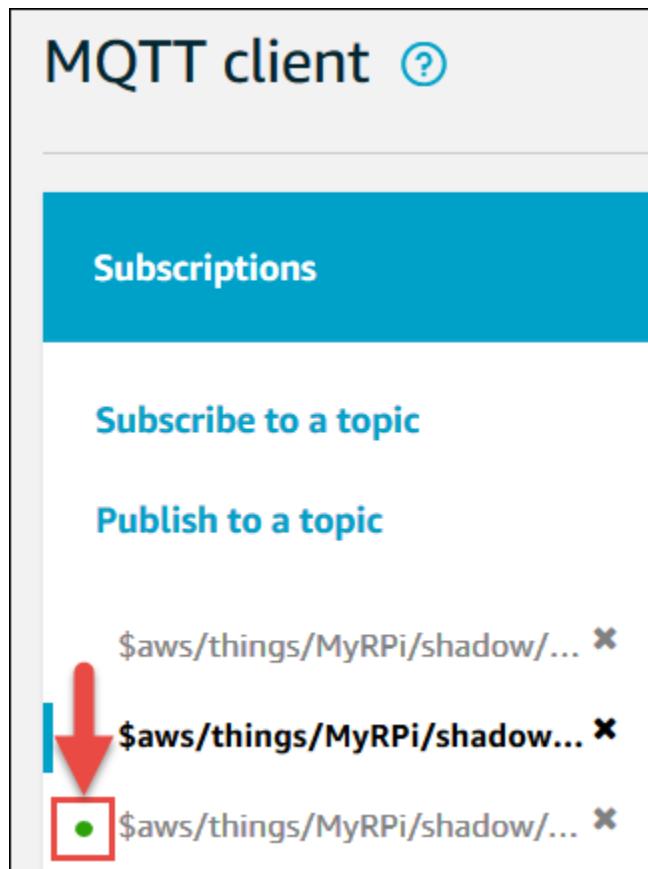
```

1 {
2   "state": {
3     "desired": {
4       "welcome": null
5     },
6     "reported": {
7       "welcome": null,
8       "moisture": "low"
}

```

Two red circles are overlaid on the code editor: one labeled "1" pointing to the opening brace {}, and another labeled "2" pointing to the "moisture" key.

Accanto al valore MQTT per Get this device shadow accepted (Richiesta di ottenere questa shadow oggetto accettata) è visibile un punto verde. Ciò significa che sono visibili nuove informazioni per tale argomento MQTT.



16. Scegliere il valore dell'argomento MQTT per Get this device shadow accepted (Richiesta di ottenere questa shadow dispositivo accettata) (ad esempio, `$aws/things/MyRPi/shadow/get/accepted`) e annotare l'output, ad esempio:

```
{  
  "state": {  
    "reported": {  
      "moisture": "low"  
    }  
  },  
  "metadata": {  
    "reported": {  
      "moisture": {  
        "timestamp": 1539272338  
      }  
    }  
  },  
  "version": 19,  
  "timestamp": 1539272436  
}
```

Nel precedente output, viene mostrato il valore `moisture` segnalato in precedenza, l'ora in cui si è verificato ogni evento corrispondente e la versione corrente del documento shadow.

17. Creare un altro aggiornamento della shadow. Per eseguire questa operazione, nel riquadro di navigazione del client MQTT, scegliere il valore dell'argomento MQTT per Update to thisdevice shadow (Aggiorna a questa shadow oggetto) (ad esempio, `$aws/things/MyRPi/shadow/update`).

18. Nell'area di payload del messaggio, sostituire il payload corrente con il seguente per modificare il valore di umidità corrente:

```
{  
  "state": {  
    "reported": {  
      "moisture": "okay"  
    }  
  }  
}
```

19. Scegliere Publish to topic (Pubblica nell'argomento).
20. Selezionare il valore dell'argomento MQTT per Get this device shadow (Ottieni questa shadow dispositivo) (ad esempio, **\$aws/things/MyRPi/shadow/get**).
21. Nell'area di payload del messaggio, sostituire il payload corrente con il seguente:

```
{}
```

22. Scegliere Publish to topic (Pubblica nell'argomento). Accanto al valore MQTT per Get this device shadow accepted (Richiesta di ottenere questa shadow oggetto accettata) è visibile un punto verde.
23. Scegliere il valore dell'argomento MQTT per Get this device shadow accepted (Richiesta di ottenere questa shadow dispositivo accettata) (ad esempio, **\$aws/things/MyRPi/shadow/get/accepted**) e annotare l'output, ad esempio:

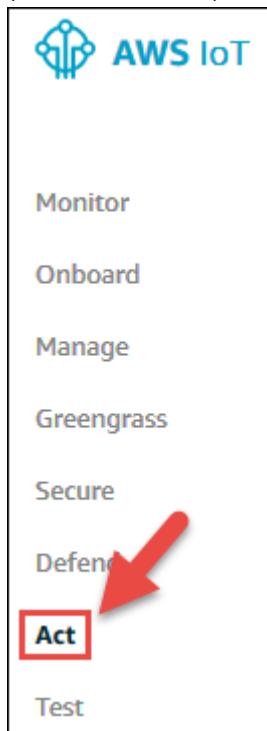
```
{  
  "state": {  
    "reported": {  
      "moisture": "okay"  
    }  
  },  
  "metadata": {  
    "reported": {  
      "moisture": {  
        "timestamp": 1539272823  
      }  
    }  
  },  
  "version": 20,  
  "timestamp": 1539272827  
}
```

Nel precedente output, viene mostrato il valore `moisture` appena modificato, l'ora in cui ogni evento corrispondente si è verificato e la nuova versione del documento shadow.

Fase 4: Configurazione di avvisi via e-mail per le letture di umidità basse

In questa fase configurerai Amazon Simple Notification Service (Amazon SNS) affinché invii automaticamente un avviso via e-mail al possessore della pianta d'appartamento per ricordargli di innaffiarla ogni volta che il livello di umidità del terreno è troppo basso.

1. Creare una regola AWS IoT per attivare l'avviso via e-mail tramite Amazon SNS. Per eseguire questa operazione, con la [console AWS IoT](#) aperta, nel riquadro di navigazione del servizio, selezionare Act (Esecuzione azioni).



2. Se viene visualizzata la finestra di dialogo You don't have any rules yet (Non hai ancora regole), selezionare Create a rule (Crea una regola). In caso contrario, scegliere Create (Crea).
3. Nella pagina Create a rule (Crea una regola), immettere un Name (Nome) per tale regola, ad esempio **MyRPiLowMoistureAlertRule**. Se si utilizza un altro nome, ricordarsi di sostituire il nome in tutto l'esempio.
4. Per Description (Descrizione), fornire una descrizione significativa per la regola, ad esempio **Sends an alert whenever soil moisture level readings are too low**.
5. Per Rule query statement (Istruzione query regola), con Using SQL version (Utilizzo della versione SQL) impostato su 2016-03-23, nella casella Rule query statement (Istruzione query regola) immettere la seguente istruzione AWS IoT su una sola riga, senza interruzioni di riga:

```
SELECT * FROM '$aws/things/MyRPi/shadow/update/accepted' WHERE state.reported.moisture = 'low'
```

Rule query statement

Indicate the source of the messages you want to process with this rule.

Using SQL version

2016-03-23

Rule query statement

To learn more about constructing a SQL statement, see [AWS IoT SQL Reference](#).

```
1 | SELECT * FROM '$aws/things/MyRPi/shadow/update/accepted' WHERE state.reported.moisture = 'low'
```

Questa istruzione attiva la regola ogni volta che il valore `moisture` è segnalato come `low` per l'argomento MQTT specificato.

Important

Se all'oggetto è stato assegnato un nome diverso da **MyRPi**, ricordarsi di sostituire il nome nella precedente istruzione SQL AWS IoT. In caso contrario, la regola potrebbe non essere attivata.

6. Per Set one or more actions (Imposta una o più operazioni), scegliere Add action (Aggiungi operazione).
7. Nella pagina Select an action (Seleziona un'operazione), selezionare Send a message as an SNS push notification (Invia un messaggio come notifica push SNS).

Select an action

Select an action.



Insert a message into a DynamoDB table
DYNAMODB



Split message into multiple columns of a database table (DynamoDBv2)
DYNAMODBV2



Invoke a Lambda function passing the message data
LAMBDA



Send a message as an SNS push notification
SNS

8. Selezionare Configure action (Configura operazione).
9. Nella pagina Configure action (Configura operazione), scegliere Create (Crea) per SNS target (Destinazione SNS). Immettere un nome per l'argomento SNS, ad esempio **MyRPiLowMoistureTopic**, quindi selezionare Create (Crea). Se si decide di usare un altro nome, ricordarsi di sostituire il nome in tutto l'esempio.
10. Per Message format (Formato messaggio), scegliere RAW.
11. Per IAM role name (Nome ruolo IAM), selezionare Create a new role (Crea un nuovo ruolo), quindi immettere un nome per il nuovo ruolo, ad esempio **MyRPiLowMoistureTopicRole**. Se si decide di usare un altro nome, ricordarsi di sostituire il nome in tutto l'esempio.
12. Scegliere Create a new role (Crea un nuovo ruolo).
13. Per IAM role name (Nome ruolo IAM), scegliere MyRPiLowMoistureTopicRole.
14. Selezionare Add action (Aggiungi operazione).

Configure action

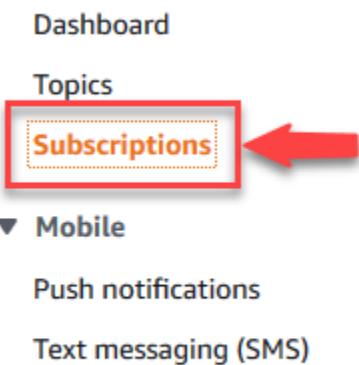
SNS target: MyRPiLowMoistureTopic 2 1 Create Clear Select

Message format: RAW 3

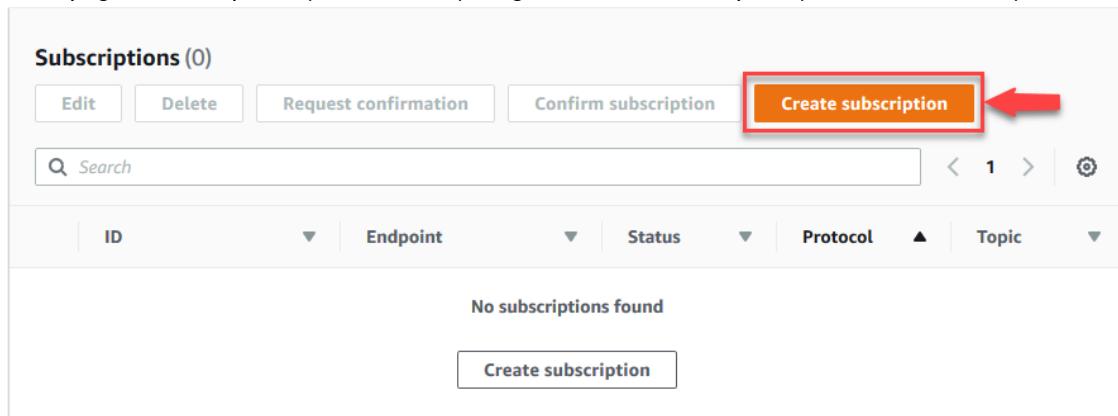
IAM role name: MyRPiLowMoistureTopicRole 5 Update role 4 Create a new role

Cancel 6 Add action

15. Scegliere Create rule (Crea regola).
16. Configurare Amazon SNS affinché invii messaggi tramite il proprio argomento Amazon SNS alla propria casella di posta. Sulla barra di navigazione AWS, scegliere Services (Servizi). Nella casella Find a service by name or feature (Trova un servizio per nome o caratteristica), inserire **SNS** e premere Enter (Invio).
17. Nel riquadro di navigazione, selezionare Subscriptions (Sottoscrizioni).



18. Nella pagina Subscriptions (Sottoscrizioni) scegliere Create subscription (Crea sottoscrizione).



19. Per Topic ARN (ARN argomento), scegliere l'ARN per l'argomento creato quando è stata configurata l'operazione precedente in questa procedura.

The screenshot shows the 'Create subscription' wizard. Step 1: 'Topic ARN' shows a search bar with 'arn:aws:iot:eu-central-1:123456789012:topic/MyRPiLowMoistureTopic' and a red box and arrow highlighting it. Step 2: 'Protocol' shows a dropdown menu set to 'Email' with a red box and arrow highlighting it. Step 3: 'Endpoint' shows an input field with '@amazon.com' and a red box and arrow highlighting it. Step 4: 'Subscription filter policy - optional' shows a note about confirming the subscription with a red box and arrow highlighting it. At the bottom right, there is a 'Cancel' button, a 'Create subscription' button highlighted with a red box and a red arrow pointing to it from the right, and a small red circle with the number '4' indicating the step.

20. Per Protocol, scegliere Email.
21. Per Endpoint, immettere il proprio indirizzo e-mail.
22. Scegliere Create Subscription (Crea sottoscrizione).
23. Monitorare la Posta in arrivo in attesa di un'e-mail di conferma della sottoscrizione intitolata AWS Notification - Subscription Confirmation from no-reply@sns.amazonaws.com (Notifica di AWS - Conferma della sottoscrizione da no-reply@sns.amazonaws.com). Quando si riceve l'e-mail, aprirla e fare clic sul collegamento Confirm subscription (Conferma sottoscrizione). Una volta selezionato il collegamento, verrà visualizzata una pagina di conferma nel browser Web. Si può chiudere questa pagina di conferma.

Important

Finché non si conferma la sottoscrizione, non si riceveranno avvisi via e-mail da questo argomento Amazon SNS, a prescindere dall'eventuale invio di avvisi da AWS IoT all'argomento.

Fase 5: Simulazione di livelli di umidità casuali

In questa fase, utilizzerai il computer di sviluppo per simulare letture dell'umidità del terreno generando dati casuali. In un secondo momento trasmitterai tali letture alla shadow corrispondente in AWS IoT. Quando le letture diventano troppo basse, Amazon SNS invia automaticamente un avviso via e-mail al possessore della pianta d'appartamento.

1. Verificare che sul computer di sviluppo siano installati [Python](#) e [pip](#).

pip è incluso nella versione di Python 3.4 e successive. Per controllare la versione installata di Python, eseguire il comando `python --version` dalla riga di comando in modalità di amministrazione per Windows o da una sessione del terminale in macOS, Linux o Unix. Per controllare se pip è installato, eseguire il comando `pip --version`.

2. Utilizzare pip per installare SDK di dispositivo AWS IoT per Python sul computer di sviluppo. A tale scopo, eseguire il comando `pip install AWSIoTPythonSDK`.
3. Utilizzare un editor di testo per creare un nuovo file sul computer di sviluppo con il codice seguente:

```
from AWSIoTPythonSDK.MQTTLib import AWSIoTMQTTShadowClient
import random, time

# A random programmatic shadow client ID.
SHADOW_CLIENT = "myShadowClient"

# The unique hostname that &IoT; generated for
# this device.
HOST_NAME = "yourhostname-ats.iot.us-east-1.amazonaws.com"

# The relative path to the correct root CA file for &IoT|,
# which you have already saved onto this device.
ROOT_CA = "AmazonRootCA1.pem"

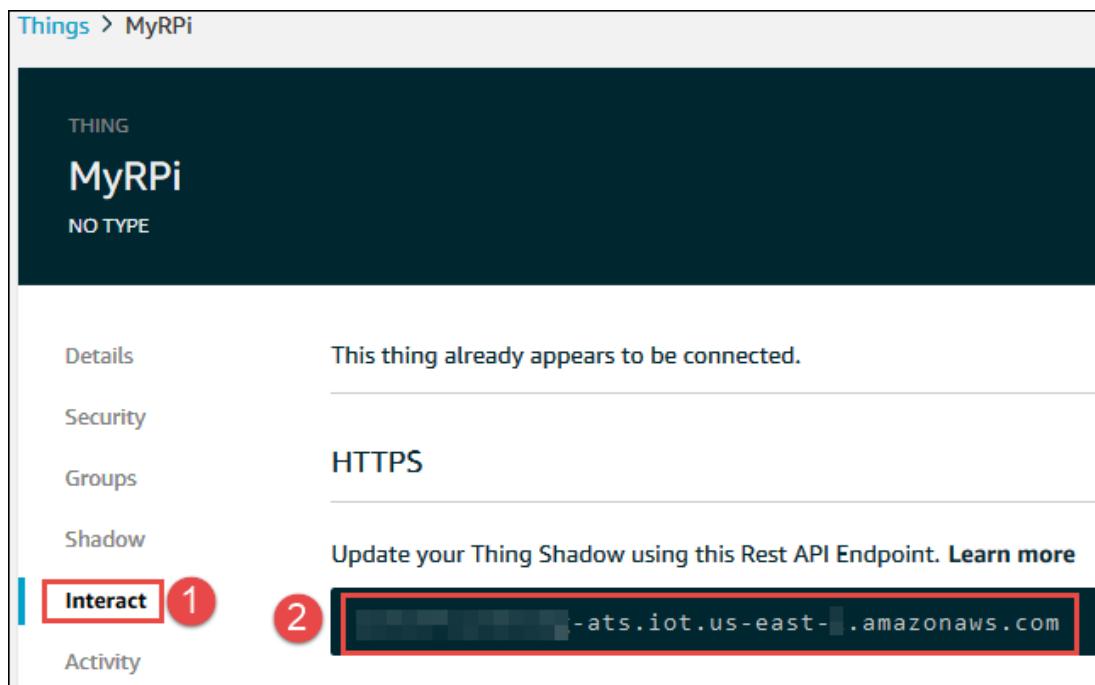
# The relative path to your private key file that
# &IoT; generated for this device, which you
# have already saved onto this device.
PRIVATE_KEY = "yourkeyid-private.pem.key"

# The relative path to your certificate file that
# &IoT; generated for this device, which you
# have already saved onto this device.
CERT_FILE = "yourkeyid-certificate.pem.crt.txt"
```

```
# A programmatic shadow handler name prefix.  
SHADOW_HANDLER = "MyRPi"  
  
# Automatically called whenever the shadow is updated.  
def myShadowUpdateCallback(payload, responseStatus, token):  
    print()  
    print('UPDATE: $aws/things/' + SHADOW_HANDLER +  
        '/shadow/update/#')  
    print("payload = " + payload)  
    print("responseStatus = " + responseStatus)  
    print("token = " + token)  
  
# Create, configure, and connect a shadow client.  
myShadowClient = AWSIoTMQTTShadowClient(SHADOW_CLIENT)  
myShadowClient.configureEndpoint(HOST_NAME, 8883)  
myShadowClient.configureCredentials(ROOT_CA, PRIVATE_KEY,  
    CERT_FILE)  
myShadowClient.configureConnectDisconnectTimeout(10)  
myShadowClient.configureMQTTOperationTimeout(5)  
myShadowClient.connect()  
  
# Create a programmatic representation of the shadow.  
myDeviceShadow = myShadowClient.createShadowHandlerWithName(  
    SHADOW_HANDLER, True)  
  
# Keep generating random test data until this script  
# stops running.  
# To stop running this script, press Ctrl+C.  
while True:  
    # Generate random True or False test data to represent  
    # okay or low moisture levels, respectively.  
    moisture = random.choice([True, False])  
  
    if moisture:  
        myDeviceShadow.shadowUpdate(  
            '{"state":{"reported":{"moisture":"okay"}}}',  
            myShadowUpdateCallback, 5)  
    else:  
        myDeviceShadow.shadowUpdate(  
            '{"state":{"reported":{"moisture":"low"}}}',  
            myShadowUpdateCallback, 5)  
  
    # Wait for this test value to be added.  
    time.sleep(60)
```

Nel codice precedente, sostituire i valori seguenti:

- **yourhostname-ats.iot.us-east-1.amazonaws.com** con l'endpoint dell'API REST che AWS IoT ha generato per l'utente. Per ottenere l'endpoint, nel riquadro di navigazione della [console AWS IoT](#), espandere Manage (Gestione), quindi scegliere Things (Oggetti) e infine selezionare il nome dell'oggetto (ad esempio, MyRPi). Scegliere Interact (Interazione) ed esaminare l'area HTTPS.



- *AmazonRootCA1.pem* con il nome della CA root per AWS IoT, salvata precedentemente sul computer di sviluppo.
 - *yourkeyid-private.pem.key* con il nome della chiave privata per il proprio dispositivo in AWS IoT, salvata precedentemente sul computer di sviluppo.
 - *yourkeyid-certificate.pem.crt.txt* con il nome del file del certificato root per il proprio dispositivo in AWS IoT, salvato precedentemente sul computer di sviluppo.
 - Il *60* in *time.sleep(60)* con il numero di secondi di attesa prima che ciascuna nuova lettura casuale simulata venga generata. Minore è il valore che si utilizza per questo numero, maggiore sarà la frequenza con cui si potrebbero ricevere avvisi via e-mail.
4. Salvare il file con estensione .py, ad esempio *moisture.py*, nella stessa directory in cui è stata salvata la CA root per AWS IoT, il file della chiave privata per il proprio dispositivo in AWS IoT e il certificato root del file per lo stesso dispositivo in AWS IoT. Se si decide di utilizzare un altro nome per il file .py, ricordarsi di sostituire il nome in tutto l'esempio.
 5. Spostarsi nella directory che contiene il file *moisture.py* dal prompt dei comandi in modalità di amministrazione per Windows o da una sessione del terminale in macOS, Linux o Unix. Quindi, eseguire il comando *python moisture.py* per Python per avviare l'esecuzione dello script *moisture.py*.

Ogni *60* secondi, lo script genera un valore casuale *True* o *False*. Se il valore è *True*, Python invia una lettura "moisture okay" a AWS IoT. Se il valore è *False*, Python invia una lettura di umidità bassa a AWS IoT. Quando AWS IoT riceve una lettura di umidità bassa, attiva una regola per l'invio di un avviso all'indirizzo e-mail dell'utente tramite Amazon SNS.

6. Al termine, premere *Ctrl+C* per interrompere l'esecuzione dello script.

Se non si ha a disposizione un Raspberry Pi, la procedura guidata di esempio è terminata e puoi passare direttamente a [Pulizia \(p. 151\)](#). In caso contrario, procedi con [Modulo 2: Invio di dati con il Raspberry Pi \(p. 132\)](#) per iniziare a preparare il tuo Raspberry Pi.

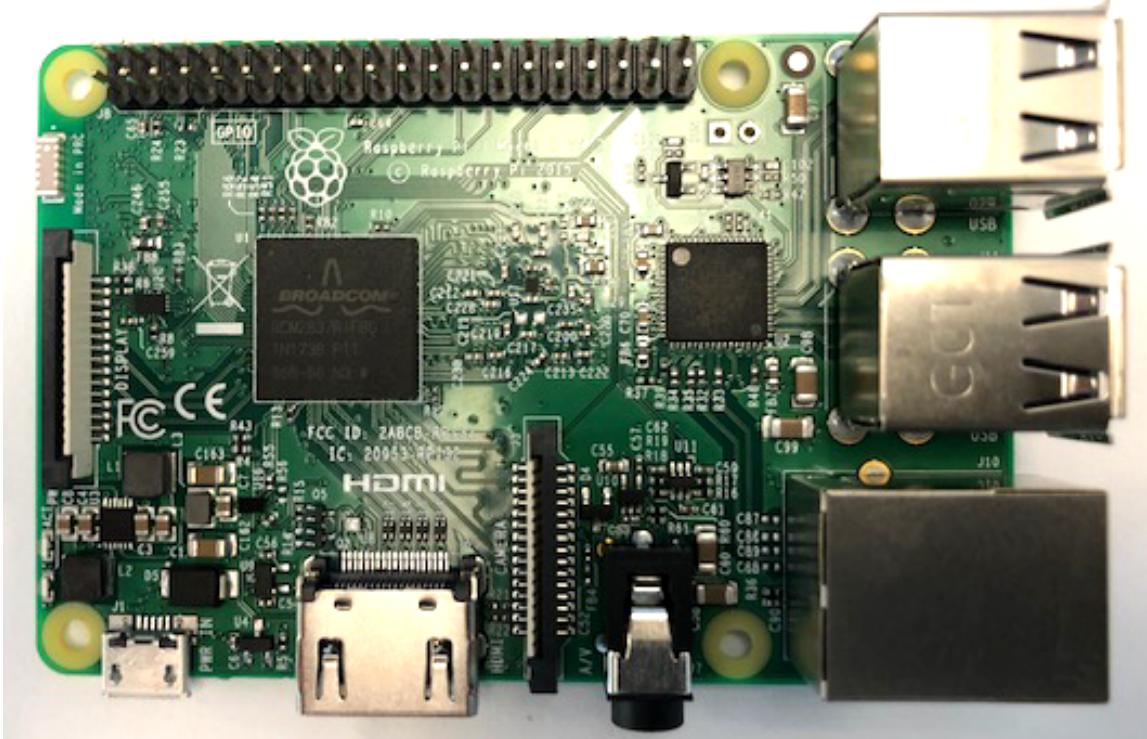
Modulo 2: Invio di dati con il Raspberry Pi

Prerequisiti delle Fasi 6–12

In [Modulo 1: Configurazione di AWS IoT e invio dei dati con il computer di sviluppo \(p. 111\)](#), hai utilizzato il computer di sviluppo per simulare letture di umidità del terreno generando dati casuali e hai inoltrato tali letture simulate a AWS IoT. Nella Parte 2 (Fasi 6–12), invece, genererai letture reali dell'umidità del terreno con un'apparecchiatura Raspberry Pi e le inoltrerai a AWS IoT.

Prerequisiti delle Fasi 6–12

- Completa tutte le fasi in [Modulo 1: Configurazione di AWS IoT e invio dei dati con il computer di sviluppo \(p. 111\)](#).
- Un'apparecchiatura Raspberry Pi 3. Questo esempio è stato testato con un'apparecchiatura [Raspberry Pi 3 Modello B](#).



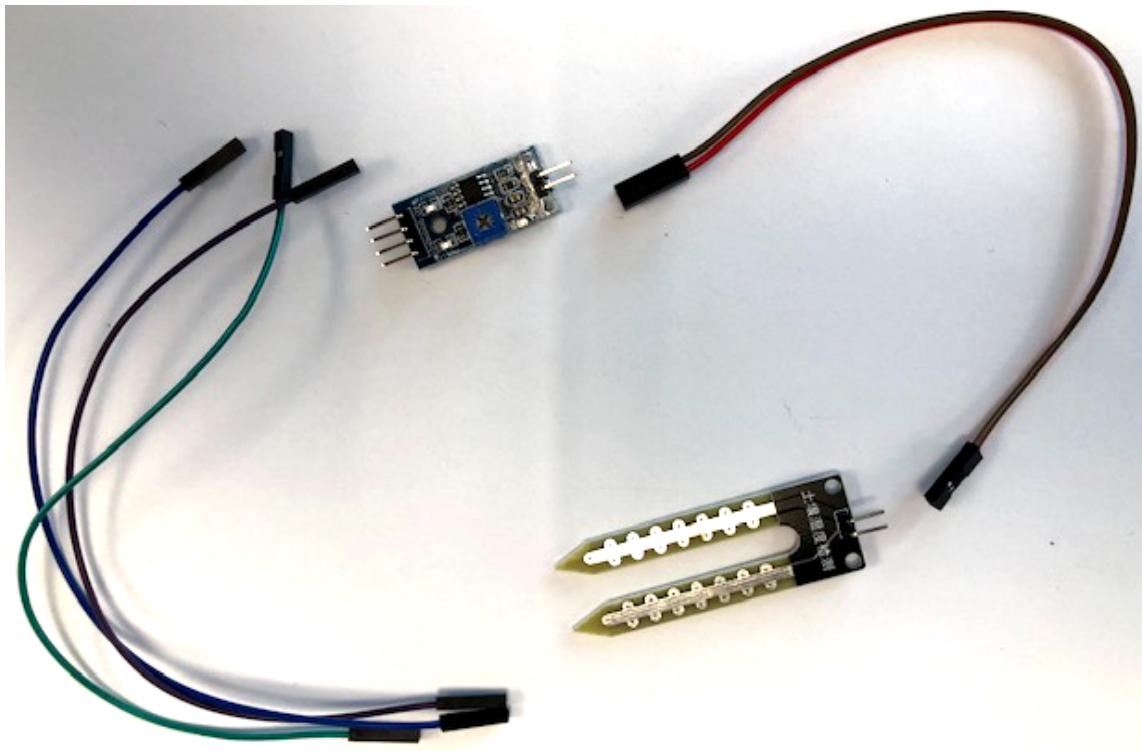
- Un [alimentatore adattatore micro USB](#) per Raspberry Pi 3 da almeno 5 V 2,5 A. Questo esempio è stato testato con un alimentatore da 5 V 2,5 A.



- Una [scheda micro SD](#) con almeno 16 GB. Questo esempio è stato testato con una scheda microSDHC da 16 GB.



- Un computer fisso o portatile di sviluppo con uno slot per la scheda micro SD o un lettore di schede micro SD in grado di connettersi al computer. Questo esempio è stato testato con un portatile con Windows 10 Enterprise e un lettore di schede SD integrato.
- Una rete per collegare il Raspberry Pi a AWS IoT e, facoltativamente, per collegare il tuo computer di sviluppo all'apparecchiatura Raspberry Pi. Tale configurazione di rete può consistere in una rete wireless o nel router di una rete fisica collegabile con cavi Ethernet. Il Raspberry Pi 3 Modello B offre sia il Wi-Fi integrato che una porta Ethernet. Questo esempio è stato testato con una rete wireless.
- Se non desideri accedere al Raspberry Pi dal tuo computer di sviluppo, devi collegare l'apparecchiatura Raspberry Pi a una tastiera, un mouse e un monitor separati. L'apparecchiatura Raspberry Pi 3 Modello B è dotata di quattro porte USB e una porta HDMI full-size. Questo esempio è stato testato con una tastiera, un mouse USB e un monitor con ingresso HDMI.
- Un [kit di sensori dell'umidità del terreno](#) compatibile con Raspberry Pi. Il kit include il modulo di rilevamento (la "sonda") e un microcontroller. Hai inoltre bisogno di due cavi di connessione femmina-femmina, dal modulo di rilevamento al microcontroller, e di tre cavi di connessione femmina-femmina, dal microcontroller ai pin GPIO integrati del Raspberry Pi. Questo esempio è stato testato con un sensore di umidità del terreno Gikfun.



- Un bicchiere d'acqua.
- Una pianta d'appartamento comune.

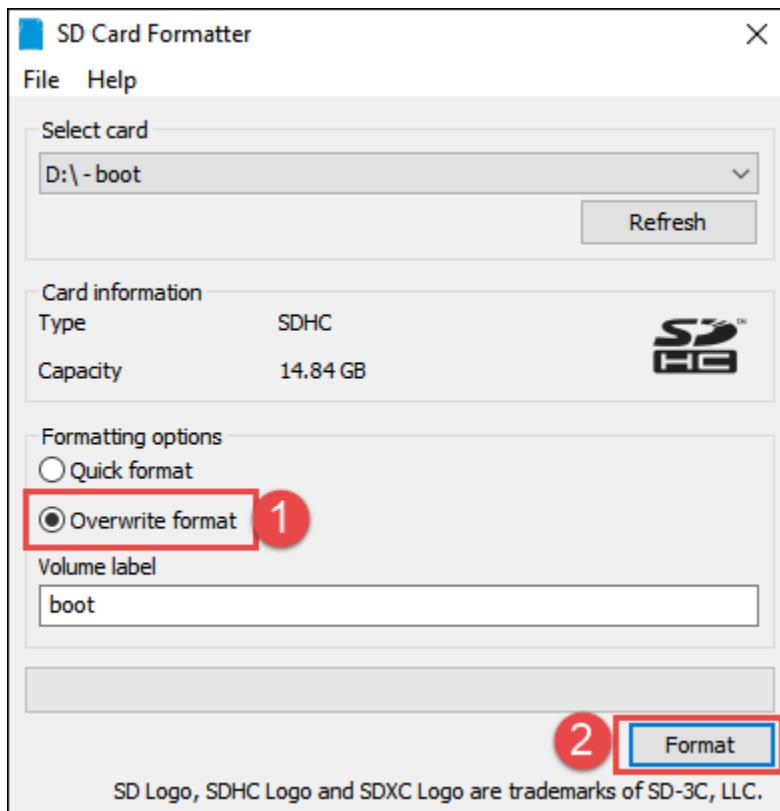
Fase 6: Preparazione della scheda microSDHC (inizio)

In questa fase, preparerai una scheda microSDHC per l'archiviazione del sistema operativo del Raspberry Pi.

Se già possiedi un Raspberry Pi con un sistema operativo come Raspbian installato, collegati al Raspberry Pi e passa direttamente a [Fase 10: Configurazione del kit di sensori dell'umidità del terreno \(p. 142\)](#).

Inserire una scheda microSDHC vuota nel computer fisso o portatile. Utilizzare un'app o un'utilità per la formattazione di schede SD per formattare la scheda SD. Ad esempio, se si utilizza Windows o macOS, completare le fasi seguenti:

1. a. Scaricare e installare [SD Card Formatter](#).
2. Eseguire SD Card Formatter.
3. In Select card (Selezione carta) dovrebbe essere già impostata la lettera dell'unità corrispondente alla scheda microSDHC. In caso contrario, selezionarla.
4. Per Formatting options (Opzioni di formattazione), scegliere Overwrite format (Sovrascrivi formato).
5. Scegliere Format (Formatta).



Quando viene chiesto se procedere alla formattazione della scheda microSDHC, scegliere Yes (Si). L'operazione di formattazione può richiedere alcuni minuti.

Fase 7: Download di Raspbian sulla scheda microSDHC

In questa fase scaricherai Raspbian sulla scheda microSDHC formattata. Raspbian è un sistema operativo basato su Debian e ottimizzato per l'hardware Raspberry Pi.

1. Accedere alla pagina [Raspberry Pi Downloads](#).
2. Scegliere Raspbian.
3. Nella pagina Download Raspbian (Scarica Raspbian), per Raspbian Stretch with Desktop (Raspbian Stretch con desktop), scegliere Download ZIP (Scarica ZIP).

The screenshot shows the official Raspbian website. At the top, there's a navigation bar with links for Blog, Downloads, Community, Help, Forums, and Education. A small green icon with the letters 'BI' is visible on the right side. Below the navigation, a red banner displays the word 'RASPBIAN'. The main content area contains text about Raspbian being the Foundation's official supported operating system, mentioning NOOBS and an installation guide. It also notes that Raspbian comes pre-installed with various software like Python, Scratch, Sonic Pi, and Java. A note cautions against using older unzip tools and suggests using 7Zip or The Unarchiver. Two download options are shown: 'RASPBIAN STRETCH WITH DESKTOP' and 'RASPBIAN STRETCH LITE'. Each option includes a small image of the Raspberry Pi logo inside a case, version information (e.g., Version: October 2018, Release date: 2018-10-09), and download links for Torrent and ZIP files. SHA-256 checksums are also provided.

RASPBIAN STRETCH WITH DESKTOP
Image with desktop based on Debian Stretch
Version: October 2018
Release date: 2018-10-09
Kernel version: 4.14
Release notes: [Link](#)
[Download Torrent](#) [Download ZIP](#)

RASPBIAN STRETCH LITE
Minimal image based on Debian Stretch
Version: October 2018
Release date: 2018-10-09
Kernel version: 4.14
Release notes: [Link](#)
[Download Torrent](#) [Download ZIP](#)

4. Utilizzare un'app o un'utilità che esegue il flashing di immagini per eseguire il flashing del file.zip appena scaricato sulla scheda microSDHC. Ad esempio, per Windows, macOS, or Linux:

1. scaricare e installare [Etcher](#).
2. Eseguire Etcher.
3. Scegliere Select image (Seleziona immagine).
4. Scegliere il file .zip appena scaricato.
5. Accanto all'immagine dell'unità, se la scheda microSDHC non è selezionato, sceglierla.
6. Scegliere Flash! (Esegui flashing)



L'operazione di flashing può richiedere alcuni minuti.

Fase 8: Preparazione della scheda microSDHC (fine)

In questa fase, aggiungerai alcuni file alla scheda microSDHC. Questi file consentono di connettersi al Raspberry Pi da un computer fisso o portatile e abilitare la comunicazione tra il Raspberry Pi e AWS IoT.

- Se si prevede di connettersi a Raspberry Pi dal proprio computer fisso o portatile, è necessario creare un file vuoto denominato `ssh` nella radice della scheda microSDHC. Questo file consente di connettersi a Raspberry Pi da uno strumento di connessione SSH (ad esempio, PuTTY per Windows, l'utilità SSH in GitBash per Windows o l'utilità SSH per macOS, Linux o Unix) dopo l'avvio di Raspberry Pi.

Ad esempio, per Windows, nel prompt dei comandi in modalità amministratore, eseguire il comando seguente, che crea un file vuoto denominato `ssh` nella radice della scheda microSDHC. Tale comando presume che la scheda microSDHC sia collegata come unità D.

```
fsutil file createnew D:\ssh 0
```

- Se si prevede di connettersi a Raspberry Pi dal proprio computer fisso o portatile, è necessario creare un file vuoto denominato `wpa_supplicant.conf` nella radice della scheda microSDHC. Questo file consente al Raspberry Pi di connettersi a una rete wireless.

Ad esempio, per Windows, nello stesso prompt dei comandi, eseguire il comando seguente, che crea un file vuoto denominato `wpa_supplicant.conf` nella radice della scheda microSDHC. Tale comando presume che la scheda microSDHC sia collegata come unità D.

```
fsutil file createnew D:\wpa_supplicant.conf 0
```

- Se è stato creato il file vuoto `wpa_supplicant.conf`, aprire un editor di testo e aggiungere i seguenti contenuti per il file `wpa_supplicant.conf`. Quindi, salvare il file.

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
network={
    ssid="MyWirelessNetworkName"
    psk="MyWirelessNetworkPassword"
    key_mgmt=WPA-PSK
}
```

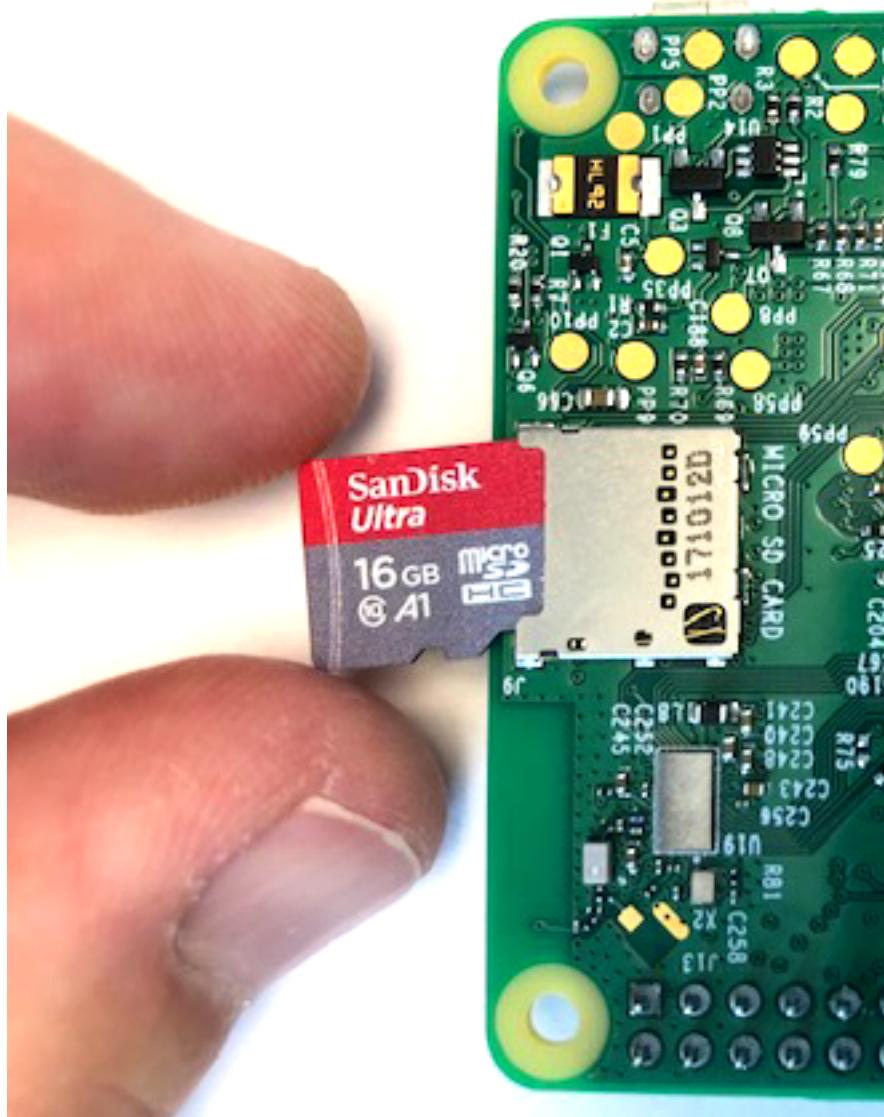
Nel contenuto precedente, sostituire *MyWirelessNetworkName* con il nome della rete wireless. Sostituire *MyWirelessNetworkPassword* con la password per la rete wireless. Per ulteriori informazioni, consultare [Wireless connectivity](#) sul sito Web di Raspberry Pi.

4. Creare una cartella nella radice della scheda microSDHC denominata deviceSDK.
5. Copiare i file generati da AWS IoT per l'utente che finiscono in .certificate.pem.crt.txt (file del certificato root del dispositivo in AWS IoT), private.pem.key (chiave privata del dispositivo in AWS IoT) e .pem (CA root per AWS IoT) nella nuova cartella deviceSDK.
6. Copiare il file con nome moisture.py da [Fase 5: Simulazione di livelli di umidità casuali \(p. 129\)](#) nella nuova cartella deviceSDK.
7. Espellere la scheda microSDHC dal computer fisso o portatile.

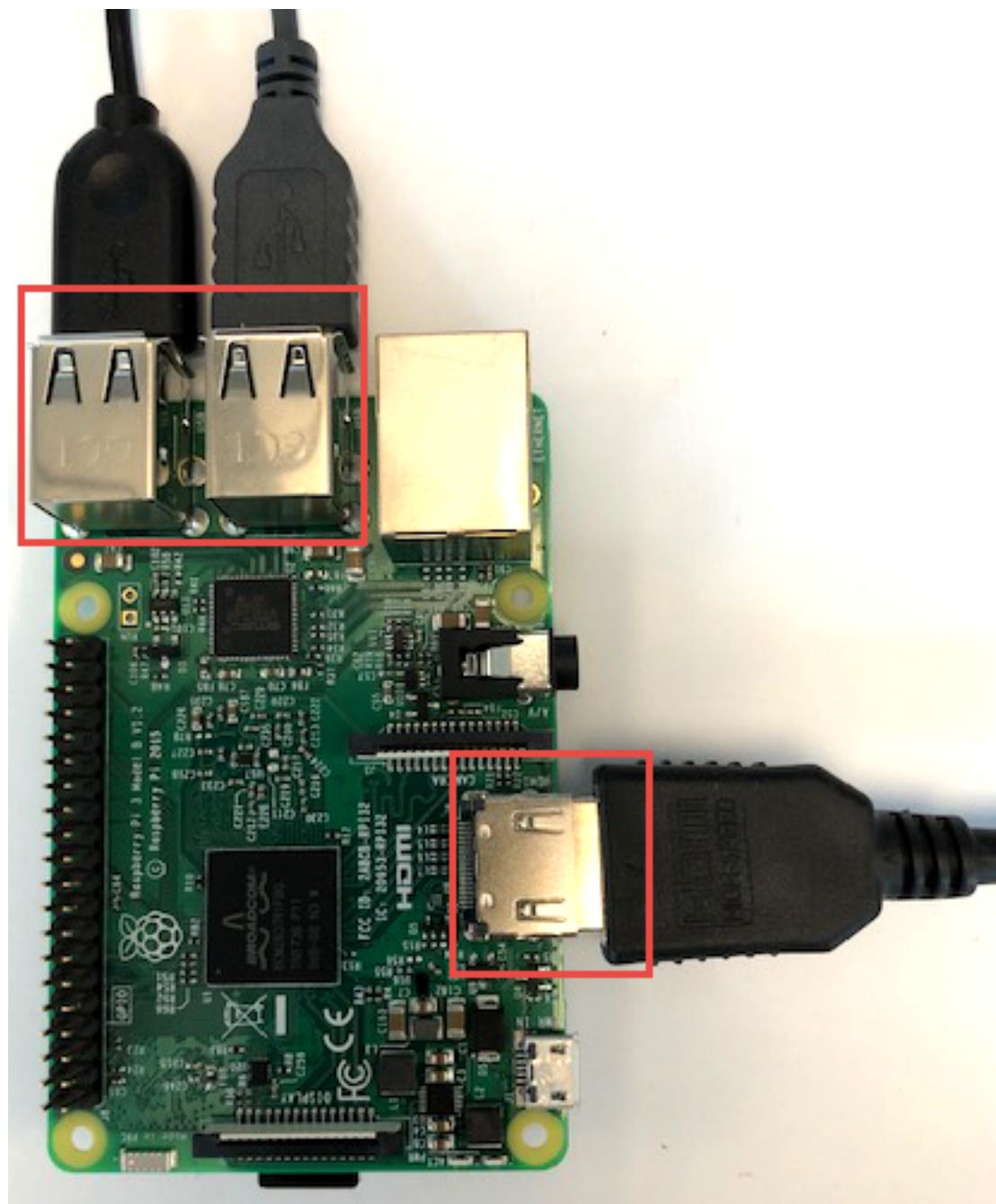
Fase 9: Connessione a Raspberry Pi e configurazione di Raspbian

In questa fase, avvierai il Raspberry Pi. Ti conserverai direttamente dal tuo computer fisso o portatile. Se ti connetti direttamente al Raspberry Pi, configurerai Raspbian sul Raspberry.

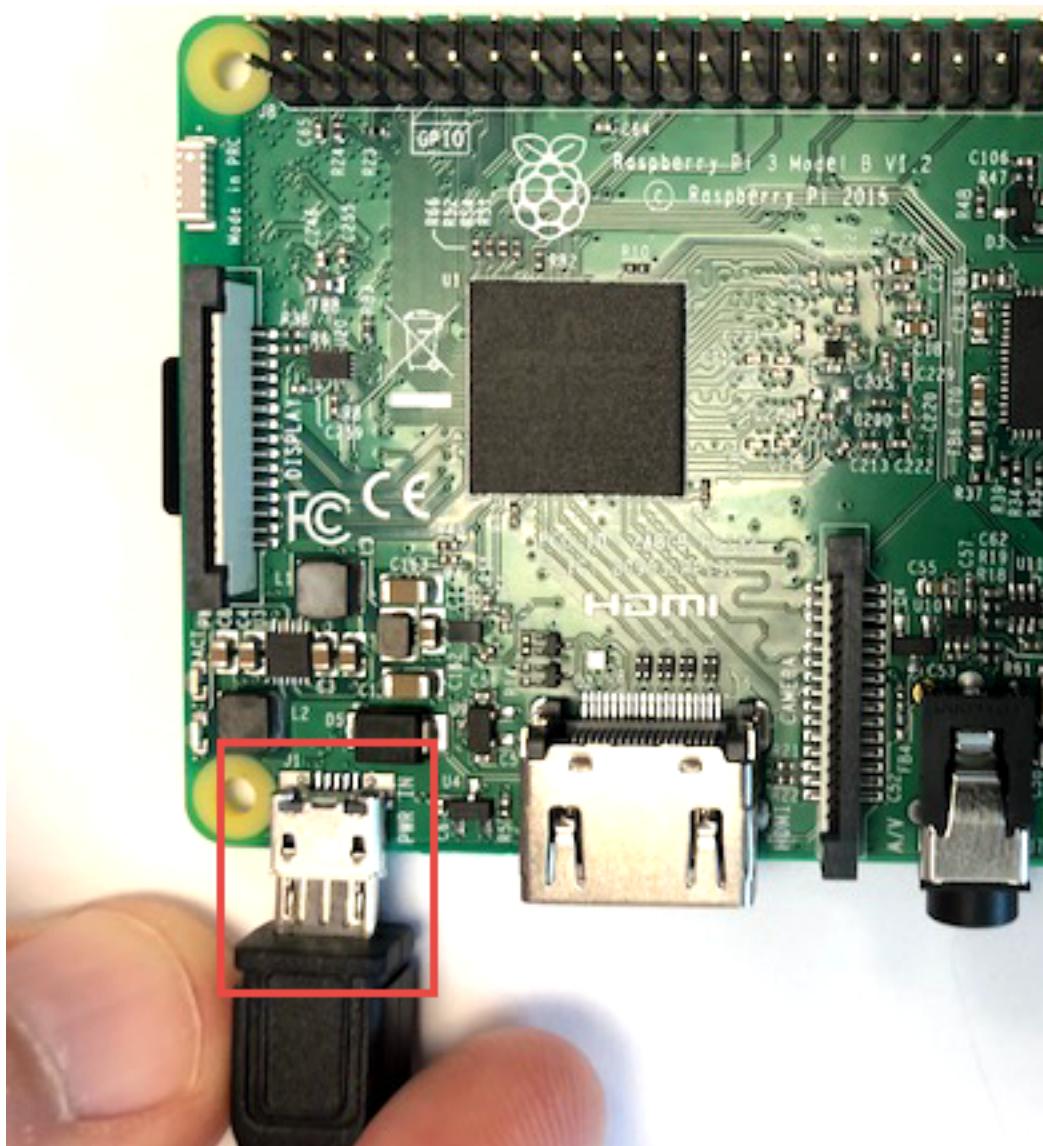
1. Inserire la scheda microSDHC nel Raspberry Pi. Lo slot della scheda si trova sul lato inferiore della scheda madre. La scheda può essere inserita nello slot in un solo verso, di solito con la scritta rivolta verso l'alto.



2. Se si desidera accedere al Raspberry Pi direttamente, anziché dal computer di sviluppo, collegare una tastiera, un mouse e un monitor direttamente al Raspberry Pi, ad esempio utilizzando le porte USB e HDMI. Anche se il Raspberry Pi 3 è dotato di connettività Bluetooth, non sarà possibile collegarsi tramite Bluetooth finché non si avvia Raspberry Pi per la prima volta.



3. Inserire i connettori dell'alimentatore adattatore micro USB nella sorgente di alimentazione, quindi collegare l'estremità della micro USB nel relativo slot del Raspberry Pi.



La luce LED rossa dell'alimentazione del Raspberry Pi si accende, quella verde dell'attività inizia a emettere sbarfallii e il sistema operativo Raspbian si avvia automaticamente. Se si accede al Raspberry Pi dal computer di sviluppo, il Raspberry Pi tenta di collegarsi alla rete wireless utilizzando la password specificata precedentemente nel file `wpa_supplicant.conf`.

4. Se non si desidera accedere al Raspberry Pi dal proprio computer di sviluppo, passare direttamente alla fase 5 della procedura.

Per accedere al Raspberry Pi dal proprio computer di sviluppo, ottenere l'indirizzo IP del Raspberry Pi, che è ora connesso alla rete wireless. Se, ad esempio, si può effettuare l'accesso al router della rete wireless come amministratore, si dovrebbe essere anche in grado di ricercare l'indirizzo IP nella rete. In caso contrario, si potrebbe utilizzare un'utilità, ad esempio il comando ping, oppure un'applicazione, ad esempio [Nmap per Windows](#).

Dopo aver ottenuto l'indirizzo IP del Raspberry Pi, connettersi al Raspberry Pi dal proprio computer fisso o portatile con Windows utilizzando uno strumento di connessione SSH, ad esempio [PuTTY](#) o l'utilità SSH in [Git Bash per Windows](#).

Se si utilizza PuTTY, per Host Name (Nome host) (o per l'indirizzo IP) utilizzare il formato `pi@X.X.X.X`. Per SSH, utilizzare `ssh pi@X.X.X.X`. In entrambi i casi, pi è il nome utente predefinito e X.X.X.X è l'indirizzo IP di Raspberry Pi. Quando viene richiesta la password, utilizzare quella predefinita, `raspberry`.

Passare a [Fase 10: Configurazione del kit di sensori dell'umidità del terreno \(p. 142\)](#).

5. Per accedere al Raspberry Pi direttamente anziché dal proprio computer di sviluppo, accendere il monitor collegandolo alla sorgente di input corretta (ad esempio, all'ingresso HDMI).

È possibile che venga visualizzata una finestra di dialogo in cui si segnala che SSH è abilitato sul Raspberry Pi e che la password predefinita per l'utente pi non è stata cambiata. Si può chiudere questa finestra di dialogo, per ora, perché sarà possibile modificare la password in un passaggio successivo di questa fase.

6. Al primo avvio di Raspberry Pi, viene visualizzata la finestra di dialogo Welcome to Raspberry Pi (Benvenuto in Raspberry Pi). Scegliere Next (Avanti).
7. Nella pagina Set Country (Imposta il paese), scegliere il Country (Paese), la Language (Lingua) e il Timezone (Fuso orario) desiderati. Se si dispone di una tastiera USA, selezionare la casella US keyboard (Tastiera USA).
8. Scegliere Next (Avanti).
9. Nella pagina Change Password (Cambia password), immettere una nuova password per l'utente predefinito pi.

Note

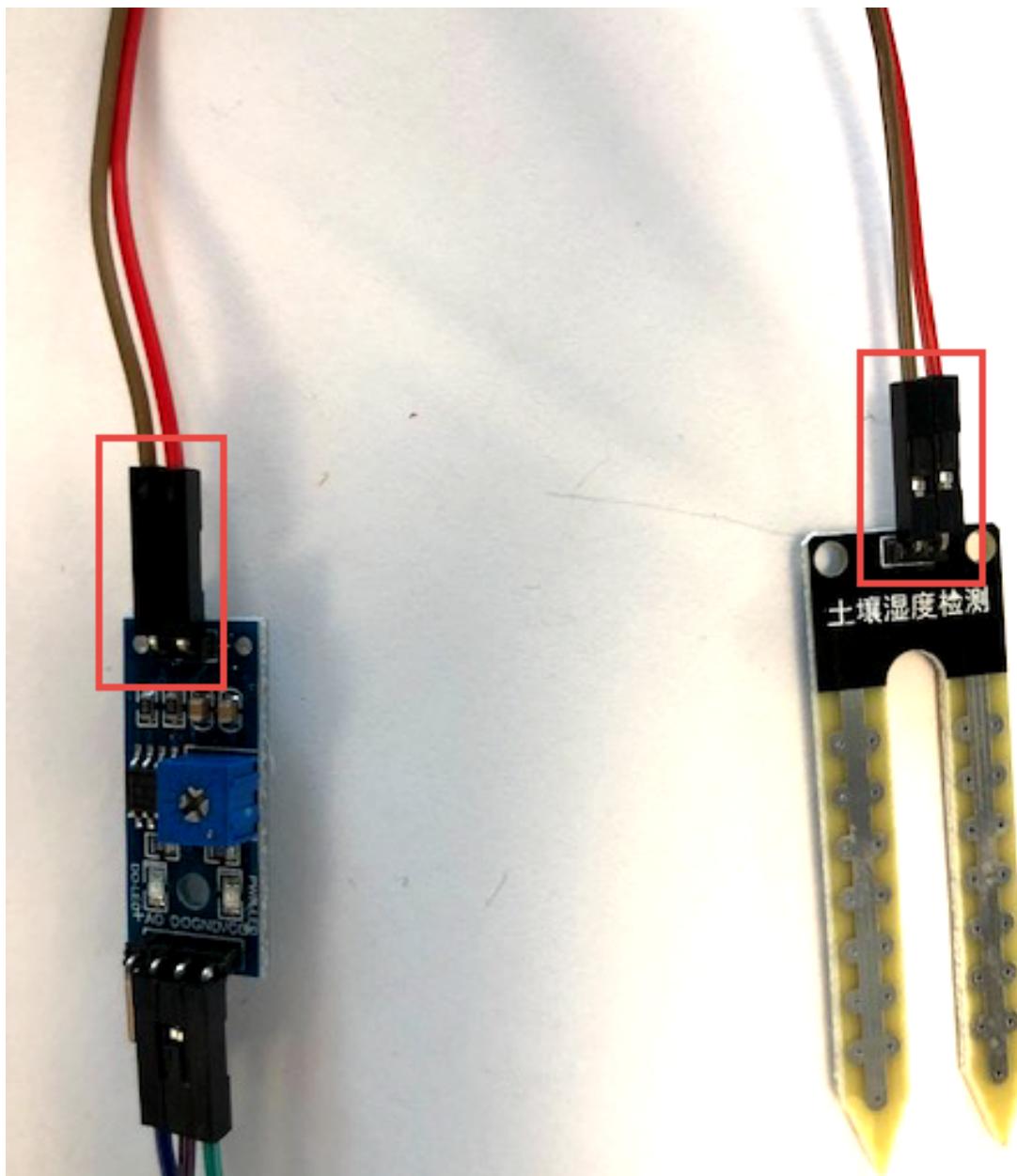
È possibile completare questa procedura anche se non si imposta una nuova password; tuttavia, impostare una nuova password aiuta a mantenere il dispositivo sicuro.

10. Scegliere Next (Avanti).
11. Nella pagina Select WiFi Network (Seleziona rete Wi-Fi), scegliere prima la rete wireless a cui connettersi, quindi Next (Avanti).
12. Nella pagina Update Software (Aggiorna software), selezionare Next (Avanti). Al termine dell'aggiornamento, scegliere OK.
13. Nella pagina Setup Complete (Configurazione completata), scegliere Reboot (Riavvia) e attendere il riavvio di Raspberry Pi.

Fase 10: Configurazione del kit di sensori dell'umidità del terreno

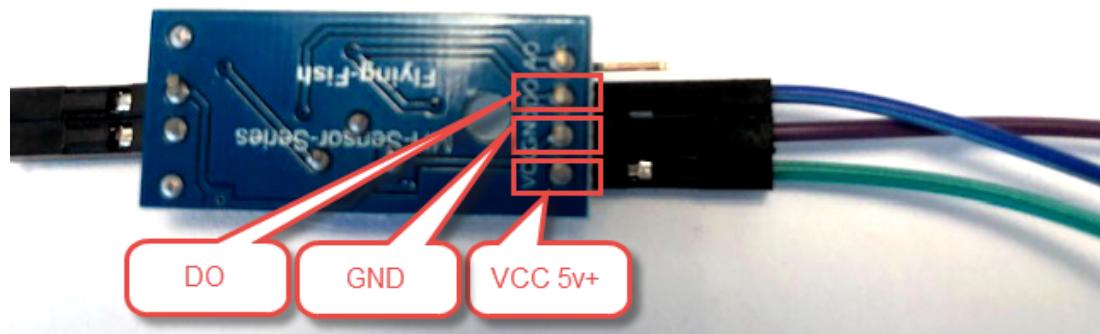
In questa fase, collegherai il kit di sensori dell'umidità del terreno al Raspberry Pi in esecuzione e lo testerai per verificare che il kit funzioni.

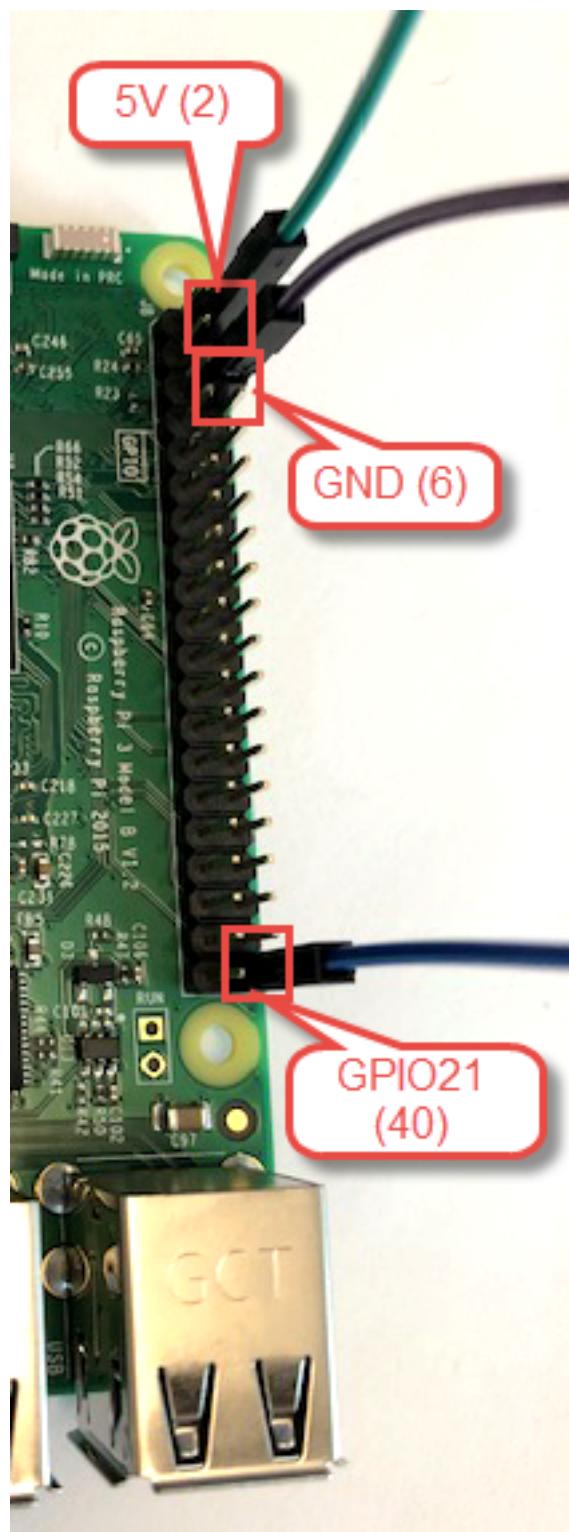
1. Collegare due cavi con connettori femmina-femmina tra i due pin del modulo di rilevamento ai due pin del microcontroller. I cavi del connettore possono essere collegati in qualsiasi ordine, ma ricordarsi di effettuare il collegamento solo con i due pin posti su un lato del microcontroller e non con uno dei quattro pin situati sull'altro lato.



2. Collegare tre cavi con connettore femmina-femmina da tre pin specifici del microcontroller a tre pin specifici del Raspberry Pi, nel modo seguente:
 1. Eseguire il collegamento dal cavo di alimentazione VCC 5 v+ del microcontroller a uno dei pin di alimentazione a 5 V sul Raspberry Pi (ad esempio, pin 2).
 2. Eseguire il collegamento dal pin GND di messa a terra del microcontroller a uno dei pin GND di messa a terra del Raspberry Pi (ad esempio, pin 6).
 3. Eseguire il collegamento dal pin digitale DO del microcontroller a uno dei pin GPIO del Raspberry Pi (ad esempio, GPIO21 su pin 40).
 4. Non collegare nulla con il pin dei dati analogici AO del microcontroller.

Per visualizzare un elenco grafico dei pin e delle rispettive etichette, è possibile eseguire il comando `pinout` sul Raspberry Pi o visitare la pagina <https://pinout.xyz>.



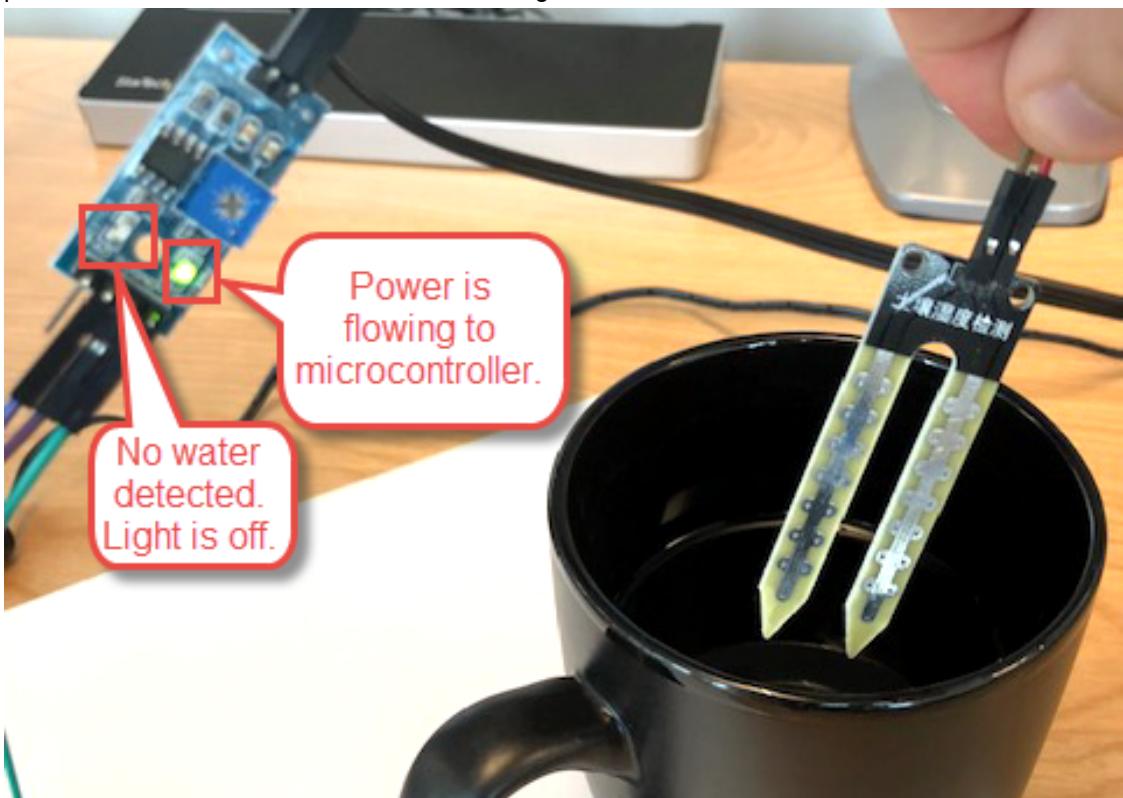


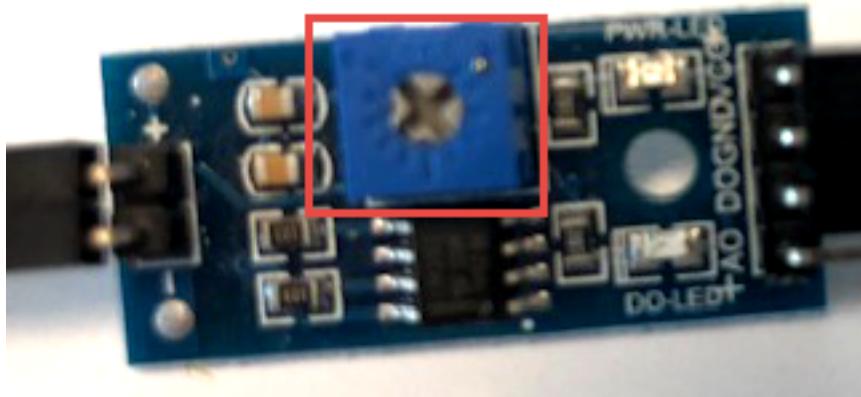
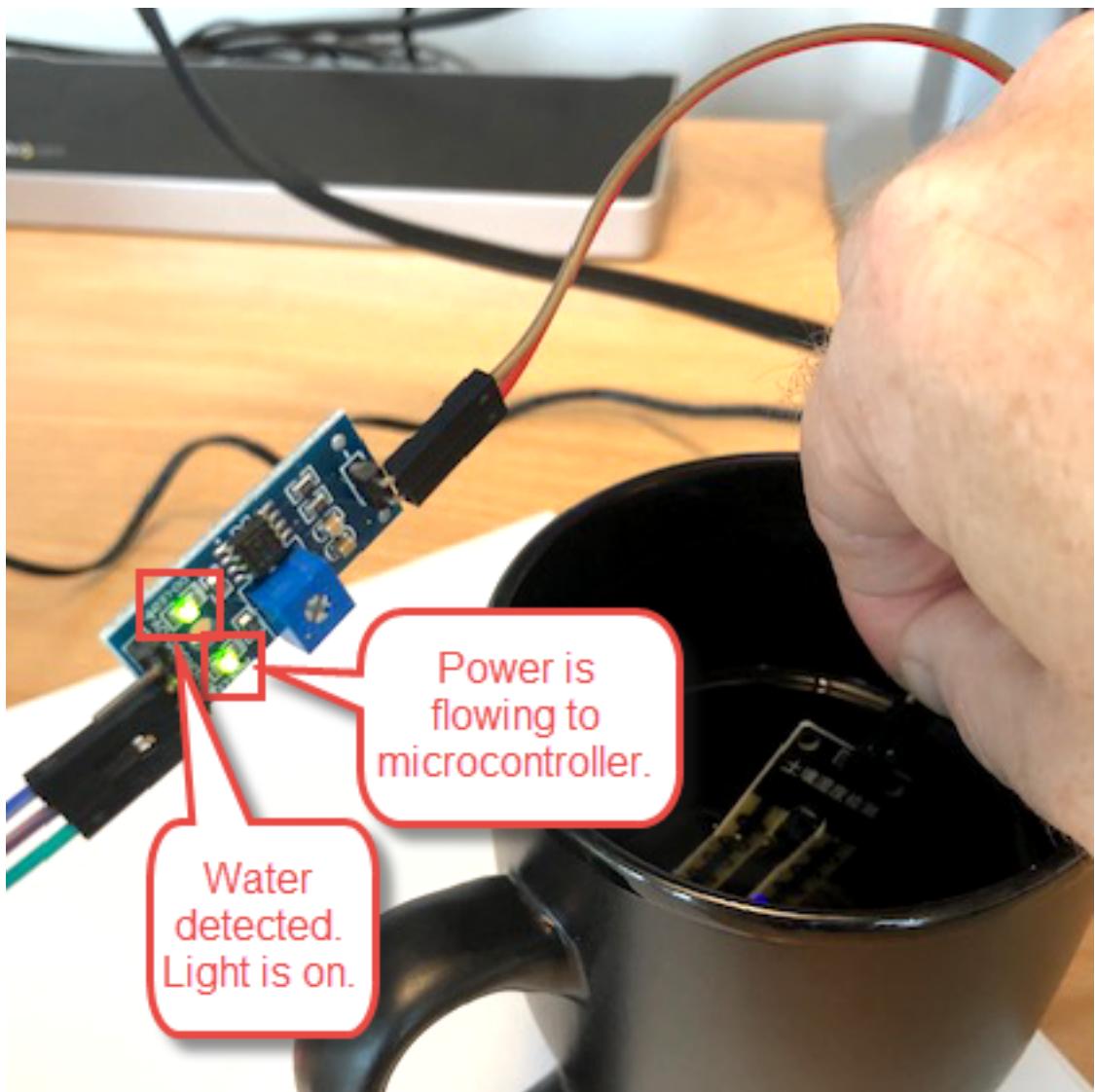
Se i collegamenti sono corretti, la luce LED di alimentazione PWR sul microcontroller è accesa.



Le luci LED di alcuni microcontroller potrebbero essere verdi, mentre quelle di altri microcontroller potrebbero essere rosse. Questi due colori hanno lo stesso significato.

3. Introdurre i connettori del modulo di rilevamento in un bicchiere d'acqua. Se il sensore rileva acqua, la luce LED dei dati digitali DO del microcontroller è accesa. Se la luce LED DO non è accesa, con i connettori ancora immersi nell'acqua, utilizzare un cacciavite a taglio per modificare la sensibilità del potenziometro del microcontroller fino a quando la luce DO non è visibile. Introdurre i connettori nell'acqua e rimuoverli per controllare se la luce DO si accende e si spegne, regolando il potenziometro del microcontroller in base alle esigenze.





Fase 11: Dati di acquisizione provenienti dal kit di sensori dell'umidità del terreno

In questa fase, utilizzerai il linguaggio di programmazione Python per eseguire sul Raspberry Pi frammenti di codice che consentono di acquisire i dati dal kit di sensori dell'umidità del terreno.

1. Utilizzare un editor di codice a propria disposizione sul Raspberry Pi (ad esempio, nano, IDLE o vi) per creare un file con il codice seguente.

```
import RPi.GPIO as GPIO
import time

# Represents the GPIO21 pin.
channel = 21

# Use the GPIO BCM pin numbering scheme.
GPIO.setmode(GPIO.BCM)

# Receive input signals through the pin.
GPIO.setup(channel, GPIO.IN)

# Infinite loop to keep this script running.
while True:
    # 'No water' = 1/True (sensor's microcontroller light is off).
    if GPIO.input(channel):
        print("No water detected")
    else:
        # 'Water' = 0/False (microcontroller light is on).
        print("Water detected!")

    # Wait 5 seconds before checking again.
    time.sleep(5)

# Clean things up if for any reason we get to this
# point before script stops.
GPIO.cleanup()
```

Ogni cinque secondi, questo codice si metterà in ascolto degli input del kit di sensori dell'umidità del terreno sul pin GPIO21 BCM (il 40° pin) del Raspberry Pi. Se la luce del microcontroller del sensore è spenta, verrà segnalato il valore 1. Se la luce è accesa, verrà segnalato il valore 0.

2. Salvare il file con estensione .py, ad esempio `gpio.py`, nella cartella `deviceSDK`. Se si decide di utilizzare un altro nome per il file .py, ricordarsi di sostituire il nome in tutto l'esempio.
3. Dal prompt dei comandi in PuTTY o SSH oppure dal terminale in Raspbian, eseguire i comandi per passare alla cartella `deviceSDK`, quindi utilizzare Python per eseguire il file `gpio.py`, ad esempio `cd /deviceSDK && python gpio.py`.
4. Ogni 5-10 secondi, introdurre i connettori del modulo di rilevamento in un bicchiere d'acqua o rimuoverli dall'acqua. Ogni 5 secondi, Python stamperà `No water detected` o `Water detected!`, a seconda che i connettori siano immersi nell'acqua o meno.
5. Al termine, interrompere l'esecuzione dello script premendo Ctrl+C.

Fase 12: Invio delle letture dei sensori dell'umidità del terreno a AWS IoT

In questa fase, utilizzerai il linguaggio di programmazione Python per eseguire sul Raspberry Pi frammenti di codice che consentono di acquisire i dati dal kit di sensori dell'umidità del terreno e inviarli a AWS IoT.

Per eseguire questa operazione, unirai una parte del codice scritto nella fase precedente con il codice scritto in `moisture.py` per [Fase 5: Simulazione di livelli di umidità casuali \(p. 129\)](#).

1. Utilizzare un editor di codice a propria disposizione sul Raspberry Pi per aprire il file `moisture.py` creato in [Fase 5: Simulazione di livelli di umidità casuali \(p. 129\)](#).
2. Aggiungere una parte del codice del file `gpio.py`, scritto precedentemente nel file `moisture.py`, e apportare alcune modifiche al codice esistente nel file `moisture.py`, come indicato tra i commenti `### BEGIN` e `### END`, nel modo seguente. Il codice finale viene riportato subito dopo il codice seguente per essere modificato.

```
from AWSIoTPythonSDK.MQTTLib import AWSIoTMQTTShadowClient
import RPi.GPIO as GPIO
import time

# A random programmatic shadow client ID.
SHADOW_CLIENT = "myShadowClient"

# The unique hostname that AWS IoT generated for
# this device.
HOST_NAME = "yourhostname-ats.iot.us-east-1.amazonaws.com"

# The relative path to the correct root CA file for AWS IoT,
# that you have already saved onto this device.
ROOT_CA = "AmazonRootCA1.pem"

# The relative path to your private key file that
# AWS IoT generated for this device, that you
# have already saved onto this device.
PRIVATE_KEY = "yourkeyid-private.pem.key"

# The relative path to your certificate file that
# AWS IoT generated for this device, that you
# have already saved onto this device.
CERT_FILE = "yourkeyid-certificate.pem.crt.txt"

# A programmatic shadow handler name prefix.
SHADOW_HANDLER = "MyRPi"

# Automatically called whenever the shadow is updated.
def myShadowUpdateCallback(payload, responseStatus, token):
    print()
    print('UPDATE: $aws/things/' + SHADOW_HANDLER +
          '/shadow/update/#')
    print("payload = " + payload)
    print("responseStatus = " + responseStatus)
    print("token = " + token)

# Create, configure, and connect a shadow client.
myShadowClient = AWSIoTMQTTShadowClient(SHADOW_CLIENT)
myShadowClient.configureEndpoint(HOST_NAME, 8883)
myShadowClient.configureCredentials(ROOT_CA, PRIVATE_KEY,
                                   CERT_FILE)
myShadowClient.configureConnectDisconnectTimeout(10)
myShadowClient.configureMQTTOperationTimeout(5)
```

```
myShadowClient.connect()

# Create a programmatic representation of the shadow.
myDeviceShadow = myShadowClient.createShadowHandlerWithName(
    SHADOW_HANDLER, True)

# Represents the GPIO21 pin on the Raspberry Pi.
channel = 21

# Use the GPIO BCM pin numbering scheme.
GPIO.setmode(GPIO.BCM)

# Receive input signals through the pin.
GPIO.setup(channel, GPIO.IN)

while True:

    if GPIO.input(channel):
        myDeviceShadow.shadowUpdate(
            '{"state":{"reported":{"moisture":"low"}}}',
            myShadowUpdateCallback, 5)
    else:
        myDeviceShadow.shadowUpdate(
            '{"state":{"reported":{"moisture":"okay"}}}',
            myShadowUpdateCallback, 5)

    # Wait for this test value to be added.
    time.sleep(60)
```

Note

Nel codice precedente, si noti che i seguenti valori non coincidono con quelli nel proprio codice:

1. *yourhostname-ats.iot.us-east-1.amazonaws.com* sarà l'endpoint dell'API REST generata da AWS IoT per l'utente.
2. *AmazonRootCA1.pem* sarà la CA root per AWS IoT.
3. *yourkeyid-private.pem.key* sarà il nome della chiave privata del dispositivo in AWS IoT.
4. *yourkeyid-certificate.pem.crt.txt* sarà il nome del file del certificato root del dispositivo in AWS IoT.
5. Il *60* in *time.sleep(60)* sarà il numero di secondi che si è disposti ad attendere prima che ciascuna nuova lettura venga generata. Più basso è questo numero, maggiore sarà la frequenza con cui si potrebbero ricevere avvisi via e-mail.
3. Salvare le proprie modifiche nel file *moisture.py*.
4. Dal prompt dei comandi in PuTTY o SSH, oppure dal terminale in Raspbian, eseguire il comando seguente per utilizzare il programma pip, che consente installare il dispositivo SDK AWS IoT per Python sul Raspberry Pi:

```
pip install AWSIoTPythonSDK
```

5. Eseguire i comandi per passare alla cartella *deviceSDK*, se non si è già in tale cartella. Quindi, utilizzare Python per eseguire il file *moisture.py*, ad esempio *cd /deviceSDK && python moisture.py*.

6. Ogni 45–60 secondi, introdurre i connettori del modulo di rilevamento in un bicchiere d'acqua o rimuoverli dall'acqua. Ogni 60 secondi, Python segnala "moisture": "low" o "moisture": "okay" a AWS IoT, a seconda che i connettori siano immersi nell'acqua o meno. Quando AWS IoT riceve una lettura di umidità bassa, attiva una regola per l'invio di un avviso all'indirizzo e-mail dell'utente tramite Amazon SNS.
7. Al termine, premere Ctrl+C per interrompere l'esecuzione dello script.
8. È ora possibile sostituire il bicchiere con una pianta d'appartamento comune. Introdurre i connettori del modulo di rilevamento nel terreno della pianta d'appartamento. Regolare il potenziometro del microcontroller del sensore per ottenere la sensibilità corretta desiderata per rilevare l'umidità del terreno.
9. Nel file `moisture.py`, modificare il 60 in `time.sleep(60)` per indicare quanti secondi intercorrono tra i vari controlli del terreno. Ad esempio, per eseguire il controllo una volta all'ora, modificare 60 in 3600. Per eseguire il controllo una volta al giorno, modificare 60 in 86400.
10. Riavviare lo script `moisture.py` eseguendo il comando `python moisture.py`.
11. Al termine di ogni intervallo per i secondi specificati in `time.sleep`, Python segnala "moisture": "low" o "moisture": "okay" a AWS IoT. Questo valore dipende dall'accensione o meno della luce DO del microcontroller del sensore, dal livello di umidità del terreno e dalla sensibilità del potenziometro impostata. Quando AWS IoT riceve una lettura di umidità bassa, attiva una regola per l'invio di un avviso all'indirizzo e-mail dell'utente tramite Amazon SNS.
12. Al termine, interrompere l'esecuzione dello script premendo Ctrl+C.

Pulizia

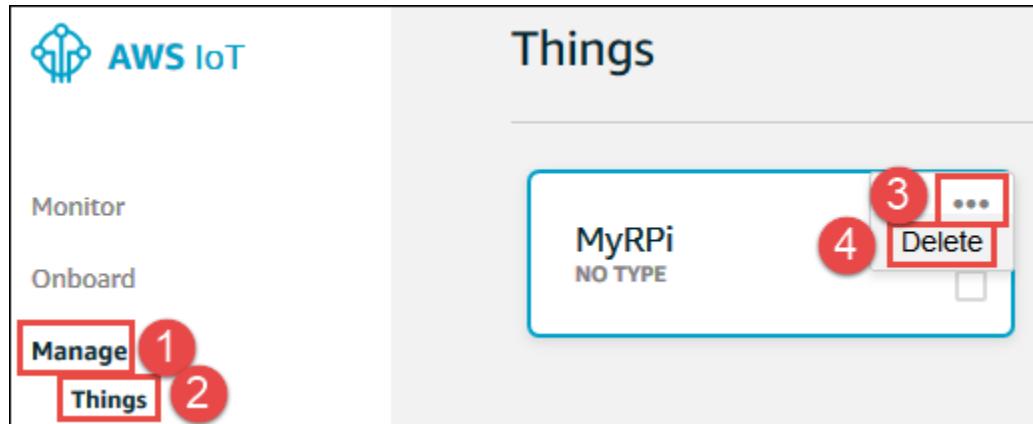
Se non si desidera più utilizzare le risorse AWS in AWS IoT, Amazon SNS e IAM create per questo codice di esempio, è possibile eliminarle seguendo le istruzioni contenute in questa sezione.

Note

Se non si eliminano tali risorse AWS, il loro utilizzo successivo potrebbe iniziare a generare addebiti per il proprio account AWS.

Per eliminare l'oggetto in AWS IoT

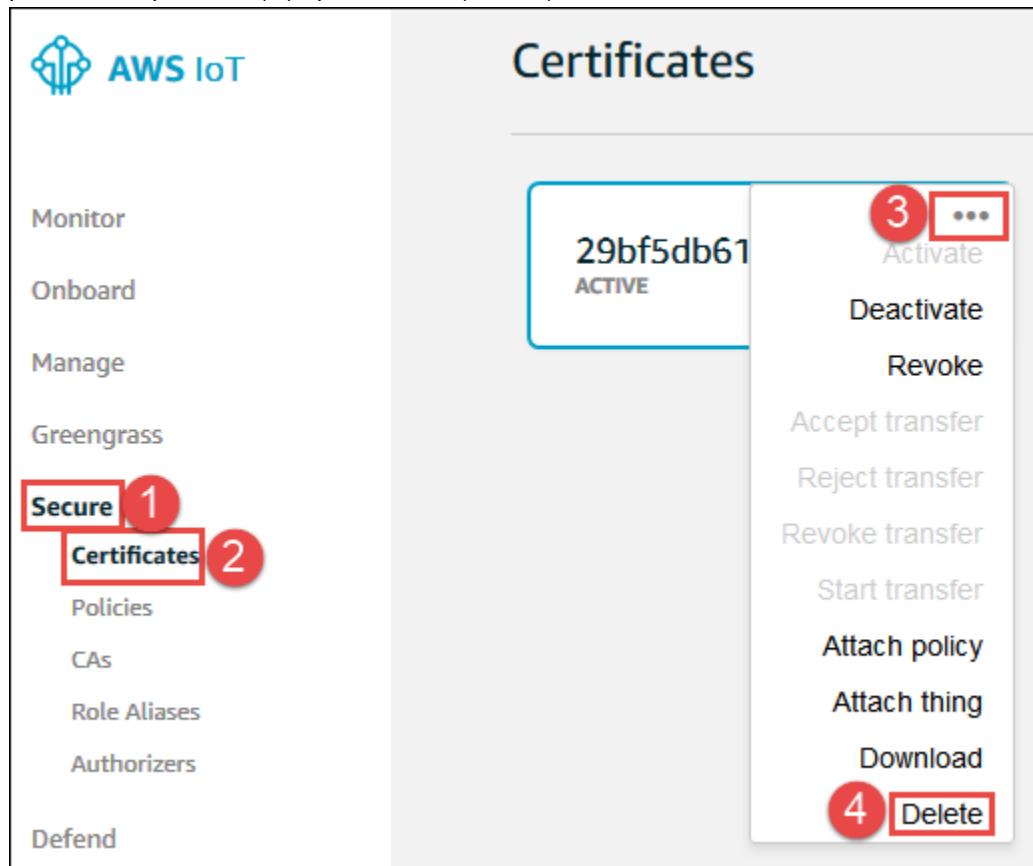
1. Nella Console di gestione AWS, aprire la [console AWS IoT](#), se non è già aperta. Per eseguire questa operazione, selezionare Services (Servizi) sulla barra di navigazione di AWS. Nella casella Find a service by name or feature (Trova un servizio per nome o caratteristica), inserire **IoT Core** e premere Enter (Invio).
2. Nel riquadro di navigazione, espandere Manage (Gestione).
3. Se la finestra di dialogo Introducing AWS IoT Device Management (Presentazione della gestione dei dispositivi IoT) è visibile, selezionare Show me later (Mostra più tardi), oppure premere Esc.
4. Scegliere Things (Oggetti).
5. Nell'elenco di oggetti, nella scheda corrispondente al nome dell'oggetto da eliminare (ad esempio, MyRPi), scegliere prima i puntini di sospensione (...), quindi Delete (Elimina).



6. Alla richiesta di conferma, scegliere Yes, continue with delete (Si, procedi all'eliminazione).

Per eliminare il certificato dell'oggetto in AWS IoT

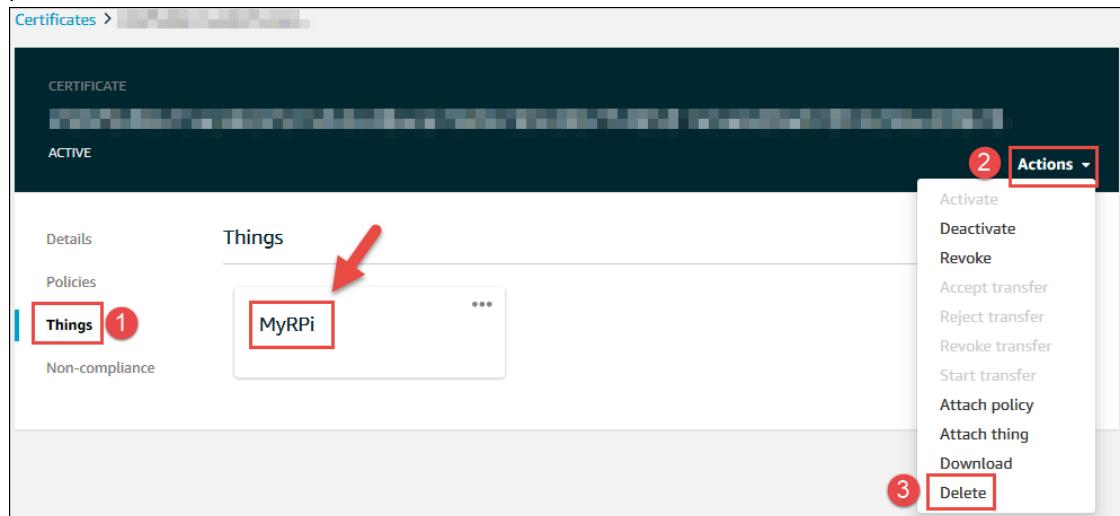
1. Nella [console AWS IoT](#), nel riquadro di navigazione del servizio, espandere Secure (Sicurezza), quindi scegliere Certificates (Certificati).
2. Nell'elenco dei certificati, nella scheda corrispondente al certificato dell'oggetto, scegliere prima i puntini di sospensione (...), quindi Delete (Elimina).



Se non si è certi del certificato da eliminare, nell'elenco dei certificati scegliere l'ID del certificato che si ritiene corretto. Quindi, scegliere Things (Oggetti).

Se viene visualizzato il nome dell'oggetto, quello selezionato è il certificato corretto da eliminare. Scegliere prima Actions (Operazioni), quindi Delete (Elimina).

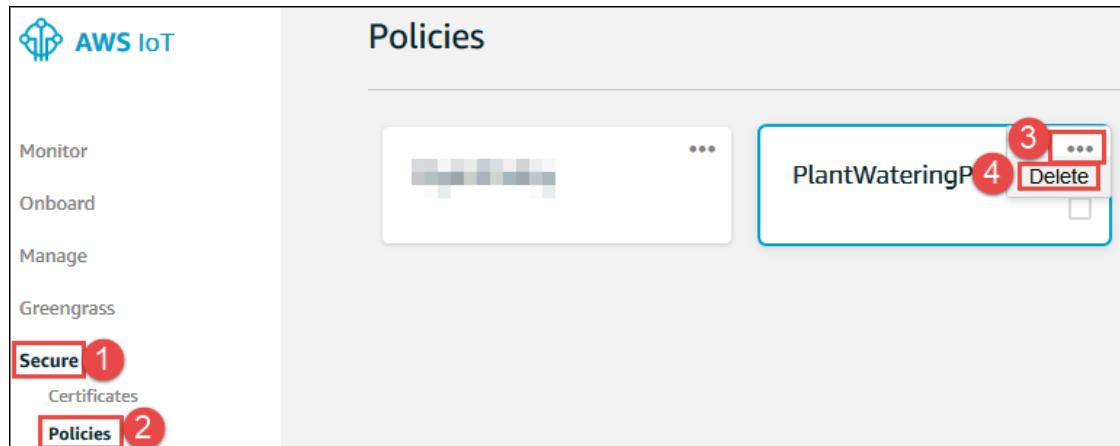
Se l'oggetto non è visibile, quello selezionato non è il certificato corretto. Scegliere il pulsante Indietro per tornare alla lista di certificati.



3. Alla richiesta di conferma, scegliere Yes, continue with delete (Sì, procedi all'eliminazione).

Per eliminare la policy dell'oggetto in AWS IoT

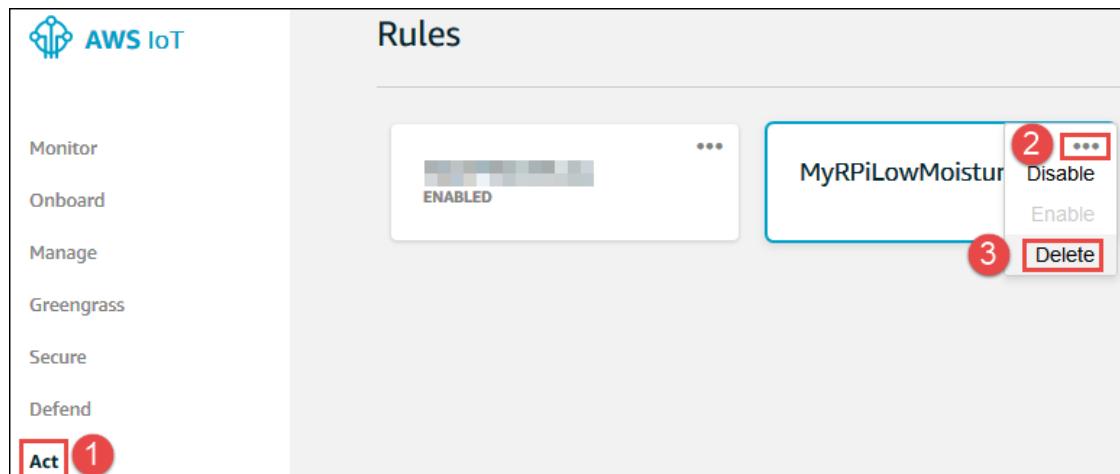
1. Nella [console AWS IoT](#), nel riquadro di navigazione del servizio, espandere Secure (Sicurezza), quindi scegliere Policies (Policy).
2. Nell'elenco delle politiche, nella scheda corrispondente alla policy dell'oggetto (ad esempio, PlantWateringPolicy), scegliere prima i punti di sospensione (...), quindi Delete (Elimina).



3. Alla richiesta di conferma, scegliere Yes, continue with delete (Sì, procedi all'eliminazione).

Per eliminare la regola dell'oggetto in AWS IoT

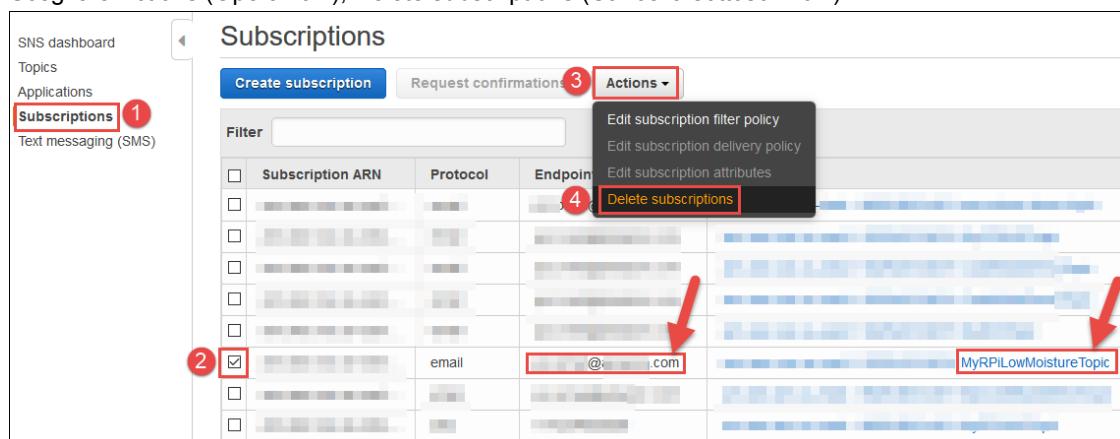
1. Nella [console AWS IoT](#), nel riquadro di navigazione del servizio, scegliere Act (Esecuzione azioni).
2. Nell'elenco delle regole, nella scheda corrispondente alla regola dell'oggetto (ad esempio, MyRPiLowMoistureAlertRule), scegliere prima i punti di sospensione (...), quindi Delete (Elimina).



3. Alla richiesta di conferma, scegliere Yes, continue with delete (Sì, procedi all'eliminazione).

Per eliminare la sottoscrizione corrispondente in Amazon SNS

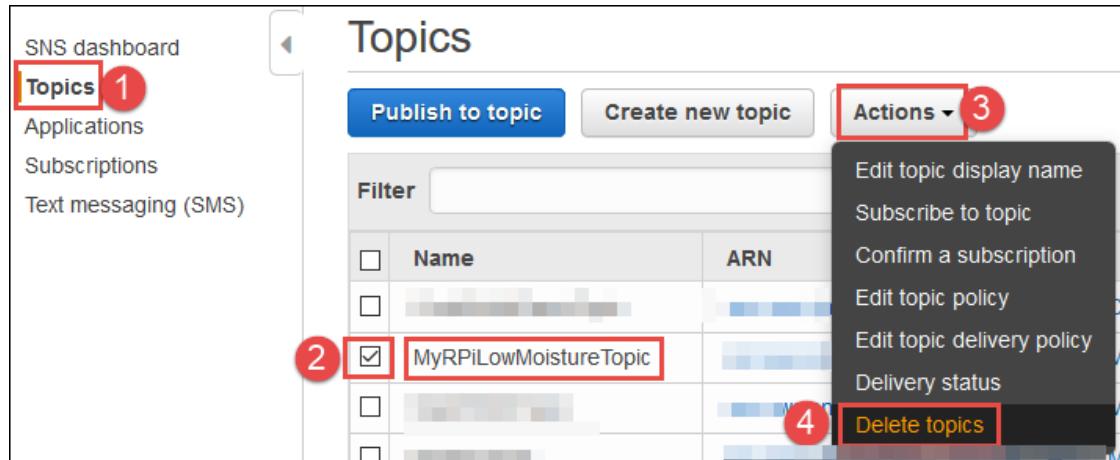
1. Aprire la console Amazon SNS. Per eseguire questa operazione, selezionare Services (Servizi) sulla barra di navigazione di AWS. Nella casella Find a service by name or feature (Trova un servizio per nome o caratteristica), inserire **SNS** e premere Enter (Invio).
2. Nel riquadro di navigazione, selezionare Subscriptions (Sottoscrizioni).
3. Nell'elenco delle sottoscrizioni, selezionare la casella per la riga in cui Topic ARN (Argomento ARN) contiene il nome dell'argomento correlato (ad esempio, MyRPiLowMoistureTopic) ed Endpoint contiene il proprio indirizzo e-mail.
4. Scegliere Actions (Operazioni), Delete subscriptions (Cancella sottoscrizioni).



5. Quando viene richiesto, scegliere Delete (Elimina).

Per eliminare l'argomento corrispondente in Amazon SNS

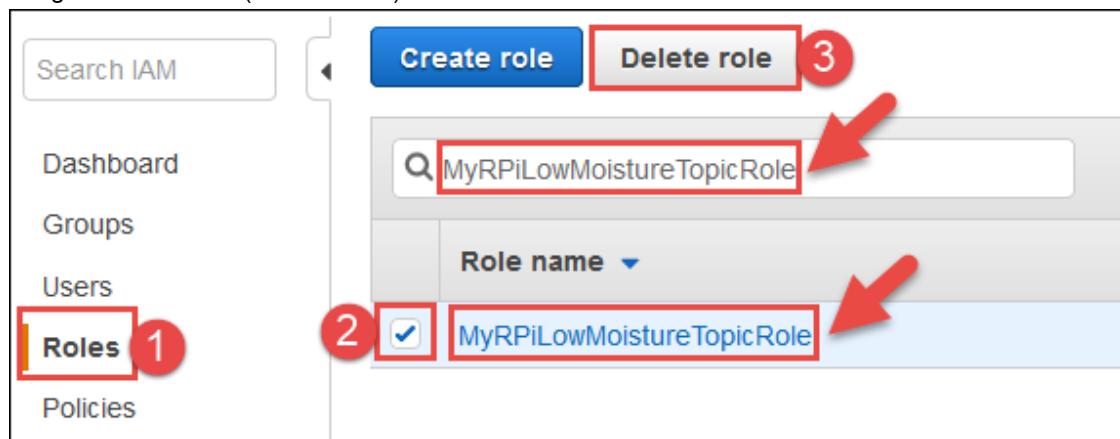
1. Nella console Amazon SNS, nel riquadro di navigazione, scegliere Topics (Argomenti).
2. Nell'elenco di argomenti, selezionare la casella della riga in cui Name (Nome) contiene il nome dell'argomento correlato (ad esempio, MyRPiLowMoistureTopic).
3. Scegliere Actions (Operazioni), Delete topics (Elimina argomenti).



- Quando viene richiesto, scegliere Delete (Elimina).

Per eliminare il ruolo Amazon SNS correlato in IAM

- Aprire la console IAM. Per eseguire questa operazione, selezionare Services (Servizi) sulla barra di navigazione di AWS. Nella casella Find a service by name or feature (Trova un servizio per nome o caratteristica), inserire IAM e premere Enter (Invio).
- Nel riquadro di navigazione di servizio, selezionare Roles (Ruoli).
- Nell'elenco di ruoli, selezionare la casella in cui Role name (Nome ruolo) contiene il nome del ruolo correlato (ad esempio, MyRPiLowMoistureTopicRole). Se non è possibile trovare il ruolo, nella casella Search (Cerca), inserire il nome del ruolo. Quindi, premere Enter (Invio).
- Scegliere Delete role (Elimina ruolo).



- Quando viene richiesto, scegliere Yes, delete (Sì, elimina).

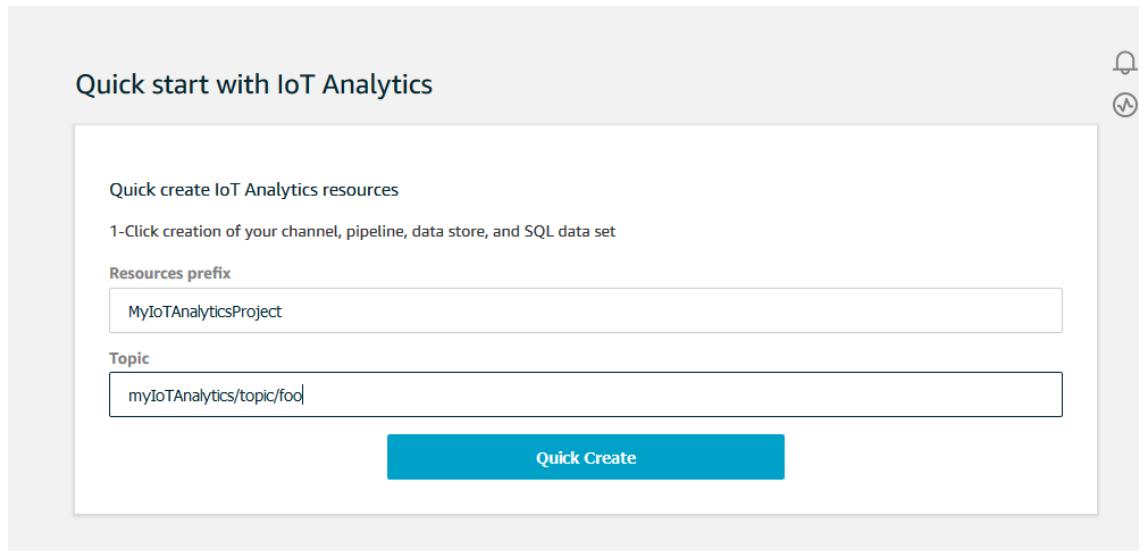
Fasi successive

Ulteriori informazioni su come utilizzare AWS IoT. Consulta le seguenti risorse.

- [Guida per lo sviluppatore di AWS IoT](#) - Ulteriori informazioni sui concetti in questa procedura guidata di esempio, incluso il modo per lavorare maggiormente con oggetti, regole e shadow. Ulteriori informazioni su tipi di oggetti, gruppi di oggetti, processi e servizi come AWS IoT Device Defender.

2. [AWS IoT Greengrass Developer Guide](#) - Scopri come AWS IoT Greengrass consente di eseguire in modo sicuro le funzionalità locali di calcolo, messaggistica, caching dei dati, sincronizzazione e inferenza del linguaggio macchina per i dispositivi connessi.
3. [AWS IoT Analytics User Guide](#) - Scopri come AWS IoT Analytics, un servizio completamente gestito, semplifica l'esecuzione e l'operatività di analisi sofisticate su enormi volumi di dati IoT. Con AWS IoT Analytics non dovrà preoccuparti dei costi e della complessità generalmente impliciti nella distribuzione di una piattaforma di analisi IoT.

La console AWS IoT Analytics offre anche una funzione Quick Start che consente di creare un canale, i dati archiviati, pipeline e data store con un solo clic. Cerca questa pagina quando inserisci la console di AWS IoT Analytics:



4. [AWS IoT 1-Click Developer Guide](#) - Scopri come utilizzare AWS IoT 1-Click, un servizio che consente a dispositivi semplici di attivare funzioni [AWS Lambda](#) per eseguire azioni.
5. [Amazon FreeRTOS User Guide](#) - Scopri come utilizzare Amazon FreeRTOS, un sistema operativo per microcontroller che rende semplice programmare, distribuire, proteggere, collegare e gestire dispositivi edge di piccole dimensioni e a basso consumo.
6. [AWS IoT Events Developer Guide](#) - Scopri come utilizzare AWS IoT Events per monitorare le apparecchiature e i parchi di dispositivi e individuare errori o modifiche di funzionamento e per attivare le relative operazioni quando tali eventi si verificano.

Gestione di dispositivi con AWS IoT

AWS IoT fornisce un registro che semplifica la gestione degli oggetti. Un oggetto è una rappresentazione di un'entità logica o un dispositivo specifico. Può trattarsi di un dispositivo fisico o un sensore, ad esempio una lampadina o un interruttore su un muro. Può anche trattarsi di un'entità logica, ad esempio un'istanza di un'applicazione, o un'entità fisica che non si connette ad AWS IoT ma che è correlata ad altri dispositivi che si connettono, ad esempio un'auto con sensori per il motore o un pannello di controllo.

Le informazioni su un oggetto vengono archiviate nel registro come dati JSON. Di seguito è illustrato un esempio di oggetto:

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

Gli oggetti sono identificati da un nome. Gli oggetti possono anche avere attributi, che sono coppie nome–valore che è possibile usare per archiviare le informazioni sull'oggetto, ad esempio il numero di serie o il produttore.

Un tipico caso d'uso di un dispositivo prevede l'uso del nome dell'oggetto come ID client MQTT predefinito. Anche se non viene imposta una mappatura tra un nome di un oggetto nel registro e l'uso di ID client MQTT, certificati o stato della copia shadow, è consigliabile scegliere un nome di oggetto e usarlo come ID client MQTT sia per il registro che per il servizio Device Shadows. In questo modo, puoi ottenere organizzazione e comodità per il parco istanze IoT senza rinunciare alla flessibilità del modello di certificati dei dispositivi sottostante o delle copie shadow.

Non è necessario creare un oggetto nel registro per connettere un dispositivo ad AWS IoT. L'aggiunta di oggetti al registro permette di semplificare le attività di gestione e ricerca di dispositivi.

Come gestire gli oggetti con il registro

Per interagire con il registro, è possibile usare la console AWS IoT o l'interfaccia a riga di comando (CLI) di AWS. Nelle seguenti sezioni viene illustrato come usare l'interfaccia a riga di comando per lavorare con il registro.

Creare un oggetto

Di seguito viene illustrato come usare il comando AWS IoT di CreateThing dall'interfaccia a riga di comando per creare un oggetto:

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

Il comando CreateThing permette di visualizzare il nome e l'ARN del nuovo oggetto:

```
{
```

```
    "thingArn": "arn:aws:iot:us-east-1:123456789012:thing/MyLightBulb",
    "thingName": "MyLightBulb"
    "thingId": "12345678abcdefghijklmnopqrstuvwxyz"
}
```

Note

Non è consigliabile utilizzare informazioni di identificazione personale nei nomi degli oggetti.

Elenco di oggetti

Usa il comando ListThings per elencare tutti gli oggetti nell'account:

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

Ricerca di oggetti

Usa il comando DescribeThing per elencare le informazioni su un oggetto:

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

Usa il comando ListThings per cercare tutti gli oggetti associati a un nome di tipo di oggetto:

```
$ aws iot list-things --thing-type-name "LightBulb"
```

```
{
```

```
"things": [
  {
    "thingType": "LightBulb",
    "version": 1,
    "thingName": "MyRGBLight"
  },
  {
    "thingType": "LightBulb",
    "version": 1,
    "thingName": "MySecondLightBulb"
  }
]
```

Usa il comando ListThings per cercare tutti gli oggetti che hanno un attributo con un valore specifico:

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

```
{
  "things": [
    {
      "thingType": "StopLight",
      "version": 3,
      "thingName": "MyLightBulb"
    },
    {
      "thingType": "LightBulb",
      "version": 1,
      "thingName": "MyRGBLight"
    },
    {
      "thingType": "LightBulb",
      "version": 1,
      "thingName": "MySecondLightBulb"
    }
  ]
}
```

Aggiornamento di un oggetto

Usa il comando UpdateThing per aggiornare un oggetto:

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

Il comando UpdateThing non produce output. Usa il comando DescribeThing per visualizzare il risultato:

```
$ aws iot describe-thing --thing-name "MyLightBulb"
{
    "attributes": {
        "model": "456",
        "wattage": "150"
    },
    "version": 2,
    "thingName": "MyLightBulb"
}
```

Eliminazione di un oggetto

Usa il comando DeleteThing per eliminare un oggetto:

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

Questo comando ha esito positivo senza alcun errore se l'eliminazione va a buon fine oppure se specifichi un oggetto che non esiste.

Collegamento di un principale a un oggetto

Un dispositivo fisico deve disporre di un certificato X.509 per comunicare con AWS IoT. È possibile associare il certificato nel dispositivo con l'oggetto nel registro che rappresenta il dispositivo. Per collegare un certificato all'oggetto, usa il comando AttachThingPrincipal:

```
$ aws iot attach-thing-principal --thing-name "MyLightBulb" --principal "arn:aws:iot:us-east-1:123456789012:cert/a0c01f5835079de0a7514643d68ef8414ab739a1e94ee4162977b02b12842847"
```

Il comando AttachThingPrincipal non produce output.

Scollegamento di un principale da un oggetto

Usa il comando DetachThingPrincipal per scollegare un certificato da un oggetto:

```
$ aws iot detach-thing-principal --thing-name "MyLightBulb" --principal "arn:aws:iot:us-east-1:123456789012:cert/a0c01f5835079de0a7514643d68ef8414ab739a1e94ee4162977b02b12842847"
```

Il comando DetachThingPrincipal non produce output.

Tipi di oggetti

I tipi di oggetti permettono di archiviare la descrizione e le informazioni di configurazione comuni a tutti gli oggetti associati allo stesso tipo. Ciò semplifica la gestione degli oggetti nel registro. Puoi ad esempio definire un tipo di oggetto LightBulb, ovvero lampadina. Tutti gli oggetti associati al tipo LightBulb condividono un set di attributi: numero di serie, produttore e potenza in watt. Quando crei un oggetto di tipo LightBulb (o modifichi il tipo di un oggetto esistente in LightBulb), puoi specificare i valori per ognuno degli attributi definiti nel tipo di oggetto LightBulb.

Anche se i tipi di oggetti sono facoltativi, il loro uso permette una migliore individuazione degli oggetti.

- Gli oggetti con un tipo possono avere fino a 50 attributi.
- Gli oggetti senza un tipo possono avere fino a tre attributi.
- Un oggetto può essere associato a un solo tipo.
- Non vi è alcun limite al numero di tipi di oggetti che è possibile creare nell'account.

I tipi di oggetti non sono modificabili. Non è possibile modificare il nome di un tipo di oggetto dopo averlo creato. È possibile dichiarare obsoleto un tipo di oggetto in qualsiasi momento per impedire che vi vengano associati nuovi oggetti. È inoltre possibile eliminare i tipi di oggetti a cui non sono associati oggetti.

Creazione di un tipo di oggetto

Usa il comando `CreateThingType` per creare un tipo di oggetto:

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

Il comando `CreateThingType` restituisce una risposta che contiene il tipo di oggetto e il relativo ARN:

```
{  
    "thingTypeName": "LightBulb",  
    "thingTypeId": "df9c2d8c-894d-46a9-8192-9068d01b2886",  
    "thingTypeArn": "arn:aws:iot:us-west-2:123456789012:thingtype/LightBulb"  
}
```

Elenco di tipi di oggetti

Usa il comando `ListThingTypes` per elencare i tipi di oggetti:

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

Il comando `ListThingTypes` restituisce un elenco dei tipi di oggetti definiti nell'account AWS:

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

Descrizione di un tipo di oggetto

Usa il comando `DescribeThingType` per ottenere informazioni su un tipo di oggetto:

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

Il comando `DescribeThingType` restituisce le informazioni relative al tipo specificato:

```
{  
    "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  
    }  
}
```

Associazione di un tipo di oggetto a un oggetto

Usa il comando `CreateThing` per specificare un tipo di oggetto durante la creazione di un oggetto:

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

Usa il comando `UpdateThing` in qualsiasi momento per modificare il tipo di oggetto associato a un oggetto:

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

Puoi anche usare il comando `UpdateThing` per eliminare l'associazione di un oggetto a un tipo.

Impostazione di un tipo di oggetto come obsoleto

I tipi di oggetti non sono modificabili. Dopo essere stati definiti, non possono essere modificati. È possibile tuttavia dichiarare obsoleto un tipo di oggetto per impedire agli utenti di associarvi nuovi oggetti. Tutti gli oggetti esistenti associati al tipo di oggetto non vengono modificati.

Per dichiarare obsoleto un tipo di oggetto, usa il comando `DeprecateThingType`:

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

Usa il comando `DescribeThingType` per visualizzare il risultato:

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

```
{  
    "thingTypeName": "StopLight",  
    "thingTypeProperties": {  
        "searchableAttributes": [  
            "wattage",  
            "model"  
        ]  
    }  
}
```

```
        "numOfLights",
        "model"
    ],
    "thingTypeDescription": "traffic light type",
},
"thingTypeMetadata": {
    "deprecated": true,
    "creationDate": 1468425854308,
    "deprecationDate": 1468446026349
}
}
```

La dichiarazione di un tipo di oggetto come obsoleto è un'operazione reversibile. È possibile annullare la dichiarazione di un tipo come obsoleto usando il flag `--undo-deprecate` con il comando `DeprecateThingType` dell'interfaccia a riga di comando:

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

Usa il comando `DescribeThingType` dell'interfaccia a riga di comando per visualizzare il risultato:

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

```
{
    "thingTypeName": "StopLight",
    "thingTypeArn": "arn:aws:iot:us-east-1:123456789012:thingtype/StopLight",
    "thingTypeId": "12345678abcdefhijklmnop12345678"
    "thingTypeProperties": {
        "searchableAttributes": [
            "wattage",
            "numOfLights",
            "model"
        ],
        "thingTypeDescription": "traffic light type"
    },
    "thingTypeMetadata": {
        "deprecated": false,
        "creationDate": 1468425854308,
    }
}
```

Eliminazione di un tipo di oggetto

È possibile eliminare i tipi di oggetti solo dopo averli dichiarati obsoleti. Per eliminare un tipo di oggetto, usa il comando `DeleteThingType`:

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

Note

Dopo aver dichiarato obsoleto un tipo di oggetto, è necessario attendere cinque minuti prima di eliminarlo.

Gruppi di oggetti

La classificazione degli oggetti in gruppi consente di gestire diversi oggetti contemporaneamente. I gruppi possono contenere anche altri gruppi — puoi creare una gerarchia di gruppi. È possibile collegare una

policy a un gruppo padre affinché venga ereditata dai gruppi figlio, oltre che da tutti gli oggetti nel gruppo e nei relativi gruppi figlio. In questo modo, si semplifica il controllo delle autorizzazioni per un numero elevato di oggetti.

Di seguito sono elencate le operazioni che è possibile eseguire con i gruppi di oggetti:

- Creare, descrivere o eliminare un gruppo.
- Aggiungere un oggetto a un gruppo o a più gruppi.
- Rimuovere un oggetto da un gruppo.
- Elencare i gruppi creati.
- Elencare tutti i gruppi figlio di un gruppo (i relativi discendenti diretti e indiretti).
- Elencare gli oggetti in un gruppo, inclusi tutti gli oggetti nei relativi gruppi figlio.
- Elencare tutti i gruppi predecessore di un gruppo (i relativi oggetti padre diretti e indiretti).
- Aggiungere, eliminare o aggiornare gli attributi di un gruppo. Gli attributi sono coppie nome–valore che è possibile usare per archiviare le informazioni su un gruppo.
- Collegare o scollegare una policy a o da un gruppo.
- Elencare le policy collegate a un gruppo.
- Elencare le policy ereditate da un oggetto (in forza delle policy collegate al relativo gruppo o a uno dei gruppi padre).
- Configurare le opzioni di logging per gli oggetti in un gruppo. Consulta ([Configurazione del logging di AWS IoT \(p. 657\)](#)).
- Creare processi che verranno inviati ed eseguiti su ogni oggetto in un gruppo e nei relativi gruppi figlio. Consulta ([Processi \(p. 368\)](#)).

Di seguito sono elencate alcune limitazioni dei gruppi di oggetti:

- Un gruppo può avere un solo elemento padre diretto.
- Se un gruppo sarà figlio di un altro gruppo, ciò deve essere specificato al momento della creazione.
- Non è possibile modificare il padre di un gruppo in un secondo momento. Assicurati quindi di pianificare la gerarchia dei gruppi e creare un gruppo padre prima di creare i gruppi figlio che conterrà.
- Non è possibile aggiungere un oggetto a più di 10 gruppi.
- Non è possibile aggiungere un oggetto a più di un gruppo nella stessa gerarchia. In altre parole, non è possibile aggiungere un oggetto a due gruppi che condividono un padre.
- Non è possibile rinominare un gruppo.
- I nomi dei gruppi di oggetti non possono contenere caratteri internazionali, ad esempio, û, é e ñ.

Le operazioni di collegamento e scollegamento di policy ai e dai gruppi possono migliorare notevolmente la sicurezza delle operazioni di AWS IoT in diversi modi. Il metodo per dispositivo di collegamento di una policy a un certificato, che viene quindi collegato a un oggetto, richiede molto tempo e rende difficile aggiornare rapidamente le policy o modificarle in un parco istanze di dispositivi. Se si collega una policy al gruppo di oggetti, sono necessarie meno operazioni quando è il momento di ruotare i certificati di un oggetto. Le policy vengono inoltre applicate dinamicamente agli oggetti quando cambia l'appartenenza ai gruppi, quindi non è necessario ricreare un set di autorizzazioni complesso ogni volta che per un dispositivo cambia l'appartenenza a un gruppo.

Creazione di un gruppo di oggetti

Usa il comando `CreateThingGroup` per creare un gruppo di oggetti:

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

Il comando CreateThingGroup restituisce una risposta che contiene il gruppo di oggetti e i relativi ID e ARN:

```
{  
    "thingGroupName": "LightBulbs",  
    "thingGroupId": "abcdefghijklmnopqrstuvwxyz12345678ijklmnop12345678qrstuvwxyz",  
    "thingGroupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/LightBulbs"  
}
```

Note

Non è consigliabile utilizzare informazioni di identificazione personale nei nomi dei gruppi di oggetti.

Di seguito è illustrato un esempio in cui viene specificato un elemento padre del gruppo di oggetti al momento della creazione:

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

Come in precedenza, il comando CreateThingGroup restituisce una risposta che contiene il gruppo di oggetti e i relativi ID e ARN:

```
{  
    "thingGroupName": "RedLights",  
    "thingGroupId": "abcdefghijklmnopqrstuvwxyz12345678ijklmnop12345678qrstuvwxyz",  
    "thingGroupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/RedLights",  
}
```

Important

Quando crei gerarchie di gruppi, tieni presenti i limiti seguenti:

- Un gruppo può avere un solo elemento padre diretto.
- Un gruppo non può avere più di 100 gruppi figlio diretti.
- La profondità massima di una gerarchia di gruppi è pari a 7.
- Un gruppo può avere fino a 50 attributi. Gli attributi sono coppie nome–valore che è possibile usare per archiviare le informazioni su un gruppo. Ogni nome di attributo può essere composto da un massimo di 128 caratteri e ogni valore da un massimo di 800 caratteri.

Descrizione di un gruppo di oggetti

Usa il comando DescribeThingGroup per ottenere informazioni su un gruppo di oggetti:

```
$ aws iot describe-thing-group --thing-group-name RedLights
```

Il comando DescribeThingGroup restituisce le informazioni relative al gruppo specificato:

```
{  
    "thingGroupName": "RedLights",  
    "thingGroupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/RedLights",  
    "thingGroupId": "12345678abcdefghijklmnopqrstuvwxyz12345678ijklmnop12345678",  
    "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"  
    },  
},  
}  
}
```

Aggiunta di un oggetto a un gruppo di oggetti

Usa il comando AddThingToThingGroup per aggiungere un oggetto a un gruppo:

```
$ aws iot add-thing-to-thing-group --thing-name MyLightBulb --thing-group-name RedLights
```

Il comando AddThingToThingGroup non produce output.

Important

È possibile aggiungere un oggetto a un massimo di 10 gruppi. Non è tuttavia possibile aggiungere un oggetto a più di un gruppo nella stessa gerarchia. In altre parole, non è possibile aggiungere un oggetto a due gruppi che condividono un padre.

Se un oggetto appartiene a 10 gruppi di oggetti e almeno uno di questi gruppi è un gruppo di oggetti dinamico, è possibile utilizzare il flag `overrideDynamicGroups` per far sì che i gruppi statici abbiano la priorità sui gruppi dinamici.

Rimozione di un oggetto da un gruppo di oggetti.

Usa il comando RemoveThingFromThingGroup per rimuovere un oggetto da un gruppo:

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

Il comando RemoveThingFromThingGroup non produce output.

Elenco di oggetti in un gruppo di oggetti

Utilizza il comando ListThingsInThingGroup per elencare gli oggetti che appartengono a un gruppo:

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

Il comando ListThingsInThingGroup restituisce un elenco degli oggetti nel gruppo specificato:

```
{  
    "things": [  
]
```

```
        "TestThingA"  
    ]  
}
```

Il parametro `--recursive` permette di elencare gli oggetti appartenenti a un gruppo oltre a quelli nei relativi gruppi figlio:

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

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

Note

Questa operazione è [consistente finale](#). In altre parole, le modifiche al gruppo di oggetti possono non essere visualizzate immediatamente.

Elenco di gruppi di oggetti

Usa il comando `ListThingGroups` per elencare i gruppi creati:

```
$ aws iot list-thing-groups
```

Il comando `ListThingGroups` restituisce un elenco dei gruppi definiti nell'account AWS:

```
{  
    "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"  
        }  
    ]  
}
```

Usa i filtri facoltativi per elencare i gruppi con un determinato gruppo padre (`--parent-group`) o i gruppi il cui nome inizia con un determinato prefisso (`--name-prefix-filter`). Il parametro `--recursive` permette di elencare anche tutti i gruppi figlio e non solo i gruppi figlio diretti di un gruppo di oggetti:

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

In questo caso, il comando ListThingGroups restituisce un elenco dei gruppi figlio diretti del gruppo di oggetti definito nell'account AWS:

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

Utilizza il parametro **--recursive** con il comando ListThingGroups per elencare tutti i gruppi figlio di un gruppo di oggetti, non solo i figli diretti:

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

Il comando ListThingGroups restituisce un elenco di tutti i gruppi figlio del gruppo di oggetti:

```
{  
    "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

Questa operazione è **consistente finale**. In altre parole, le modifiche al gruppo di oggetti possono non essere visualizzate immediatamente.

Elenco dei gruppi per un oggetto

Usa il comando ListThingGroupsForThing per elencare i gruppi a cui un oggetto appartiene, inclusi i gruppi padre:

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

Il comando ListThingGroupsForThing restituisce un elenco dei gruppi di oggetti a cui l'oggetto appartiene, inclusi i gruppi padre:

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

```
{  
    "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"  
}  
]  
}
```

Aggiornamento di un gruppo di oggetti

Usa il comando `UpdateThingGroup` per aggiornare gli attributi di un gruppo di oggetti:

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

Il comando `UpdateThingGroup` restituisce una risposta che contiene il numero di versione del gruppo dopo l'aggiornamento:

```
{  
    "version": 4  
}
```

Note

Un gruppo può avere fino a 50 attributi.

Eliminazione di un gruppo di oggetti

Per eliminare un gruppo di oggetti, usa il comando `DeleteThingGroup`:

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

Il comando `DeleteThingGroup` non produce output.

Important

Se tenti di eliminare un gruppo di oggetti con gruppi di oggetti figlio, viene generato un errore:

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

È necessario eliminare i gruppi figlio prima di eliminare il gruppo.

È possibile eliminare un gruppo con oggetti figlio, ma le autorizzazioni concesse agli oggetti in virtù dell'appartenenza al gruppo non sono più valide. Prima di eliminare un gruppo a cui è collegata una policy, controlla attentamente che la rimozione delle autorizzazioni non comprometta il corretto funzionamento

degli oggetti nel gruppo. Tieni inoltre presente che i comandi che mostrano i gruppi a cui un oggetto appartiene (ad esempio, `ListGroupsForThing`) potrebbero continuare a segnalare il gruppo mentre i record nel cloud vengono aggiornati.

Collegamento di una policy a un gruppo di oggetti

Usa il comando `AttachPolicy` per collegare una policy a un gruppo di oggetti e, di conseguenza, a tutti gli oggetti presenti nel gruppo e agli oggetti nei relativi gruppi figlio:

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

Il comando `AttachPolicy` non produce output

Important

È possibile collegare un numero massimo di due policy per un gruppo.

Note

Non è consigliabile utilizzare informazioni di identificazione personale nei nomi delle policy.

Il parametro `--target` può essere l'ARN di un gruppo di oggetti (come sopra), l'ARN di un certificato o un'identità Amazon Cognito. Per ulteriori informazioni su policy, certificati e autenticazione, consulta [Sicurezza e identità per AWS IoT](#) (p. 183).

Scollegamento di una policy da un gruppo di oggetti

Usa il comando `DetachPolicy` per scollegare una policy da un gruppo di oggetti e, di conseguenza, da tutti gli oggetti presenti nel gruppo e gli oggetti nei relativi gruppi figlio:

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

Il comando `DetachPolicy` non produce output.

Elenco di policy collegate a un gruppo di oggetti

Usa il comando `ListAttachedPolicies` per elencare le policy collegate a un gruppo:

```
$ aws iot list-attached-policies --target "arn:aws:iot:us-west-2:123456789012:thinggroup/RedLights"
```

Il parametro `--target` può essere l'ARN di un gruppo di oggetti (come sopra), l'ARN di un certificato o un'identità Amazon Cognito.

Aggiungi il parametro opzionale `--recursive` per includere anche tutte le policy collegate ai gruppi padre del gruppo.

Il comando `ListAttachedPolicies` restituisce un elenco di policy:

```
{
  "policies": [
    "MyLightBulbPolicy"
    ...
}
```

```
    ]  
}
```

Elenco di gruppi per una policy

Usa il comando `ListTargetsForPolicy` per elencare i target, inclusi i gruppi, a cui una policy è collegata:

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

Aggiungi il parametro opzionale `--page-size number` per specificare il numero massimo di risultati da restituire per ogni query e il parametro `--marker string` nelle chiamate successive per recuperare il set di risultati successivo, se presente.

Il comando `ListTargetsForPolicy` restituisce un elenco di target e il token da usare per recuperare ulteriori risultati:

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

Recupero delle policy valide per un oggetto

Usa il comando `GetEffectivePolicies` per elencare le policy valide per un oggetto, incluse le policy collegate ai gruppi a cui l'oggetto appartiene, indipendentemente dal fatto che il gruppo sia un padre diretto o un predecessore indiretto:

```
$ aws iot get-effective-policies \  
  --thing-name "MyLightBulb" \  
  --principal "arn:aws:iot:us-east-1:123456789012:cert/  
a0c01f5835079de0a7514643d68ef8414ab739a1e94ee4162977b02b12842847"
```

Usa il parametro `--principal` per specificare l'ARN del certificato collegato all'oggetto. Se usi l'autenticazione dell'identità di Amazon Cognito, adopera il parametro `--cognito-identity-pool-id` e, facoltativamente, aggiungi il parametro `--principal` per specificare un'identità di Cognito. Se specifichi solo `--cognito-identity-pool-id`, vengono restituite le policy associate al ruolo del pool di identità per gli utenti non autenticati. Se usi entrambi i parametri, vengono restituite le policy associate al ruolo del pool di identità per gli utenti autenticati.

Il parametro `--thing-name` è opzionale e può essere usato al posto del parametro `--principal`. Quando viene usato, vengono restituite le policy collegate a qualsiasi gruppo a cui l'oggetto appartiene e le policy collegate a qualsiasi gruppo padre di questi gruppi (fino al gruppo root nella gerarchia).

Il comando `GetEffectivePolicies` restituisce un elenco di policy:

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

Test dell'autorizzazione per le operazioni MQTT

Usa il comando TestAuthorization per verificare se un'operazione MQTT è permessa per un oggetto:

```
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\"]}"
```

Usa il parametro `--principal` per specificare l'ARN del certificato collegato all'oggetto. Se usi l'autenticazione dell'identità di Amazon Cognito, specifica un'identità di Cognito come `--principal` oppure usa il parametro `--cognito-identity-pool-id` o entrambe le cose. Se specifichi solo `--cognito-identity-pool-id`, vengono considerate le policy associate al ruolo del pool di identità per gli utenti non autenticati. Se usi entrambi i parametri, vengono considerate le policy associate al ruolo del pool di identità per gli utenti autenticati.

Specifica una o più operazioni MQTT da testare elencando i set di risorse e i tipi di operazioni dopo il parametro `--auth-infos`. Il campo `actionType` deve contenere "PUBLISH", "SUBSCRIBE", "RECEIVE" o "CONNECT". Il campo `resources` deve contenere un elenco di ARN di risorse. Per ulteriori informazioni, consulta [Policy AWS IoT \(p. 198\)](#).

È possibile testare gli effetti dell'aggiunta di policy specificandole con il parametro `--policy-names-to-add`. In alternativa, è possibile testare gli effetti della rimozione di policy con il parametro `--policy-names-to-skip`.

Puoi usare il parametro opzionale `--client-id` per affinare ulteriormente i risultati.

Il comando TestAuthorization restituisce i dettagli delle operazionimesse o non messe per ogni set di query `--auth-infos` specificato:

```
{
  "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" ]
  ]
}
```

Gruppo di oggetti dinamici

I gruppi di oggetti dinamici aggiornano l'appartenenza al gruppo tramite le query di ricerca. Utilizzando i gruppi di oggetti dinamici, è possibile modificare la modalità di interazione con gli oggetti a seconda dei dati di connettività, registro o shadow.

È possibile applicare una policy a un gruppo di oggetti dinamico. Un oggetto può appartenere a non più di 10 gruppi dinamici. Se una stringa di query di ricerca definisce un gruppo di oggetti dinamici che contiene un elemento che appartiene già a 10 gruppi di oggetti dinamici, la policy non viene applicata a quell'oggetto.

Poiché i gruppi di oggetti dinamici sono collegati all'indice del parco istanze, è necessario abilitare il servizio di indicizzazione del parco istanze per utilizzarli. È possibile visualizzare in anteprima gli oggetti in un gruppo di oggetti dinamico prima di creare il gruppo con una query di ricerca di indicizzazione del parco istanze. Per ulteriori informazioni, consulta la sezione relativa al [servizio di indicizzazione del parco istanze](#) e la sezione relativa al [servizio di indicizzazione del parco istanze: sintassi della query](#).

È possibile specificare un gruppo di oggetti dinamico come destinazione per un processo. Solo gli oggetti che soddisfano i criteri che definiscono il gruppo di oggetti dinamico eseguono il processo.

Ad esempio, supponiamo che si desideri aggiornare il firmware per i propri dispositivi ma, per ridurre al minimo la possibilità che l'aggiornamento venga interrotto, si desidera solo aggiornare firmware su dispositivi la cui batteria sia carica almeno all'80%. È possibile creare un gruppo di oggetti dinamico che includa solo i dispositivi con batteria carica almeno all'80% ed è possibile utilizzare quel gruppo come destinazione per il processo di aggiornamento del firmware. Solo i dispositivi che soddisfano i criteri di durata della batteria riceveranno l'aggiornamento firmware. Poiché i dispositivi raggiungono i criteri di carica della batteria pari all'80%, vengono automaticamente aggiunti al gruppo di oggetti dinamico e ricevono l'aggiornamento del firmware.

Per ulteriori informazioni sull'indicazione di gruppi di oggetti come destinazioni di processo, consulta la sezione relativa all'[utilizzo di API dei processi AWS IoT](#).

I gruppi di oggetti dinamici differiscono dai gruppi di oggetti statici per le seguenti caratteristiche:

- L'appartenenza degli oggetti non è esplicitamente definita. Per creare un gruppo di oggetti dinamico, è necessario definire una stringa di query che stabilisce l'appartenenza al gruppo.
- I gruppi di oggetti dinamici non possono essere parte di una gerarchia.
- È possibile utilizzare un altro set di comandi per creare, aggiornare ed eliminare i gruppi di oggetti dinamici. Per tutte le altre operazioni, gli stessi comandi utilizzati per l'interazione con i gruppi di oggetti statici possono essere utilizzati per interagire con i gruppi di oggetti dinamici.
- Un singolo account non può avere più di 100 gruppi di oggetti dinamici definiti.

Per ulteriori informazioni sui gruppi di oggetti statici, consulta [Gruppi di oggetti \(p. 163\)](#).

Ad esempio, supponiamo di creare un gruppo dinamico che contiene tutte le stanze in un warehouse la cui temperatura è superiore a 60 gradi Fahrenheit. Quando la temperatura di una stanza è di almeno 61°C, viene aggiunta al gruppo di oggetti dinamico RoomTooWarm. In tutte le stanze del gruppo di oggetti

dinamico RoomTooWarm vengono accese le ventole di raffreddamento. Quando la temperatura di una stanza scende almeno sotto i 60° C, viene rimossa dal gruppo di oggetti dinamico e la relativa ventola viene spenta.

Creazione di un gruppo di oggetti dinamico

Utilizza il comando `CreateDynamicThingGroup` per creare un gruppo di oggetti dinamico. Per creare un gruppo di oggetti dinamico per la stanza troppo calda utilizzare il comando CLI `create-dynamic-thing-group`:

```
$ aws iot create-dynamic-thing-group --thing-group-name "RoomTooWarm" --query-string "attributes.temperature>60"
```

Note

Non è consigliabile utilizzare informazioni di identificazione personale nei nomi dei gruppi di oggetti dinamici.

Il comando `CreateDynamicThingGroup` restituisce una risposta che contiene il nome dell'indice, la stringa di query, versione di query, nome del gruppo di oggetti, ID del gruppo di oggetti e ARN del gruppo di oggetti:

```
{  
    "indexName": "AWS_Things",  
    "queryVersion": "2017-09-30",  
    "thingGroupName": "RoomTooWarm",  
    "thingGroupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/RoomTooWarm",  
    "queryString": "attributes.temperature>60\\n",  
    "thingGroupId": "abcdefghijklmnopqrstuvwxyz12345678ijklmnop12345678qrstuvwxyz"  
}
```

Creazione del gruppo di oggetti dinamici non è immediata. Il backfill del gruppo di oggetti dinamici richiede tempo per il completamento. Quando un gruppo di oggetti dinamico viene creato, lo stato del gruppo è impostato su `BUILDING`. Quando il backfill è completo, lo stato diventa `ACTIVE`. Per controllare lo stato dei tuoi gruppi di oggetti dinamici, utilizza il comando [DescribeThingGroup](#).

Descrizione di un gruppo di oggetti dinamico

Utilizza il comando `DescribeThingGroup` per ottenere informazioni su un gruppo di oggetti dinamico:

```
$ aws iot describe-thing-group --thing-group-name "RoomTooWarm"
```

Il comando `DescribeThingGroup` restituisce le informazioni relative al gruppo specificato:

```
{  
    "status": "ACTIVE",  
    "indexName": "AWS_Things",  
    "thingGroupName": "RoomTooWarm",  
    "thingGroupArn": "arn:aws:iot:us-west-2:123456789012:thinggroup/RoomTooWarm",  
    "queryString": "attributes.temperature>60\\n",  
    "version": 1,  
    "thingGroupMetadata": {  
        "creationDate": 1548716921.289  
    },  
    "thingGroupProperties": {},  
    "queryVersion": "2017-09-30",  
    "thingGroupId": "84dd9b5b-2b98-4c65-84e4-be0e1ecf4fd8"  
}
```

L'esecuzione di `DescribeThingGroup` su un gruppo di oggetti dinamico restituisce attributi specifici per i gruppi di oggetti dinamici, come il `queryString` e lo stato.

Lo stato di un gruppo di oggetti dinamici può utilizzare i seguenti valori:

ACTIVE

Il gruppo di oggetti dinamico è pronto per l'uso.

BUILDING

Il gruppo di oggetti dinamico viene creato e l'appartenenza agli oggetti è in fase di elaborazione.

REBUILDING

L'appartenenza del gruppo di oggetti dinamico viene aggiornata in seguito all'adeguamento della query di ricerca del gruppo.

Note

Dopo aver creato un gruppo di oggetti dinamico, è possibile utilizzare il gruppo, indipendentemente dal suo stato. Solo i gruppi di oggetti dinamici con uno stato **ACTIVE** includono tutti gli oggetti che corrispondono alle query di ricerca per quel gruppo di oggetti dinamico. I gruppi di oggetti dinamici con gli stati **REBUILDING** e **BUILDING** potrebbero non includere tutti gli oggetti che corrispondono alla query di ricerca.

Aggiornamento di un gruppo di oggetti dinamico

Utilizzare il comando `UpdateDynamicThingGroup` per aggiornare gli attributi di un gruppo di oggetti dinamico, tra cui la query di ricerca del gruppo. Il comando seguente aggiorna la descrizione del gruppo di oggetti e la stringa di query cambiando il criterio di appartenenza in `> 65`:

```
$ aws iot update-dynamic-thing-group --thing-group-name "RoomTooWarm" --thing-group-properties "thingGroupDescription=\"This thing group contains rooms warmer than 65F.\" --query-string "attributes.temperature>65"
```

Il comando `UpdateDynamicThingGroup` restituisce una risposta che contiene il numero di versione del gruppo dopo l'aggiornamento:

```
{  
    "version": 2  
}
```

Gli aggiornamenti del gruppo di oggetti dinamico non sono immediati. Il backfill del gruppo di oggetti dinamici richiede tempo per il completamento. Quando un gruppo di oggetti dinamici viene aggiornato, lo stato del gruppo diventa **REBUILDING** mentre il gruppo aggiorna la sua appartenenza. Quando il backfill è completo, lo stato diventa **ACTIVE**. Per controllare lo stato dei tuoi gruppi di oggetti dinamici, utilizza il comando [DescribeThingGroup](#).

Eliminazione di un gruppo di oggetti dinamico

Utilizzare il comando `DeleteDynamicThingGroup` per eliminare un gruppo di oggetti dinamico:

```
$ aws iot delete-dynamic-thing-group --thing-group-name "RoomTooWarm"
```

Il comando `DeleteDynamicThingGroup` non produce output.

Prima di eliminare un gruppo a cui è collegata una policy, controlla che la rimozione delle autorizzazioni non comprometta il corretto funzionamento degli oggetti nel gruppo. I comandi che mostrano i gruppi a cui un oggetto appartiene (ad esempio, `ListGroupsForThing`) potrebbero continuare a segnalare il gruppo mentre i record nel cloud vengono aggiornati.

Restrizioni e conflitti

I gruppi di oggetti dinamici condividono alcune restrizioni dei gruppi di oggetti statici:

- Un gruppo di oggetti può avere fino a 50 attributi.
- Un oggetto può appartenere fino a un massimo di 10 gruppi di oggetti.
- Questo gruppo di oggetti non può essere rinominato.
- I nomi dei gruppi di oggetti non possono contenere caratteri internazionali, ad esempio, û, é e ñ.

Quando usi i gruppi di oggetti dinamici, tieni presente quanto segue.

I gruppi di oggetti dinamici precedenti hanno la priorità sui gruppi più recenti

Per impostazione predefinita, se un oggetto appartiene a 10 gruppi di oggetti, non è possibile aggiungerlo a ulteriori gruppi. Se si verifica un conflitto di appartenenza tra i gruppi di oggetti dinamici quando si crea o si aggiorna un gruppo di oggetti dinamici, i gruppi di oggetti dinamici precedenti hanno la priorità rispetto a quelli più recenti.

Con `overrideDynamicGroups` abilitato, i gruppi statici hanno la priorità sui gruppi dinamici

Per impostazione predefinita, se un oggetto appartiene a 10 gruppi di oggetti, non è possibile aggiungere l'oggetto a ulteriori gruppi. Se si aggiorna l'appartenenza dell'oggetto con i comandi [AddThingToThingGroup](#) o [UpdateThingGroupsForThing](#), è possibile utilizzare il flag `overrideDynamicGroups` per far sì che i gruppi di oggetti statici abbiano la priorità sui gruppi di oggetti dinamici. Con `overrideDynamicGroups` abilitato, se un oggetto appartiene a 10 gruppi di oggetti e uno o più di questi gruppi è dinamico, l'aggiunta dell'oggetto a un gruppo di oggetti statico lo rimuove dal gruppo di oggetti dinamico più recente.

Ad esempio, supponiamo che si crei un gruppo di oggetti dinamico denominato `DynamicGroup1` e quindi che si creino altri nove gruppi di oggetti dinamici, dove `DynamicGroup10` è l'ultimo gruppo creato. Se `Thing1` appartiene a tutti i 10 gruppi di oggetti dinamici, l'aggiunta manuale di `Thing1` a un gruppo statico con `OverrideDynamicGroups` abilitato rimuove l'oggetto da `DynamicGroup10`.

Applicazione di policy ai membri di un gruppo di oggetti dinamico

Una policy può essere applicata a un gruppo di oggetti dinamico. Un oggetto può appartenere a non più di 10 gruppi dinamici. Se una stringa di query di ricerca definisce un gruppo di oggetti dinamici che contiene un elemento che appartiene già a 10 gruppi di oggetti dinamici, la policy non viene applicata a quell'oggetto.

L'appartenenza a un gruppo di oggetti dinamico è consistente finale

Solo lo stato finale di un oggetto è valutato per il registro. Gli stati intermedi possono essere ignorati se vengono aggiornati rapidamente. Evitare l'associazione di una regola, di un processo o di una policy con un gruppo di oggetti dinamico la cui appartenenza dipenda dallo stato intermedio.

Il servizio di indicizzazione del parco istanze deve essere abilitato

Il servizio di indicizzazione del parco istanze deve essere abilitato e il backfill di indicizzazione del parco istanze deve essere completato prima di poter creare e utilizzare gruppi di oggetti dinamici. Prevedere un ritardo dopo l'abilitazione del servizio di indicizzazione del parco istanze. Il completamento del backfill potrebbe richiedere un po' di tempo. Maggiore è il numero di oggetti registrati, maggiore è il tempo necessario al processo di backfill. Una volta attivato il servizio di indicizzazione del parco istanze per i gruppi di oggetti dinamici, non è possibile eliminare tutti i gruppi di oggetti dinamici.

Note

Se si dispone di autorizzazioni per eseguire query all'indice del parco istanze, è possibile accedere ai dati degli oggetti sull'intero parco istanze.

Tagging delle risorse AWS IoT

Per facilitare la gestione e l'organizzazione di gruppi di oggetti, tipi di oggetti, regole di argomenti, processi, audit pianificati e profili di sicurezza, puoi scegliere di assegnare i metadati a ciascuna di queste risorse sotto forma di tag. Questa sezione descrive i tag e mostra come crearli.

Per aiutarti a gestire i costi correlati agli oggetti, è possibile creare [gruppi di fatturazione \(p. 181\)](#) che contengono gli oggetti. Puoi quindi assegnare i tag contenenti i metadati a ognuno di questi gruppi di fatturazione. Questa sezione illustra inoltre i gruppi di fatturazione e i comandi disponibili per crearli e gestirli.

Nozioni di base sui tag

I tag ti consentono di categorizzare le risorse AWS in modi diversi, ad esempio per scopo, proprietario o ambiente. Questa funzionalità è molto utile quando hai tante risorse dello stesso tipo: puoi rapidamente individuare una risorsa specifica in base ai tag assegnati. Ogni tag è formato da una chiave e da un valore opzionale, entrambi personalizzabili. Ad esempio, puoi definire un set di tag per i tuoi tipi di oggetti che consente di monitorare i dispositivi per tipo. Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti di ciascun tipo di risorsa. Tramite un set di chiavi di tag coerente la gestione delle risorse risulta notevolmente semplificata.

Puoi cercare e filtrare le risorse in base ai tag che aggiungi o applichi. Puoi anche utilizzare i tag dei gruppi di fatturazione per classificare e monitorare i costi. È possibile anche utilizzare i tag per controllare l'accesso alle risorse come descritto in [Utilizzo dei tag con policy IAM \(p. 181\)](#).

Per semplicità di utilizzo, Tag Editor nella Console di gestione AWS fornisce una soluzione centrale e unificata per creare e gestire i tag. Per ulteriori informazioni, consulta [Utilizzo con l'editor di tag](#) in [Utilizzo della Console di gestione AWS](#).

Puoi utilizzare i tag anche con l'interfaccia a riga di comando di AWS e l'API di AWS IoT. Puoi associare i tag a gruppi di oggetti, tipi di oggetti, regole di argomenti, processi, profili di sicurezza e gruppi di fatturazione quando li crei tramite il campo "Tags" nei seguenti comandi:

- [CreateBillingGroup \(p. 706\)](#)
- [CreateDynamicThingGroup \(p. 710\)](#)
- [CreateJob \(p. 713\)](#)
- [CreateOTAUpdate \(p. 720\)](#)
- [CreateScheduledAudit \(p. 731\)](#)
- [CreateSecurityProfile \(p. 733\)](#)
- [CreateStream \(p. 737\)](#)
- [CreateThingGroup \(p. 742\)](#)
- [CreateThingType \(p. 745\)](#)
- [CreateTopicRule \(p. 747\)](#)

Puoi aggiungere, modificare o eliminare i tag per le risorse esistenti che supportano il tagging utilizzando i comandi seguenti:

- [TagResource \(p. 999\)](#)
- [ListTagsForResource \(p. 932\)](#)
- [UntagResource \(p. 1007\)](#)

Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore sovrascrive quello precedente. Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa.

Ulteriori informazioni sono disponibili in [Strategie di tagging di AWS](#).

Restrizioni e limitazioni di tag

Si applicano le seguenti limitazioni di base ai tag:

- Numero massimo di tag per risorsa: 50
- Lunghezza massima della chiave: 127 caratteri Unicode in formato UTF-8
- Lunghezza massima del valore: 255 caratteri Unicode in formato UTF-8
- Per chiavi e valori di tag viene fatta la distinzione tra maiuscole e minuscole.
- Non utilizzare il prefisso "aws:" nei nomi o nei valori dei tuoi tag perché è prenotato per l'utilizzo in AWS. Non è possibile modificare né eliminare i nomi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati per il limite del numero di tag per risorsa.
- Se lo schema di tagging viene utilizzato in più servizi e risorse, è necessario tenere presente che in altri servizi possono essere presenti limiti sui caratteri consentiti. In generale, i caratteri consentiti sono in genere lettere, spazi e numeri rappresentabili in formato UTF-8, più i caratteri speciali + - = . _ : / @.

Utilizzo dei tag con policy IAM

È possibile applicare autorizzazioni a livello di risorsa basate su tag nelle policy IAM utilizzate per le operazioni API AWS IoT. In questo modo è possibile controllare meglio le risorse che un utente può creare, modificare o utilizzare. Puoi utilizzare l'elemento `Condition` (denominato anche blocco `Condition`) con i seguenti valori e chiavi di contesto di condizione in una policy IAM per controllare l'accesso dell'utente (autorizzazione) in base ai tag della risorsa:

- Utilizza `aws:ResourceTag/tag-key: tag-value` per concedere o negare agli utenti operazioni su risorse con specifici tag.
- Utilizza `aws:RequestTag/tag-key: tag-value` per richiedere che un tag specifico venga utilizzato (o non utilizzato) durante la creazione di una richiesta API per creare o modificare una risorsa che abilita i tag.
- Utilizza `aws:TagKeys: [tag-key, ...]` per richiedere che un set di tag specifico venga utilizzato (o non utilizzato) durante la creazione di una richiesta API per creare o modificare una risorsa che abilita i tag.

Note

Le chiavi di contesto della condizione e i valori all'interno di una policy di IAM si applicano solo alle azioni AWS IoT in cui un identificatore per una risorsa in grado di essere taggata è un parametro obbligatorio. Ad esempio, l'uso di [DescribeEndpoint \(p. 802\)](#) non sarà consentito né negato in base a valori e chiavi di contesto della condizione perché nessuna risorsa taggabile (gruppi di oggetti, tipi di oggetti, regole di argomento, processi o profili di sicurezza) viene mostrata in questa richiesta.

Il controllo degli accessi utilizzando i tag nella Guida per l'utente AWS Identity and Access Management contiene ulteriori informazioni sull'utilizzo dei tag. La sezione relativa al riferimento alle policy JSON IAM della guida ha una sintassi dettagliata, descrizioni ed esempi di elementi, variabili e logica di valutazione delle policy JSON in IAM.

La policy di esempio seguente applica due restrizioni basate su tag. Un utente IAM limitato da questa policy:

- Non può assegnare a una risorsa il tag "env = prod" (nell'esempio, consulta la riga "aws:RequestTag/env" : "prod")
- Non può modificare o accedere a una risorsa con un tag esistente "env = prod" (nell'esempio, consulta la riga "aws:ResourceTag/env" : "prod").

```
{  
    "Version" : "2012-10-17",  
    "Statement" : [  
        {  
            "Effect" : "Deny",  
            "Action" : "iot:*",  
            "Resource" : "*",  
            "Condition" : {  
                "StringEquals" : {  
                    "aws:RequestTag/env" : "prod"  
                }  
            }  
        },  
        {  
            "Effect" : "Deny",  
            "Action" : "iot:*",  
            "Resource" : "*",  
            "Condition" : {  
                "StringEquals" : {  
                    "aws:ResourceTag/env" : "prod"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "iot:*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

È anche possibile specificare più valori di tag per una determinata chiave tag racchiudendoli in un elenco, come segue:

```
"StringEquals" : {  
    "aws:ResourceTag/env" : ["dev", "test"]  
}
```

Note

Se consenti o neghi a un utente l'accesso a risorse in base ai tag, devi considerare esplicitamente di negare agli utenti la possibilità di aggiungere o rimuovere tali tag dalle stesse risorse. In caso contrario, un utente può eludere le restrizioni e ottenere l'accesso a una risorsa modificandone i tag.

Gruppi di fatturazione

AWS IoT non consente di applicare direttamente i tag a oggetti singoli, ma consente di posizionare gli oggetti nei gruppi di fatturazione e applicare i tag a essi. Per AWS IoT, l'allocazione dei costi e l'utilizzo dei dati in base ai tag è limitato ai gruppi di fatturazione.

Sono disponibili i seguenti comandi:

- [AddThingToBillingGroup \(p. 689\)](#) aggiunge un oggetto a un gruppo di fatturazione.
- [CreateBillingGroup \(p. 706\)](#) crea un gruppo di fatturazione.
- [DeleteBillingGroup \(p. 764\)](#) elimina il gruppo di fatturazione.
- [DescribeBillingGroup \(p. 794\)](#) restituisce informazioni su un gruppo di fatturazione.
- [ListBillingGroups \(p. 895\)](#) elenca i gruppi di fatturazione creati.
- [ListThingsInBillingGroup \(p. 948\)](#) elenca gli oggetti che hai aggiunto al gruppo di fatturazione specificato.
- [RemoveThingFromBillingGroup \(p. 966\)](#) rimuove l'oggetto specificato dal gruppo di fatturazione.
- [UpdateBillingGroup \(p. 1012\)](#) aggiorna le informazioni sul gruppo di fatturazione.
- [CreateThing \(p. 740\)](#) consente di specificare un gruppo di fatturazione per l'oggetto al momento della creazione.
- [DescribeThing \(p. 828\)](#) restituisce la descrizione di un oggetto, incluso il gruppo di fatturazione a cui appartiene l'oggetto, se presente.

Visualizzazione dell'allocazione dei costi e dei dati di utilizzo

Puoi utilizzare i tag dei gruppi di fatturazione per classificare e monitorare i costi. Quando applichi i tag a zone ospitate (e quindi agli oggetti che includono), AWS genera un report di allocazione dei costi come un file CSV (comma-separated value) con l'utilizzo e i costi aggregati dai tuoi tag. Puoi applicare i tag che rappresentano categorie di business (come centri di costo, nomi di applicazioni o proprietari) per organizzare i costi tra più servizi. Per ulteriori informazioni sull'utilizzo dei tag per l'allocazione dei costi, consulta la pagina relativa all'[utilizzo di tag per l'allocazione dei costi](#) nella [Guida per l'utente sulla gestione di costi e fatturazione AWS](#).

Note

Per associare in modo preciso i dati sull'utilizzo e sui costi agli oggetti inseriti nei gruppi di fatturazione, ogni dispositivo o applicazione deve:

- Essere registrato come oggetto su AWS IoT (consulta [Gestione di dispositivi con AWS IoT \(p. 157\)](#)).
- Connetersi al broker di messaggi AWS IoT tramite MQTT utilizzando solo il nome dell'oggetto, come l'ID client (consulta [Broker di messaggi per AWS IoT \(p. 239\)](#)).
- Eseguire l'autenticazione utilizzando un certificato client associato all'oggetto.

Per i gruppi di fatturazione sono disponibili le seguenti dimensioni di prezzo (in base alle attività degli oggetti associati al gruppo di fatturazione):

- Connattività (in base al nome dell'oggetto utilizzato come ID client per la connessione)
- Messaggistica (in base ai messaggi in entrata e in uscita da e verso un oggetto; solo MQTT)
- Operazioni shadow (in base all'oggetto il cui messaggio ha attivato un aggiornamento shadow)

- Regole attivate (in base all'oggetto il cui messaggio in entrata ha attivato la regola; non si applica alle regole attivate da eventi del ciclo di vita MQTT)
- Aggiornamenti indice dell'oggetto (in base all'oggetto aggiunto all'indice)
- Azioni remote (in base all'oggetto aggiornato)
- Report [Rilevamento \(p. 558\)](#) (in base all'oggetto di cui viene riportata l'attività)

I dati sui costi e sull'utilizzo basati sui tag (e riportati per un gruppo di fatturazione) non riflettono le seguenti attività:

- Operazioni di registro del dispositivo (inclusi gli aggiornamenti di oggetti, gruppi di oggetti e tipi di oggetti; consulta [Gestione di dispositivi con AWS IoT \(p. 157\)](#))
- Aggiornamenti indice gruppo oggetti (quando si aggiunge un gruppo di oggetti)
- Query di ricerca indice
- [Provisioning dei dispositivi \(p. 482\)](#)
- Report di Audit (p. 505)

Limiti

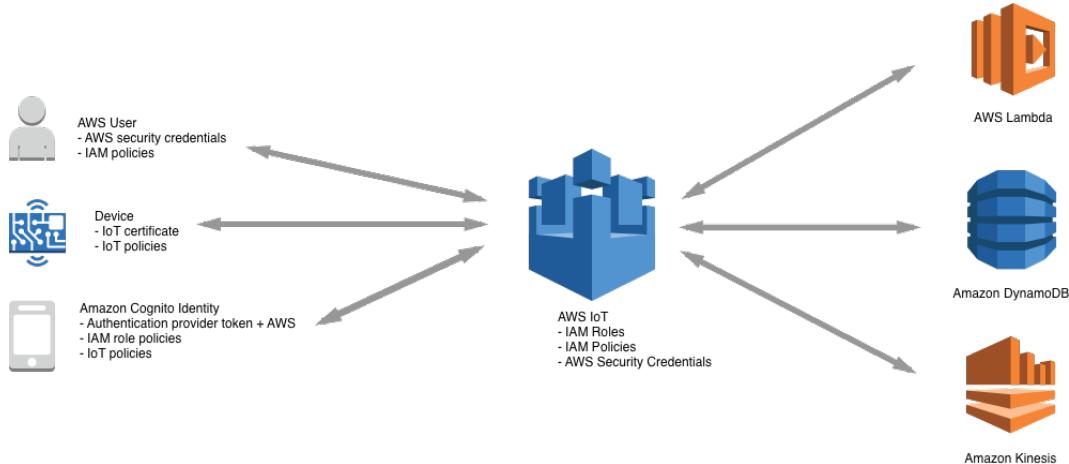
- Un oggetto può appartenere esattamente a un gruppo di fatturazione.
- A differenza dei gruppi di oggetti, i gruppi di fatturazione non possono essere organizzati in gerarchie.
- Affinché il loro utilizzo possa essere registrato per scopi di tagging e di fatturazione, un dispositivo deve:
 - Essere registrato come oggetto su AWS IoT.
 - Comunicare con AWS IoT utilizzando solo MQTT.
 - Eseguire l'autenticazione con AWS IoT utilizzando solo il proprio nome oggetto come ID client.
 - Utilizzare solo un certificato X.509 o Amazon Cognito Identity per eseguire l'autenticazione.

Ulteriori informazioni sono disponibili in [Gestione di dispositivi con AWS IoT \(p. 157\)](#), [Sicurezza e identità per AWS IoT \(p. 183\)](#) e in [Provisioning dei dispositivi \(p. 482\)](#). Il comando di API [AttachThingPrincipal \(p. 697\)](#) può essere utilizzato per collegare un certificato o altre credenziali a una cosa.

- Il numero massimo di gruppi di fatturazione per ogni account è 20.000.

Sicurezza e identità per AWS IoT

Ogni dispositivo connesso deve disporre di una credenziale per accedere al broker di messaggi o al servizio Device Shadow. Tutto il traffico da e verso AWS IoT deve essere crittografato tramite Transport Layer Security (TLS). Le credenziali del dispositivo devono essere sempre protette per poter inviare i dati in tutta sicurezza al broker di messaggi. I sistemi di sicurezza del cloud AWS proteggono i dati durante il trasferimento da AWS IoT ad altri dispositivi o servizi AWS.



- Sei responsabile della gestione delle credenziali del dispositivo (certificati X.509, credenziali AWS) nei dispositivi e nelle policy in AWS IoT. Hai anche la responsabilità dell'assegnazione di identità univoca a ogni dispositivo e della gestione delle autorizzazioni per un dispositivo o un gruppo di dispositivi.
- I tuoi dispositivi devono connettersi utilizzando i certificati X.509 o le identità Amazon Cognito tramite una connessione sicura in base al modello di connessione AWS IoT. Durante l'attività di ricerca e sviluppo e per alcune applicazioni che effettuano chiamate API o utilizzano WebSocket, puoi anche usare utenti e gruppi IAM o i token di autenticazione personalizzati.
- Quando usi l'autenticazione di AWS IoT, il broker di messaggi autentica e autorizza tutte le operazioni nel tuo account. Il broker di messaggi è responsabile dell'autenticazione dei dispositivi, dell'inserimento sicuro dei dati dei dispositivi e dell'adesione alle autorizzazioni di accesso applicate ai dispositivi tramite policy.
- Quando usi l'autenticazione personalizzata, alcune autorizzazioni ad hoc sono responsabili dell'autenticazione dei dispositivi e di fornire una policy AWS IoT/IAM per autorizzare le operazioni nel tuo account.
- Il motore di regole AWS IoT inoltra i dati del dispositivo ad altri dispositivi e servizi AWS in base alle regole che hai definito. Il motore usa sistemi di gestione dell'accesso AWS per trasferire in modo sicuro i dati alla destinazione finale.

Autenticazione AWS IoT

AWS IoT supporta quattro tipi di entità principali di identità per l'autenticazione:

- Certificati X.509
- Utenti, gruppi e ruoli IAM
- Identità di Amazon Cognito
- Identità federate

Queste identità possono essere usate con applicazioni per dispositivi mobili, applicazioni Web o applicazioni desktop. Possono anche essere usate da un utente che digita i comandi dell'interfaccia a riga di comando di AWS IoT. In genere, i dispositivi AWS IoT usano i certificati X.509, mentre le applicazioni per dispositivi mobili usano le identità di Amazon Cognito. Le applicazioni Web e desktop usano le identità IAM o federate. I comandi dell'interfaccia a riga di comando usano IAM.

Certificati X.509

I certificati X.509 sono certificati digitali che usano lo [standard di infrastruttura a chiave pubblica X.509](#) per associare una chiave pubblica a un'identità contenuta in un certificato. I certificati X.509 vengono rilasciati da un'entità attendibile denominata autorità di certificazione (CA). L'autorità di certificazione mantiene uno o più certificati speciali chiamati certificati CA, che usa per rilasciare certificati X.509. Solo l'autorità di certificazione ha accesso a certificati CA.

Note

Per una gestione granulare, inclusa la revoca di certificati, consigliamo che a ogni dispositivo sia assegnato un certificato univoco.

I dispositivi devono supportare la rotazione e la sostituzione dei certificati per garantire un funzionamento corretto allo scadere dei certificati.

AWS IoT supporta gli algoritmi di firma dei certificati seguenti:

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

I certificati X.509 sono più sicuri di altri meccanismi di autenticazione come nome utente e password o i token di connessione. I certificati X.509 utilizzano la crittografia asimmetrica, pertanto è possibile masterizzare chiavi private in uno spazio di storage sicuro in un dispositivo. Il materiale crittografico riservato resta sempre nel dispositivo.

AWS IoT autentica i certificati X.509 tramite la modalità di autenticazione client del protocollo TLS. Le librerie TLS vengono comunemente utilizzate per crittografare i dati. Sono disponibili per molti linguaggi di programmazione e sistemi operativi. Durante l'autenticazione client TLS, AWS IoT richiede un certificato X.509 client e convalida lo stato del certificato e dell'account AWS rispetto a un registro di certificati. Contatta quindi il client per verificare la proprietà della chiave privata che corrisponde alla chiave pubblica contenuta nel certificato.

Per usare i certificati AWS IoT, implementazione TLS dei client deve supportare quanto indicato di seguito:

- TLS 1.2.
- Convalida della firma dei certificati SHA-256 RSA.
- Uno dei pacchetti di crittografia indicati nella sezione relativa ai pacchetti di crittografia TLS supportati.

Certificati X.509 e AWS IoT

I dispositivi possono utilizzare i certificati X.509 per eseguire l'autenticazione con AWS IoT.

Autenticazione client

Puoi utilizzare un certificato autofirmato o AWS IoT ne può generare uno per tuo conto. Per fare in modo che AWS IoT generi un certificato, utilizza la console AWS IoT, l'interfaccia a riga di comando `create-keys-and-certificate` o l'API `CreateKeysAndCertificate`. I certificati generati da AWS IoT sono di lunga durata, ma scadono in data 2049-12-31T23:59:59Z, (ossia a mezzanotte GMT del 31 dicembre 2049).

Per creare un certificato autofirmato, utilizza OpenSSL o un set di strumenti simile. Puoi anche registrare un certificato CA, firmare il certificato autofirmato e quindi registrare il certificato autofirmato con AWS IoT.

Per registrare un certificato CA con AWS IoT, utilizza il comando dell'interfaccia a riga di comando `register-ca-certificate` o l'API `RegisterCaCertificate`. Firma il certificato autofirmato utilizzando il certificato CA registrato. Puoi quindi utilizzare l'interfaccia a riga di comando `register-certificate` o l'API `RegisterCertificate` per registrare qualsiasi certificato autofirmato firmato con il CA registrato con AWS IoT.

Note

I dispositivi devono supportare la rotazione e la sostituzione dei certificati per garantire un funzionamento corretto allo scadere dei certificati.

Puoi usare la console o l'interfaccia a riga di comando di AWS IoT per eseguire le operazioni seguenti sui certificati:

- Creare e registrare un certificato AWS IoT.
- Registrare un certificato CA.
- Registrare un certificato del dispositivo.
- Attivare o disattivare un certificato del dispositivo.
- Revocare un certificato del dispositivo.
- Trasferire un certificato del dispositivo a un altro account AWS.
- Elencare tutti i certificati CA registrati nell'account AWS.
- Elencare tutti i certificati dei dispositivi registrati nell'account AWS.

Per ulteriori informazioni sui comandi dell'interfaccia a riga di comando per eseguire queste operazioni, consulta le [informazioni di riferimento sull'interfaccia a riga di comando di AWS IoT](#).

Per ulteriori informazioni sull'uso della console AWS IoT per la creazione di certificati, consulta la pagina relativa alla [creazione e all'attivazione di un certificato del dispositivo](#).

Autenticazione del server

I certificati del server permettono ai dispositivi di verificare che stanno comunicando con AWS IoT e non con un altro servizio che rappresenta AWS IoT. È necessario copiare i certificati del server sul dispositivo e farvi riferimento quando i dispositivi si connettono a AWS IoT. Per ulteriori informazioni, consulta la sezione [SDK AWS IoT per dispositivi \(p. 641\)](#).

I certificati del server AWS IoT vengono firmati da uno dei certificati CA seguenti:

Endpoint VeriSign (legacy)

- Chiave RSA a 2048 bit: [certificato dell'autorità di certificazione primaria pubblica G5 VeriSign di classe 3](#)

Amazon Trust Services Endpoint (preferito)

- Chiave RSA a 2048 bit: [autorità di certificazione root Amazon 1](#).
- Chiave RSA a 4096 bit: Amazon Root CA 2 - Riservato per uso futuro.

- Chiave ECC a 256 bit: [autorità di certificazione root Amazon 3](#).
- Chiave ECC a 384 bit: Amazon Root CA 4 - Riservato per uso futuro.

Consigliamo a tutti i clienti di creare un endpoint Amazon Trust Services (ATS) e di caricare questi certificati CA sui propri dispositivi per evitare problemi con l'imminente diffida generale dai browser di Symantec CA (tra cui VeriSign) che si sono verificati nel mese di ottobre 2018. Per garantire la compatibilità con le versioni precedenti, supportiamo ancora i clienti che utilizzano questi endpoint. I clienti possono recuperare l'endpoint ATS richiamando l'API `describe-endpoint` con il tipo di endpoint `iot:Data-ATS`. I dispositivi che operano in endpoint ATS sono completamente compatibili con i dispositivi che operano negli endpoint Symantec nello stesso account. Non richiedono un'altra registrazione.

```
AWS IoT describe-endpoint --endpoint-type iot:Data-ATS
```

L'archiviazione di tutti questi certificati nel dispositivo può richiedere una quantità notevole di spazio di memoria. Se i dispositivi implementano la convalida basata su RSA, puoi omettere i certificati ECC dell'[autorità di certificazione root Amazon 3](#) e dell'[autorità di certificazione root Amazon 4](#). Se i dispositivi implementano la convalida dei certificati basata su ECC, puoi omettere i certificati RSA dell'[autorità di certificazione root Amazon 1](#) e dell'[autorità di certificazione root Amazon 2](#).

Tutte le nuove regioni AWS IoT Core, a partire dal rilascio di AWS IoT Core nella regione Asia Pacifico (Mumbai) del 9 maggio 2018, offrono solo i certificati ATS.

Note

I certificati CA hanno una data di scadenza dopo la quale non possono più essere usati per convalidare un certificato del server. Potrebbe essere necessario sostituire i certificati CA prima della data di scadenza. Assicurati di poter aggiornare i certificati CA root in tutti i dispositivi per garantire la connessione continua e per mantenere il sistema aggiornato con le best practice di sicurezza.

Per un elenco completo di certificati CA utilizzati da AWS IoT, consulta [Amazon Trust Services](#).

Creazione e registrazione di un certificato del dispositivo AWS IoT

Puoi usare la console AWS IoT o AWS CLI per creare un certificato AWS IoT.

Per creare un certificato (console)

1. Accedi alla console di gestione AWS e apri la [console AWS IoT](#).
2. Nel riquadro di navigazione, seleziona Security (Sicurezza), scegli Certificates (Certificati), quindi Create (Crea).
3. Scegli One-click certificate creation – Create certificate (Creazione certificato con un clic – Crea certificato). In alternativa, per generare un certificato con una richiesta di firma del certificato, scegli Create with CSR (Crea con richiesta di firma del certificato).
4. Usa i collegamenti alla chiave pubblica, alla chiave privata e al certificato per scaricare ognuno di questi elementi in un percorso sicuro.
5. Seleziona Activate (Attiva).

Per creare un certificato (interfaccia a riga di comando)

Nella AWS CLI sono disponibili due comandi per la creazione dei certificati:

- `create-keys-and-certificate`

L'API `CreateKeysAndCertificate` crea una chiave privata, una chiave pubblica e un certificato X.509.

- [create-certificate-from-csr](#)

L'API [CreateCertificateFromCSR](#) crea un certificato a partire da una richiesta di firma del certificato.

Uso di un certificato personale

Per usare i tuoi certificati X.509, devi registrare un certificato CA con AWS IoT. Il certificato CA può essere quindi usato per firmare i certificati dei dispositivi. Puoi registrare fino a 10 certificati CA con lo stesso campo dell'oggetto per ogni account AWS in ogni regione AWS. In questo modo, puoi fare in modo che più di un'autorità di certificazione firmi i certificati dei dispositivi.

Note

I certificati dei dispositivi devono essere firmati dal certificato CA registrato. È una pratica comune usare un certificato CA per creare un certificato CA intermedio. Se usi un certificato intermedio per firmare i certificati dei dispositivi, devi registrare il certificato CA intermedio. Usa il certificato CA root di AWS IoT quando ti connetti a AWS IoT, anche nei casi in cui registri un certificato CA root personale. Il certificato CA root di AWS IoT viene usato dai dispositivi per verificare l'identità dei server AWS IoT.

Argomenti

- [Registrazione del certificato CA \(p. 187\)](#)
- [Creazione di un certificato del dispositivo tramite il certificato CA \(p. 188\)](#)
- [Registrazione di un certificato del dispositivo \(p. 189\)](#)
- [Registrazione manuale di certificati dei dispositivi \(p. 189\)](#)
- [Uso della registrazione automatica/just-in-time per i certificati dei dispositivi \(p. 190\)](#)
- [Disattivazione del certificato CA \(p. 190\)](#)
- [Revoca del certificato del dispositivo \(p. 191\)](#)

Se non disponi di un certificato CA, puoi usare strumenti [OpenSSL](#) per crearne uno.

Per creare un certificato CA

1. Genera una coppia di chiavi.

```
openssl genrsa -out rootCA.key 2048
```

2. Usa la chiave privata della coppia di chiavi per generare un certificato CA.

```
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
```

Registrazione del certificato CA

Per registrare il certificato CA, devi eseguire le operazioni seguenti:

- Ottenerne un codice di registrazione da AWS IoT.
- Firma un certificato di verifica della chiave privata con il certificato CA.
- Passa il certificato CA e un certificato di verifica della chiave privata al comando `register-ca-certificate` della AWS CLI.

Il campo `Common Name` nel certificato di verifica della chiave privata deve essere impostato sul codice di registrazione generato dal comando `get-registration-code` dell'interfaccia a riga di comando. Per ogni account AWS viene generato un singolo codice di registrazione. Puoi usare il comando `register-ca-certificate` o la console AWS IoT per registrare i certificati CA.

Note

Un certificato CA non può essere registrato per più di un account nella stessa regione AWS. Tuttavia, un certificato CA può essere registrato per più di un account se questi si trovano in regioni AWS diverse.

Per registrare un certificato CA

1. Ottenerne un codice di registrazione da AWS IoT. Questo codice viene usato come Common Name del certificato di verifica della chiave privata.

```
AWS IoT get-registration-code
```

2. Genera una coppia di chiavi per il certificato di verifica della chiave privata.

```
openssl genrsa -out verificationCert.key 2048
```

3. Crea una richiesta di firma del certificato per il certificato di verifica della chiave privata. Imposta il campo Common Name del certificato sul codice di registrazione.

```
openssl req -new -key verificationCert.key -out verificationCert.csr
```

Ti verrà richiesto di immettere alcune informazioni, tra cui il Common Name per il certificato.

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

4. Usa la richiesta di firma del certificato per creare un certificato di verifica della chiave privata.

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

5. Registra il certificato CA con AWS IoT. Passa il certificato CA e il certificato di verifica della chiave privata al comando register-ca-certificate dell'interfaccia a riga di comando.

```
AWS IoT register-ca-certificate --ca-certificate file://rootCA.pem --verification-cert  
file://verificationCert.pem
```

6. Usa il comando update-certificate dell'interfaccia a riga di comando per attivare il certificato CA.

```
AWS IoT update-ca-certificate --certificate-id XXXXXXXXXXXX --new-status ACTIVE
```

Creazione di un certificato del dispositivo tramite il certificato CA

Puoi usare un certificato CA registrato con AWS IoT per creare un certificato del dispositivo. Il certificato del dispositivo deve essere registrato con AWS IoT prima dell'uso.

Per creare un certificato del dispositivo

1. Genera una coppia di chiavi.

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

2. Crea una richiesta di firma del certificato per il certificato del dispositivo.

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

Ti verrà richiesto di immettere alcune informazioni, come mostrato qui.

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

3. Crea un certificato del dispositivo dalla richiesta di firma del certificato.

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

Note

Per creare i certificati dei dispositivi, devi usare un certificato CA registrato con AWS IoT. Se nell'account AWS hai registrato più di un certificato CA (con lo stesso campo dell'oggetto e la stessa chiave pubblica), devi specificare il certificato CA usato per creare il certificato del dispositivo quando registri quest'ultimo.

4. Registrare un certificato del dispositivo.

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

5. Usa il comando update-certificate dell'interfaccia a riga di comando per attivare il certificato del dispositivo.

```
aws iot update-certificate --certificate-id xxxxxxxxxxxx --new-status ACTIVE
```

Registrazione di un certificato del dispositivo

Per firmare i certificati dei dispositivi, occorre usare un certificato CA registrato con AWS IoT. Se nell'account AWS hai registrato più di un certificato CA (con lo stesso campo dell'oggetto e la stessa chiave pubblica), devi specificare il certificato CA usato per firmare il certificato del dispositivo quando registri quest'ultimo. Puoi registrare ogni certificato del dispositivo manualmente oppure puoi usare la registrazione automatica, che permette ai dispositivi di registrare il proprio certificato quando si connettono a AWS IoT per la prima volta.

Registrazione manuale di certificati dei dispositivi

Usa il comando dell'interfaccia a riga di comando seguente per registrare un certificato del dispositivo:

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

Uso della registrazione automatica/just-in-time per i certificati dei dispositivi

Per registrare i certificati dei dispositivi automaticamente quando i dispositivi si connettono per la prima volta a AWS IoT, abilita la registrazione automatica per il certificato CA. Questa operazione regista qualsiasi certificato del dispositivo firmato dal certificato CA al momento della connessione a AWS IoT.

Abilitazione della registrazione automatica

Usa l'API `update-ca-certificate` per impostare il valore di `auto-registration-status` del certificato CA su `ENABLE`.

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

Puoi anche impostare `auto-registration-status` su `ENABLE` quando usi l'API `register-ca-certificate` per registrare il certificato CA:

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

Quando un dispositivo tenta di connettersi per la prima volta a AWS IoT, come parte dell'handshake TLS, deve presentare un certificato CA registrato e un certificato del dispositivo. AWS IoT riconosce il certificato CA come registrato, registra il certificato del dispositivo e ne imposta lo stato su `PENDING_ACTIVATION`. Questo significa che il certificato del dispositivo è stato automaticamente registrato ed è in attesa dell'attivazione. Un certificato deve essere nello stato `ACTIVE` prima di poter essere usato per la connessione a AWS IoT. Quando AWS IoT registra automaticamente un certificato o quando un certificato nello stato `PENDING_ACTIVATION` si connette, AWS IoT pubblica un messaggio nell'argomento MQTT seguente:

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

Dove `caCertificateID` è l'ID del certificato CA che ha rilasciato il certificato del dispositivo.

Il messaggio pubblicato in questo argomento ha la struttura seguente:

```
{  
    "certificateId": "certificateID",  
    "caCertificateId": "caCertificateID",  
    "timestamp": timestamp,  
    "certificateStatus": "PENDING_ACTIVATION",  
    "awsAccountId": "awsAccountId",  
    "certificateRegistrationTimestamp": "certificateRegistrationTimestamp"  
}
```

Puoi creare una regola che resti in ascolto in questo argomento ed esegua alcune operazioni. Ti consigliamo di creare una regola Lambda che verifichi che il certificato del dispositivo non sia incluso in un elenco di revoche di certificati (CRL), che attivi il certificato e crei e colleghi una policy a quest'ultimo. La policy determina le risorse cui il dispositivo è in grado di accedere. Per ulteriori informazioni su come creare una regola Lambda che resti in attesa nell'argomento `$aws/events/certificates/registered/caCertificateID` ed esegua queste operazioni, consulta la sezione sulla [registrazione just-in-time](#).

Disattivazione del certificato CA

Quando registri un certificato del dispositivo, AWS IoT controlla se lo stato del certificato CA associato è `ACTIVE`. Se il certificato CA è `INACTIVE`, AWS IoT non permette la registrazione del certificato del dispositivo. Contrassegnando il certificato CA come `INACTIVE`, impedisce la registrazione nel tuo account di

qualsiasi nuovo certificato del dispositivo rilasciato dalla CA compromessa. Puoi usare l'API `update-ca-certificate` per disattivare il certificato CA:

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

Note

Qualsiasi certificato del dispositivo registrato che sia stato firmato dal certificato CA compromesso continuerà a funzionare finché non lo revochi esplicitamente.

Usa l'API `ListCertificatesByCA` per ottenere un elenco di tutti i certificati dei dispositivi registrati che sono stati firmati dalla CA compromessa. Per ogni certificato del dispositivo firmato dal certificato CA compromesso, usa l'API `UpdateCertificate` per revocare il certificato del dispositivo in modo da impedirne l'uso.

Revoca del certificato del dispositivo

Se rilevi un'attività sospetta in un certificato del dispositivo registrato, puoi usare l'API `update-certificate` per revocarlo:

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

Se si verificano errori o eccezioni durante la registrazione automatica dei certificati dei dispositivi, AWS IoT invia eventi o messaggi ai log in CloudWatch Logs. Per ulteriori informazioni sulla configurazione dei log per il tuo account, consulta la [documentazione di Amazon CloudWatch](#).

Utenti, gruppi e ruoli IAM

Gli utenti, i gruppi e i ruoli IAM sono dei sistemi standard per la gestione dell'identità e dell'autenticazione in AWS. Puoi usarli per connetterti alle interfacce HTTP di AWS IoT usando l'SDK e l'interfaccia a riga di comando di AWS.

I ruoli IAM permettono a AWS IoT anche di accedere ad altre risorse AWS nel tuo account per tuo conto. Ad esempio, se vuoi che un dispositivo pubblico il proprio stato in una tabella DynamoDB, i ruoli IAM permettono a AWS IoT di interagire con Amazon DynamoDB. Per ulteriori informazioni, consulta la sezione relativa ai [ruoli IAM](#).

Per le connessioni del broker di messaggi tramite HTTP, AWS IoT autentica gli utenti, i gruppi e i ruoli IAM tramite il processo di firma Signature Version 4. Per informazioni, consulta la pagina sulla [firma di richieste API AWS](#).

Se usi AWS Signature Version 4 con AWS IoT, è necessario che i client supportino quanto indicato di seguito nell'implementazione TLS:

- TLS 1.2, TLS 1.1, TLS 1.0.
- Convalida della firma dei certificati SHA-256 RSA.
- Uno dei pacchetti di crittografia indicati nella sezione relativa ai pacchetti di crittografia TLS supportati.

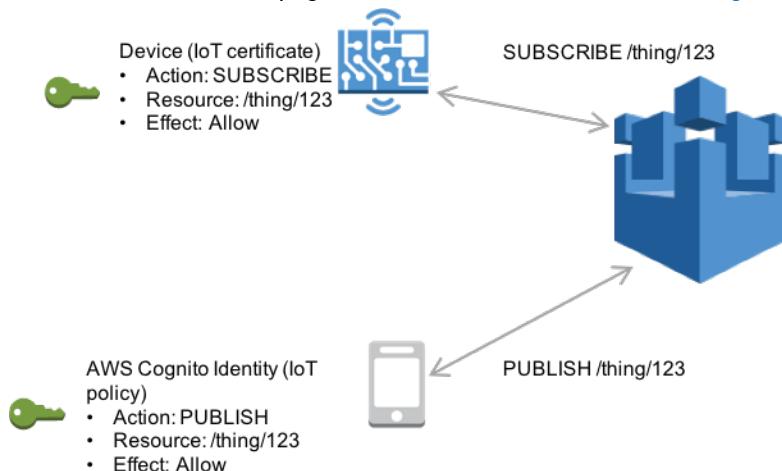
Per ulteriori informazioni, consulta la [Guida per l'utente di IAM](#).

Identità di Amazon Cognito

Un'identità di Amazon Cognito ti permette di usare il tuo provider di identità o altri provider di identità tra i più diffusi, tra cui Login with Amazon, Facebook o Google. Dovrai scambiare un token del provider di

identità per le credenziali di sicurezza AWS. Le credenziali rappresentano un ruolo IAM e possono essere usate con AWS IoT.

È possibile collegare una policy AWS IoT a un'identità di Amazon Cognito utilizzando l'API [AttachPrincipalPolicy](#) e concedere autorizzazioni granulari a un singolo utente dell'applicazione AWS IoT. In questo modo, puoi assegnare autorizzazioni tra clienti specifici e i rispettivi dispositivi. Per ulteriori informazioni, consulta la pagina relativa alle [identità di Amazon Cognito](#).



Autenticazione personalizzata

AWS IoT ti permette di definire autorizzazioni ad hoc per la gestione della tua strategia di autenticazione e autorizzazione tramite un servizio di autenticazione personalizzato e una funzione Lambda. Le autorizzazioni ad hoc permettono a AWS IoT di autenticare i dispositivi e autorizzare le operazioni tramite strategie di autenticazione e autorizzazione con token di connessione.

Quando viene stabilita una connessione HTTP (e questa facoltativamente viene aggiornata a una connessione WebSocket) e non sono presenti intestazioni Signature Version 4, il gateway dei dispositivi AWS IoT verifica se è configurata un'autorizzazione ad hoc per l'endpoint e, in tal caso, la utilizza per autenticare la connessione e autorizzare il dispositivo. Le autorizzazioni ad hoc possono implementare diverse strategie di autenticazione (ad esempio la verifica JWT, la chiamata del provider OAuth e così via) e devono restituire documenti di policy che vengono usati dal gateway dei dispositivi per autorizzare le operazioni MQTT.

Autorizzazioni ad hoc

Le autorizzazioni ad hoc sono costituite dagli elementi seguenti:

Nome

Stringa arbitraria univoca che identifica le autorizzazioni.

ARN della funzione Lambda

ARN di una funzione Lambda che implementa la logica di autenticazione e restituisce le policy di autorizzazione.

Chiavi pubbliche

Chiave pubblica di una coppia di chiavi usata per impedire chiamate non autorizzate alla funzione Lambda delle autorizzazioni.

Usa questo comando per generare una coppia di chiavi:

```
openssl genrsa  
          -out myKeyPair.pem 2048
```

Usa questo comando per estrarre la chiave pubblica dalla coppia di chiavi:

```
openssl rsa -in myKeyPair.pem  
          -pubout > mykey.pub
```

Nome della chiave dei token

Nome della chiave usato per estrarre token dalle intestazioni delle connessioni WebSocket.

La logica che esegue l'autenticazione viene implementata in una funzione Lambda.

Note

L'uso di AWS Lambda viene [fatturato](#). Per ulteriori informazioni su Lambda, consulta [AWS Lambda Developer Guide](#).

Questa funzione usa un token presentato da un dispositivo, autentica il dispositivo e restituisce le informazioni seguenti:

isAuthenticated

Valore booleano che indica se il token è stato autenticato. Se è `false`, gli altri campi della risposta devono essere ignorati.

principalId

Entità principale che riceve l'autorizzazione.

policyDocuments

Elenco di policy che specifica le operazioni che possono essere eseguite dal token di connessione.

DisconnectAfterInSecs

Periodo di tempo, in secondi, durante il quale tenere aperta la connessione WebSocket.

RefreshAfterInSecs

Periodo di tempo, in secondi, dopo il quale la funzione Lambda viene richiamata per aggiornare le policy.

Context

Ulteriori informazioni derivate dopo la convalida del token. Queste informazioni sono rese disponibili nelle [istruzioni SQL del motore di regole AWS IoT](#) e nelle [variabili delle policy IAM/AWS IoT](#).

Occorre concedere l'autorizzazione all'entità principale del servizio AWS IoT per richiamare la funzione Lambda che implementa la logica di autenticazione/autorizzazione personalizzata. A questo scopo, puoi eseguire il comando dell'interfaccia a riga di comando seguente:

```
aws lambda add-permission --function-name <lambda_function_name>  
          --statement-id <unique_identifier_string>  
          --action 'lambda:InvokeFunction'  
          --principal iot.amazonaws.com  
          --source-arn arn:aws:iot:<your-aws-region>:<account_id>:authorizer/<authorizer-name>
```

function-name

Il nome della funzione Lambda a cui stai concedendo l'autorizzazione per la chiamata.

statement-id

Un identificatore di istruzione

action

L'operazione Lambda cui stai concedendo l'autorizzazione di esecuzione.

principal

Il principale cui stai concedendo l'autorizzazione.

source-arn

L'ARN dell'autorizzazione personalizzata; specificando questo valore garantisci che la funzione Lambda può essere richiamata solo dalle autorizzazioni ad hoc desiderate.

Per ulteriori informazioni su come concedere l'autorizzazione per richiamare le funzioni Lambda, consulta la pagina relativa alle [autorizzazioni AWS Lambda](#).

Puoi impostare autorizzazioni predefinite da usare quando le informazioni sulle autorizzazioni non sono incluse in una richiesta di connessione:

```
aws iot set-default-authorizer --authorizer-name <my-authorizer>
```

Configurazione di autorizzazioni ad hoc

1. Creare una funzione Lambda che implementi la logica di autenticazione/autorizzazione (ad esempio, `MyAuthorizerFunction` nella fase seguente). Di seguito è riportato un esempio del risultato che può essere restituito da un'autorizzazione personalizzata di una funzione Lambda:

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

Il valore restituito dalla funzione Lambda deve essere simile ai valori indicati qui sopra. Può essere un oggetto JSON serializzato o non serializzato.

2. Registrare le autorizzazioni ad hoc con AWS IoT tramite l'API `create-authorizer`.

```
aws iot create-authorizer --authorizer-name MyAuthorizer
--authorizer-function-arn arn:aws:lambda:us-
west-2:<account_id>:function:MyAuthorizerFunction // Lambda ARN
```

```
--token-key-name MyAuthorizerToken // Key use to
extract token from headers
--token-signing-public-keys FIRST_KEY= // Public key used
to verify token signature
"----BEGIN PUBLIC KEY----
[...insert your public key here...]
----END PUBLIC KEY----"
--status ACTIVE // Authorizer
status - must be ACTIVE
--region us-west-2 // AWS region
--endpoint https://us-west-2.iot.amazonaws.com // IoT endpoint
```

L'API `test-invoke-authorizer` può essere utilizzata per testare se la funzione Lambda delle autorizzazioni ad hoc è stata configurata correttamente, come illustrato:

```
aws iot test-invoke-authorizer --authorizer-name <NAME_OF_AUTHORIZER> --token
<TOKEN_VALUE> --token-signature <TOKEN_SIGNATURE>
```

Note

`<TOKEN_SIGNATURE>` deve essere firmato con la chiave privata della coppia di chiavi pubblica/privata caricata su AWS IoT utilizzata nella chiamata `create-authorizer`. Un metodo di creazione di `<TOKEN_SIGNATURE>` in locale da una riga di comando di tipo UNIX è il seguente:

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

È necessario tagliare tutti i caratteri di nuova riga dal risultato del comando precedente prima di trasferire il valore `<TOKEN_SIGNATURE>` all'API `test-invoke-authorizer`.

Flusso di lavoro delle autorizzazioni ad hoc

Per effettuare l'autenticazione sul gateway dei dispositivi AWS IoT tramite autorizzazioni ad hoc, il dispositivo necessita di un token e una firma usati da AWS per convalidare i token prima di richiamare le autorizzazioni.

Quando un dispositivo tenta di connettersi a AWS IoT, invia le informazioni seguenti nelle intestazioni HTTP:

- Token generato dal tuo servizio di autenticazione.
- Firma generata dal tuo servizio di autenticazione.
- Autorizzazioni usate per autenticare il token. Se omesse, vengono usate le autorizzazioni predefinite.

Di seguito viene mostrata una richiesta HTTP di esempio per la connessione a AWS IoT tramite il protocollo WebSocket.

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

```
sec-WebSocket-Version: <websocket version>
```

In questo esempio l'intestazione `x-amz-customauthorizer-name` specifica le autorizzazioni ad hoc da usare, l'intestazione `x-amz-customauthorizer-signature` contiene la firma digitale usata per verificare il token e `token-key-name` è il nome della chiave dei token specificato dal parametro `-token-key-name` passato all'API `create-authorizer`.

Note

Alcuni browser web potrebbero non supportare intestazioni HTTP personalizzate.

Il gateway dei dispositivi AWS IoT convalida la firma digitale e, se valida, richiama le autorizzazioni specificate. Di seguito viene mostrato un payload di esempio inviato da AWS IoT alla funzione Lambda dell'autenticazione personalizzata.

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

L'autorizzazione convalida il token e restituisce un ID entità principale, la policy AWS IoT/IAM associata e le informazioni time-to-live (TTL) per la connessione.

Di seguito viene mostrato un esempio di risposta da autorizzazioni ad hoc.

```
{  
  "isAuthenticated": true,  
  "principalId": "xxxxxxxxxx",  
  "disconnectAfterInSeconds": 86400,  
  "refreshAfterInSeconds": 300,  
  "policyDocuments": [  
    {"Version": "2012-10-17", "Statement": [ {"Action": "...", "Effect": "Allow/Deny", "Resource": "..." } ] }  
  ]  
}
```

Il valore restituito dalla funzione Lambda deve essere simile a quello indicato sopra e può essere un oggetto JSON serializzato o non serializzato.

Il gateway dei dispositivi AWS IoT stabilisce quindi una connessione WebSocket. AWS IoT memorizza nella cache le policy associate all'entità principale in modo che le chiamate successive possano essere autorizzate senza dover ripetere l'autenticazione del dispositivo. Qualsiasi errore restituito durante l'autenticazione personalizzata comporta un errore di autenticazione e la chiusura della connessione.

Per un esempio end-to-end di questo flusso di lavoro, consulta [Come usare i sistemi Identity and Access Management per controllare l'accesso alle risorse AWS IoT](#).

Autorizzazione

Le policy determinano che cosa può fare un'identità autenticata. Un'identità autenticata viene usata da dispositivi, applicazioni per dispositivi mobili, applicazioni Web e applicazioni desktop. Un'identità autenticata può essere anche un utente che digita i comandi dell'interfaccia a riga di comando di AWS IoT. L'identità può eseguire operazioni AWS IoT solo se dispone di una policy che concede l'autorizzazione.

Entrambe le policy AWS IoT e IAM vengono usate con AWS IoT per controllare le operazioni che un'identità (chiamata anche entità principale) può eseguire. Il tipo di policy usato dipende dal tipo di identità

che usi per eseguire l'autenticazione con AWS IoT. La tabella seguente mostra i tipi di identità, i protocolli usati da ciascuno e i tipi di policy che possono essere usati per l'autorizzazione.

Le operazioni AWS IoT sono divise in due gruppi:

- L'API control-plane ti permette di eseguire attività di amministrazione come la creazione o l'aggiornamento di certificati, oggetti, regole e così via.
- L'API data-plane ti permette di inviare e ricevere dati da e verso AWS IoT.

Il tipo di policy usato dipende dall'API in uso, control-plane o data-plane.

API data-plane e tipi di policy AWS IoT

| Protocollo e meccanismo di autenticazione | SDK | Tipo di identità | Tipo di policy | | |
|--|-----------------------|--|--|--|--|
| MQTT tramite autenticazione reciproca (porta 8883 o 443 [†] (p. 239)) | AWS IoTKit Device SDK | Certificati X.509 | Policy AWS IoT | | |
| MQTT tramite WebSocket (porta 443) | SDK AWS Mobile | Identità di Amazon Cognito, IAM o federata | Policy AWS IoT per identità di Amazon Cognito Policy IAM per altre identità | | |
| HTTP tramite autenticazione del server (porta 443) | AWS CLI | Identità di Amazon Cognito, IAM o federata | Policy AWS IoT per identità di Amazon Cognito Policy IAM per altre identità | | |
| HTTP tramite autenticazione reciproca (porta 8443) | Nessun SDK supportato | Certificati X.509 | Policy AWS IoT | | |

API control-plane e tipi di policy AWS IoT

| Protocollo e meccanismo di autenticazione | SDK | Tipo di identità | Tipo di policy | | |
|--|---------|--|--|--|--|
| HTTP tramite autenticazione del server (porta 443) | AWS CLI | Identità di Amazon Cognito, IAM o federata | Policy AWS IoT per identità di Amazon Cognito Policy IAM per altre identità | | |

Le policy AWS IoT sono associate a certificati X.509 o a identità di Amazon Cognito. Le policy IAM sono associate a un utente, gruppo o ruolo IAM. Se usi la console AWS IoT o l'interfaccia a riga di comando di AWS IoT per collegare la policy (a un certificato o a Identità di Amazon Cognito), dovrà usare una policy AWS IoT. Altrimenti, puoi usare una policy IAM.

L'autorizzazione basata sulle policy è uno strumento potente Ti offre il controllo completo sulle operazioni che dispositivi, utenti o applicazioni possono eseguire in AWS IoT. Ad esempio, immagina che un dispositivo si connetta a AWS IoT con un certificato. Puoi permettere al dispositivo di accedere a tutti gli argomenti MQTT oppure puoi limitarne l'accesso a un singolo argomento. In un altro esempio supponi che un utente digiti comandi nella riga di comando. Tramite una policy, puoi concedere o negare l'accesso a qualsiasi comando o risorsa AWS IoT per l'utente. Puoi inoltre controllare l'accesso di un'applicazione alle risorse AWS IoT.

Policy AWS IoT

Le policy AWS IoT sono documenti JSON. Seguono le stesse convenzioni delle policy IAM. AWS IoT supporta le policy denominate in modo tale che molte identità possano fare riferimento allo stesso documento di policy. Le policy denominate hanno più versioni in modo da semplificare il rollback.

AWS IoT definisce una serie di operazioni di policy che descrive le operazioni e le risorse a cui puoi concedere o negare l'accesso. Ad esempio:

- `iot:Connect` rappresenta l'autorizzazione a connettersi al broker di messaggi AWS IoT.
- `iot:Subscribe` rappresenta l'autorizzazione a sottoscrivere un argomento o un filtro di argomenti MQTT.
- `iot:GetThingShadow` rappresenta l'autorizzazione a ottenere una copia shadow di un dispositivo.

Le policy AWS IoT ti permettono di controllare l'accesso al piano dei dati AWS IoT. Il piano dei dati AWS IoT è costituito dalle operazioni che ti permettono di connetterti al broker di messaggi AWS IoT, inviare e ricevere messaggi MQTT e ottenere o aggiornare copie shadow dei dispositivi. Per ulteriori informazioni, consulta [Operazioni di policy AWS IoT \(p. 199\)](#).

Una policy AWS IoT è un documento JSON che contiene una o più dichiarazioni di policy. Ogni dichiarazione contiene un elemento `Effect`, un elemento `Action` e un elemento `Resource`. L'elemento `Effect` specifica se l'operazione sarà permessa o negata. L'elemento `Action` specifica l'operazione permessa o negata dalla policy. L'elemento `Resource` specifica la risorsa o le risorse in cui l'operazione è permessa o negata.

registered devices (1)

Per i dispositivi registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con un ID client che corrisponde al nome dell'oggetto e limita il dispositivo alla pubblicazione su un argomento MQTT specifico di ID client/nome argomento. Affinché una connessione venga stabilita, il nome dell'oggetto deve essere registrato nel registro AWS IoT ed essere autenticato utilizzando un'identità/principale collegata all'oggetto:

```
{  
    "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}"]  
        }  
    ]  
}
```

```
        "Resource": [ "arn:aws:iot:us-east-1:123456789012:client/ ${iot:Connection.Thing.ThingName}" ]
    }
}
```

unregistered devices (1)

Per i dispositivi non registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con un ID client `client1` e limita il dispositivo alla pubblicazione su un argomento MQTT specifico per ID client.

```
{
  "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" ]
    }
  ]
}
```

Operazioni di policy AWS IoT

Le operazioni di policy seguenti sono definite da AWS IoT:

Operazioni di policy MQTT

iot:Connect

Rappresenta l'autorizzazione a connettersi al broker di messaggi AWS IoT. L'autorizzazione `iot:Connect` viene controllata ogni volta che viene inviata una richiesta CONNECT al broker. Il broker di messaggi non permette a due client con lo stesso ID client di restare connessi contemporaneamente. Dopo la connessione del secondo client, il broker rileva la situazione e disconnette uno dei client. L'autorizzazione `iot:Connect` può essere usata per garantire che solo i client autorizzati possano connettersi usando un ID client specifico.

iot:Publish

Rappresenta l'autorizzazione a pubblicare in un argomento MQTT. Questa autorizzazione viene controllata ogni volta che viene inviata una richiesta PUBLISH al broker. Questa può essere usata per permettere ai client di pubblicare in modelli di argomento specifici.

Note

Devi concedere anche l'autorizzazione `iot:Connect` per concedere l'autorizzazione `iot:Publish`.

iot:Receive

Rappresenta l'autorizzazione a ricevere un messaggio da AWS IoT. L'autorizzazione `iot:Receive` viene controllata ogni volta che viene recapitato un messaggio a un client. Poiché questa autorizzazione viene controllata a ogni recapito, può essere usata per revocare le autorizzazioni ai client che hanno attualmente sottoscritto un argomento.

iot:Subscribe

Rappresenta l'autorizzazione a sottoscrivere un filtro di argomenti. Questa autorizzazione viene controllata ogni volta che viene inviata una richiesta SUBSCRIBE al broker. Questa può essere usata per permettere ai client di sottoscrivere argomenti corrispondenti a modelli di argomento specifici.

Note

Devi concedere anche l'autorizzazione `iot:Connect` per concedere l'autorizzazione `iot:Subscribe`.

Operazioni di policy per le copie shadow

iot:DeleteThingShadow

Rappresenta l'autorizzazione a eliminare una copia shadow di un dispositivo. L'autorizzazione `iot:DeleteThingShadow` viene controllata ogni volta che viene effettuata una richiesta di eliminazione dei contenuti della copia shadow.

iot:GetThingShadow

Rappresenta l'autorizzazione a recuperare una copia shadow di un dispositivo. L'autorizzazione `iot:GetThingShadow` viene controllata ogni volta che viene effettuata una richiesta di recupero dei contenuti della copia shadow.

iot:UpdateThingShadow

Rappresenta l'autorizzazione ad aggiornare una copia shadow di un dispositivo. L'autorizzazione `iot:UpdateThingShadow` viene controllata ogni volta che viene effettuata una richiesta di aggiornamento dei contenuti della copia shadow.

Note

La policy sull'esecuzione delle operazioni si applica solo all'endpoint TLS HTTP. Se utilizzi l'endpoint MQTT devi utilizzare le operazioni di policy MQTT definite in questo argomento.

Operazioni di policy relative all'esecuzione dei processi

iot:DescribeJobExecution

Rappresenta l'autorizzazione a recuperare l'esecuzione di un processo per un dato oggetto. L'autorizzazione `iot:DescribeJobExecution` viene controllata ogni volta che viene richiesto di ottenere l'esecuzione di un processo.

iot:GetPendingJobExecutions

Rappresenta l'autorizzazione a recuperare l'elenco dei processi che non si trovano in uno stato terminale per un oggetto. L'autorizzazione `iot:GetPendingJobExecutions` viene controllata ogni volta che viene effettuata una richiesta di recupero dell'elenco.

iot:UpdateJobExecution

Rappresenta l'autorizzazione ad aggiornare l'esecuzione di un processo. L'autorizzazione `iot:UpdateJobExecution` viene controllata ogni volta che viene effettuata una richiesta di aggiornamento dell'esecuzione di un processo.

iot:StartNextPendingJobExecution

Rappresenta l'autorizzazione a ottenere e avviare la successiva esecuzione in sospeso di un processo per un oggetto (ossia, per aggiornare l'esecuzione di un processo con stato QUEUED o

da IN_PROGRESS a IN_PROGRESS). L'autorizzazione `iot:StartNextPendingJobExecution` viene controllata ogni volta che viene effettuata una richiesta di avvio della successiva esecuzione in sospeso di un processo.

Risorse per operazioni

Per specificare una risorsa per un'operazione di policy AWS IoT, devi usare l'ARN della risorsa. Tutti gli ARN di risorsa hanno il formato seguente:

```
arn:aws:iot:<region>:<AWS account ID>:<resource type>/<resource name>
```

La tabella seguente mostra la risorsa da specificare per ogni tipo di operazione:

| Action | Resource |
|---|--|
| <code>iot:DeleteThingShadow</code> | ARN di un oggetto – arn:aws:iot:us-east-1:123456789012:thing/thingOne |
| <code>iot:Connect</code> | ARN di un ID client – arn:aws:iot:us-east-1:123456789012:client/myClientId |
| <code>iot:Publish</code> | ARN di un argomento – arn:aws:iot:us-east-1:123456789012:topic/myTopicName |
| <code>iot:Subscribe</code> | ARN di un filtro di argomenti – arn:aws:iot:us-east-1:123456789012:topicfilter/myTopicFilter |
| <code>iot:Receive</code> | ARN di un argomento – arn:aws:iot:us-east-1:123456789012:topic/myTopicName |
| <code>iot:UpdateThingShadow</code> | ARN di un oggetto – arn:aws:iot:us-east-1:123456789012:thing/thingOne |
| <code>iot:GetThingShadow</code> | ARN di un oggetto – arn:aws:iot:us-east-1:123456789012:thing/thingOne |
| <code>iot:DescribeJobExecution</code> | ARN di un oggetto – arn:aws:iot:us-east-1:123456789012:thing/thingOne |
| <code>iot:GetPendingJobExecutions</code> | ARN di un oggetto – arn:aws:iot:us-east-1:123456789012:thing/thingOne |
| <code>iot:UpdateJobExecution</code> | ARN di un oggetto – arn:aws:iot:us-east-1:123456789012:thing/thingOne |
| <code>iot:StartNextPendingJobExecution</code> | ARN di un oggetto – arn:aws:iot:us-east-1:123456789012:thing/thingOne |

Variabili delle policy AWS IoT

AWS IoT definisce le variabili delle policy che possono essere usate nelle policy AWS IoT all'interno del blocco di risorse o condizioni. Quando una policy viene valutata, le variabili vengono sostituite dai valori effettivi. Ad esempio, se un dispositivo si è connesso al broker di messaggi AWS IoT con l'ID client "100-234-3456", la variabile di policy `iot:ClientId` sarà sostituita con "100-234-3456" nel documento della policy. Per ulteriori informazioni sulle variabili delle policy, consulta le sezioni relative alle [variabili delle policy IAM](#) e alle [condizioni con più valori](#).

Variabili delle policy di base

AWS IoT definisce le variabili delle policy di base seguenti:

- **iot:ClientId**: ID client usato per la connessione al broker di messaggi AWS IoT.
- **aws:SourceIp**: indirizzo IP del client connesso al broker di messaggi AWS IoT.

La policy AWS IoT seguente mostra l'uso delle variabili delle policy:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": ["iot:Connect"],  
            "Resource": [  
                "arn:aws:iot:us-east-1:123451234510:client/${iot:ClientId}"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": ["iot:Publish"],  
            "Resource": [  
                "arn:aws:iot:us-east-1:123451234510:topic/my/topic/${iot:ClientId}"  
            ]  
        }  
    ]  
}
```

In questi esempi, \${iot:ClientId} viene sostituito dall'ID del client connesso al broker di messaggi AWS IoT quando la policy viene valutata. Quando usi variabili delle policy come \${iot:ClientId}, puoi aprire inavvertitamente l'accesso ad argomenti indesiderati. Ad esempio, se usi una policy che usa \${iot:ClientId} per specificare un filtro di argomenti:

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

Un client può connettersi usando + come ID client. Questo permette all'utente di sottoscrivere qualsiasi argomento corrispondente al filtro di argomenti my/+topic. Per evitare problemi di sicurezza di questo tipo, usa l'operazione di policy iot:Connect per controllare gli ID client che possono connettersi. Ad esempio, questa policy permette di connettersi solo ai client il cui ID client è clientid1:

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

Variabili delle policy di certificato X.509

Le variabili delle policy del certificato X.509 ti permettono di scrivere policy AWS IoT che concedono autorizzazioni in base agli attributi dei certificati X.509. Le sezioni seguenti descrivono come usare queste variabili delle policy di certificato.

Variabili delle policy di oggetto

Le variabili delle policy di oggetto ti permettono di scrivere policy AWS IoT che concedono o negano autorizzazioni in base alle proprietà degli oggetti, come nomi di oggetto, tipi di oggetto e valori degli attributi di oggetto. Il nome dell'oggetto viene ottenuto dall'ID client nel messaggio MQTT Connect inviato quando un oggetto si connette a AWS IoT. Le variabili delle policy di oggetto vengono sostituite quando un oggetto si connette a AWS IoT tramite MQTT con autenticazione reciproca TLS o tramite MQTT con protocollo WebSocket e identità di Amazon Cognito autenticate. Le variabili delle policy di oggetto vengono sostituite anche quando un certificato o un'identità di Amazon Cognito autenticata viene collegato a un oggetto. Puoi usare l'API [AttachThingPrincipal](#) per collegare certificati e identità di Amazon Cognito autenticate a un oggetto.

Sono disponibili le variabili delle policy di oggetto seguenti:

- `iot:Connection.Thing.ThingName`
- `iot:Connection.Thing.ThingTypeName`
- `iot:Connection.Thing.Attributes[attributeName]`
- `iot:Connection.Thing.IsAttached`

`iot:Connection.Thing.ThingName`

Questo risolve il nome dell'oggetto nel registro AWS IoT per cui la policy viene valutata. AWS IoT usa il certificato presentato dal dispositivo quando esegue l'autenticazione per determinare quale oggetto utilizzare per verificare la connessione. Questa variabile di policy è disponibile solo quando un dispositivo si connette tramite MQTT o MQTT con protocollo WebSocket.

`iot:Connection.Thing.ThingTypeName`

Questa variabile restituisce il tipo di oggetto associato all'oggetto per cui viene valutata la policy. Il nome dell'oggetto viene impostato sull'ID client della connessione MQTT/WebSocket. Il nome del tipo di oggetto viene ottenuto da una chiamata all'API [DescribeThing](#). Questa variabile di policy è disponibile solo per connessioni tramite MQTT o MQTT con protocollo WebSocket.

`iot:Connection.Thing.Attributes[NomeAttributo]`

Questa variabile restituisce il valore dell'attributo specificato associato all'oggetto per cui viene valutata la policy. A un oggetto possono essere associati fino a 50 attributi. Ogni attributo è disponibile come variabile di policy: `iot:Connection.Thing.Attributes[attributeName]`, dove `NomeAttributo` è il nome dell'attributo. Il nome dell'oggetto viene impostato sull'ID client della connessione MQTT/WebSocket. Questa variabile di policy è disponibile solo per connessioni tramite MQTT o MQTT con protocollo WebSocket.

`iot:Connection.Thing.IsAttached`

Questo viene risolto in `true` se il certificato o l'identità Amazon Cognito per cui viene valutata la policy è collegato a un oggetto IoT. È possibile utilizzare questa variabile per evitare che un dispositivo si connetta a AWS IoT se presenta un certificato che non è collegato a un oggetto IoT nel registro AWS IoT.

Attributi dell'autorità emittente

Le variabili delle policy AWS IoT seguenti ti permettono di concedere o negare autorizzazioni in base agli attributi di certificato impostati dall'autorità di certificazione.

- 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

Attributi di oggetto

Le variabili delle policy AWS IoT seguenti ti permettono di concedere o negare autorizzazioni in base agli attributi di oggetto dei certificati impostati dall'autorità di certificazione.

- 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

I certificati X.509 permettono a questi attributi di contenere uno o più valori. Per impostazione predefinita, le variabili delle policy per ogni attributo con più valori restituiscono il primo valore. Ad esempio, l'attributo Certificate.Subject.Country potrebbe contenere un elenco di nomi di paese, ma quando viene valutato in una policy, iot:Certificate.Subject.Country viene sostituito con il nome del primo paese. Puoi richiedere un valore di attributo specifico diverso dal primo usando un indice a base zero. Ad esempio, iot:Certificate.Subject.Country.1 viene sostituito dal secondo nome di paese nell'attributo Certificate.Subject.Country. Se specifichi un valore di indice che non esiste, ad esempio se richiedi un terzo valore quando all'attributo ne sono assegnati solo due, non viene eseguita alcuna sostituzione e l'autorizzazione non riesce. Puoi anche usare il suffisso .List nel nome di variabile della policy per specificare tutti i valori dell'attributo.

registered devices (2)

Per i dispositivi registrati come oggetti nel registro AWS IoT, la seguente policy consente ai client con un nome dell'oggetto registrato nel registro AWS IoT di connettersi, ma limita il diritto di pubblicazione in un argomento specifico del nome dell'oggetto a quei client che dispongono di certificati il cui attributo Certificate.Subject.Organization è impostato su "Example Corp" o "AnyCompany".

Questa limitazione è ottenuta utilizzando un campo "Condition" che specifica una condizione che deve essere soddisfatta per consentire l'operazione precedente. In questo caso, la condizione è che l'attributo `Certificate.Subject.Organization` associato al certificato deve includere uno dei valori elencati:

```
{  
    "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}"  
            ],  
            "Condition": {  
                "ForAllValues:StringEquals": {  
                    "iot:Certificate.Subject.Organization.List": [  
                        "Example Corp",  
                        "AnyCompany"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

unregistered devices (2)

Per i dispositivi non registrati come oggetti nel registro AWS IoT, la seguente policy concede l'autorizzazione per connettersi a AWS IoT con ID client `client1`, `client2` e `client3`, ma limita il diritto di pubblicazione in un argomento specifico dell'ID client a quei client che dispongono di certificati il cui attributo `Certificate.Subject.Organization` è impostato su "Example Corp" o "AnyCompany". Questa limitazione è ottenuta utilizzando un campo "Condition" che specifica una condizione che deve essere soddisfatta per consentire l'operazione precedente. In questo caso, la condizione è che l'attributo `Certificate.Subject.Organization` associato al certificato deve includere uno dei valori elencati:

```
{  
    "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/my/topic/${iot:ClientId}"  
    ],  
    "Condition": {  
        "ForAllValues:StringEquals": {  
            "iot:Certificate.Subject.Organization.List": [  
                "Example Corp",  
                "AnyCompany"  
            ]  
        }  
    }  
}
```

Attributi dei nomi alternativi dell'autorità emittente

Le variabili delle policy AWS IoT seguenti ti permettono di concedere o negare autorizzazioni in base agli attributi dei nomi alternativi dell'autorità emittente impostati dall'autorità di certificazione.

- `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`

Attributi dei nomi alternativi di oggetto

Le variabili delle policy AWS IoT seguenti ti permettono di concedere o negare autorizzazioni in base agli attributi dei nomi alternativi di oggetto impostati dall'autorità di certificazione.

- `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`

Altri attributi

Puoi usare `iot:Certificate.SerialNumber` per concedere o negare l'accesso alle risorse AWS IoT in base al numero di serie di un certificato. La variabile di policy `iot:Certificate.AvailableKeys` contiene il nome di tutte le variabili delle policy di certificato che contengono valori.

Limitazioni per le variabili delle policy di certificato X.509

Alle variabili delle policy di certificato X.509 si applicano le limitazioni seguenti:

Caratteri jolly

Se negli attributi di certificato sono presenti caratteri jolly, la variabile della policy non viene sostituita dal valore dell'attributo di certificato, lasciando il testo `#{policy-variable}` nel documento della policy. Questo comportamento può provocare un errore di autenticazione.

Campi di matrice

Gli attributi di certificato che contengono matrici sono limitati a cinque elementi. Gli elementi aggiuntivi vengono ignorati.

Lunghezza delle stringhe

Tutti i valori di stringa sono limitati a 1024 caratteri. Se un attributo di certificato contiene una stringa più lunga di 1024 caratteri, la variabile della policy non viene sostituita dal valore dell'attributo di certificato, lasciando il testo \${policy-variable} nel documento della policy. Questo comportamento può provocare un errore di autenticazione.

Policy di esempio

Le policy AWS IoT sono specificate in un documento JSON. Di seguito sono elencati i componenti di una policy AWS IoT:

Versione

Deve essere impostato su "2012-10-17".

Effetto

Deve essere impostato su "Allow" o "Deny".

Operazione

Deve essere impostato su "iot:*nome-operazione*", dove *nome-operazione* è una delle operazioni seguenti:

"iot:Connect": connessione a AWS IoT

"iot:Receive": ricezione di messaggi da AWS IoT

"iot:Publish": pubblicazione MQTT

"iot:Subscribe": sottoscrizione MQTT

"iot:UpdateThingShadow": aggiornamento di una copia shadow di un dispositivo

"iot:GetThingShadow": recupero di una copia shadow di un dispositivo

"iot>DeleteThingShadow": eliminazione di una copia shadow di un dispositivo

Risorsa

Deve essere impostato su uno dei valori seguenti:

Client – arn:aws:iot:*regione:id-account*:client/*id-client*

ARN di un argomento – arn:aws:iot:*regione:id-account*:topic/*nome-argomento*

ARN di un filtro di argomenti – arn:aws:iot:*regione:id-account*:topicfilter/*filtro-argomenti*

Esempi di policy di connessione

La policy seguente concede l'autorizzazione per connettersi a AWS IoT con ID client *client1*:

```
{  
    "Version": "2012-10-17",
```

```
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "iot:Connect"
    ],
    "Resource": [
      "arn:aws:iot:us-east-1:123456789012:client/client1"
    ]
  }
]
```

La policy seguente nega l'autorizzazione a connettersi a AWS IoT con ID client `client1` e `client2`, consentendo invece ai dispositivi di connettersi utilizzando un ID client che corrisponde al nome di un oggetto registrato nel registro AWS IoT:

```
{
  "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}"
      ]
    }
  ]
}
```

Registered devices (3)

La policy seguente concede a un dispositivo l'autorizzazione per connettersi utilizzando il rispettivo nome oggetto come ID client e per effettuare la sottoscrizione al filtro di argomenti `my/topic/filter`. Il dispositivo deve essere registrato con AWS IoT. Quando ci si connette a AWS IoT, il dispositivo deve fornire il certificato associato all'oggetto IoT nel registro AWS IoT:

```
{
  "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:Subscribe"
      ],
      "Resource": [
        "arn:aws:sns:us-east-1:123456789012:myTopic"
      ],
      "Condition": {
        "StringEquals": {
          "aws:encrypted": "false"
        }
      }
    }
  ]
}
```

```
        "Action": [
            "iot:Subscribe"
        ],
        "Resource": [
            "arn:aws:iot:us-east-1:123456789012:topicfilter/my/topic/filter"
        ]
    }
}
```

Unregistered devices (3)

Per i dispositivi non registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi utilizzando l'ID client `client1` e per effettuare la sottoscrizione al filtro di argomenti `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:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topicfilter/my/topic"
            ]
        }
    ]
}
```

Esempi di policy di pubblicazione/sottoscrizione

La policy usata dipende dalla modalità di connessione a AWS IoT. Puoi connetterti a AWS IoT tramite un client MQTT, HTTP o WebSocket. Quando ti connetti con un client MQTT, l'autenticazione viene eseguita con un certificato X.509. Quando ti connetti tramite HTTP o il protocollo WebSocket, l'autenticazione viene eseguita tramite Signature Version 4 e Amazon Cognito.

Policy per client MQTT

Quando specifichi filtri di argomenti nelle policy AWS IoT per client MQTT, i caratteri jolly MQTT "+" e "#" vengono considerati caratteri letterali. Il loro uso può produrre comportamenti imprevisti.

Registered devices (4)

Per i dispositivi registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con l'ID client che corrisponde al nome dell'oggetto e per effettuare la sottoscrizione solo al filtro di argomenti `some/+ topic`:

```
{
    "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:Subscribe"
        ],
        "Resource": [
            "arn:aws:iot:us-east-1:123456789012:topicfilter/some/+/topic"
        ]
    }
]
```

Unregistered devices (4)

Per i dispositivi non registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con l'ID client `client1` e per effettuare la sottoscrizione solo al filtro di argomenti `some/+/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:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topicfilter/some/+/topic"
            ]
        }
    ]
}
```

Note

All'interno di una policy il carattere jolly MQTT "+" non viene considerato come tale, bensì come letterale. I tentativi di effettuare la sottoscrizione a filtri di argomenti che corrispondono al modello `some/+/topic` non riescono e causano la disconnessione del client.

Puoi usare "*" come carattere jolly nell'attributo di risorsa della policy. Ad esempio, se ogni dispositivo nell'account deve pubblicare su un argomento univoco riservato solo per se stesso, utilizza la policy seguente:

Registered devices (5)

Per i dispositivi registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante un ID client che corrisponde al nome dell'oggetto e pubblicare in qualsiasi argomento preceduto dal nome dell'oggetto:

```
{  
    "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/  
${iot:Connection.Thing.ThingName}/*"  
                ]  
            }  
    ]  
}
```

Unregistered devices (5)

Per i dispositivi non registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante l'ID client `client1`, `client2` o `client3` e pubblicare in qualsiasi argomento preceduto dall'ID client:

```
{  
    "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/${iot:ClientId}/*"  
            ]  
        }  
    ]  
}
```

Puoi anche usare il carattere jolly "*" alla fine di un filtro di argomenti. L'utilizzo di caratteri jolly può portare alla concessione di privilegi indesiderati, pertanto devono essere utilizzati solo dopo un'attenta valutazione. Una situazione in cui possono essere utili è quando i dispositivi devono effettuare la sottoscrizione a messaggi con numerosi argomenti diversi, ad esempio se un dispositivo deve effettuare la sottoscrizione ai report inviati dai sensori di temperatura in più ubicazioni.

registered devices (6)

Per i dispositivi registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante il nome dell'oggetto del dispositivo come ID client ed effettuare la sottoscrizione a un argomento preceduto dal nome dell'oggetto, seguito da room, seguito da qualsiasi stringa. È previsto che questi argomenti saranno, ad esempio, thing1/room1, thing1/room2...:

```
{  
    "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:Subscribe"  
            ],  
            "Resource": [  
                "arn:aws:iot:us-east-1:123456789012:topicfilter/  
${iot:Connection.Thing.ThingName}/room*"  
            ]  
        }  
    ]  
}
```

unregistered devices (6)

Per i dispositivi non registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante gli ID client client1, client2, client3 ed effettuare la sottoscrizione a un argomento preceduto dall'ID client, seguito da room, seguito da qualsiasi stringa. È previsto che questi argomenti saranno, ad esempio, client1/room1, client1/room2...:

```
{  
    "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:Subscribe"  
    ],  
    "Resource": [  
        "arn:aws:iot:us-east-1:123456789012:topicfilter/${iot:ClientId}/room*"  
    ]  
}  
]  
}
```

registered devices (7)

Per i dispositivi registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante il nome dell'oggetto del dispositivo come ID client ed effettuare la sottoscrizione agli argomenti `my/topic` e `my/othertopic`:

```
{  
    "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:Subscribe"  
            ],  
            "Resource": [  
                "arn:aws:iot:us-east-1:123456789012:topicfilter/my/topic",  
                "arn:aws:iot:us-east-1:123456789012:topicfilter/my/othertopic"  
            ]  
        }  
    ]  
}
```

unregistered devices (7)

Per i dispositivi non registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante l'ID client `client1` ed effettuare la sottoscrizione agli argomenti `my/topic` e `my/othertopic`:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "iot:Connect"  
            ],  
            "Resource": [  
                "arn:aws:iot:us-east-1:123456789012:client/client1"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "iot:Subscribe"  
            ],  
            "Resource": [  
                "arn:aws:iot:us-east-1:123456789012:topicfilter/my/topic",  
                "arn:aws:iot:us-east-1:123456789012:topicfilter/my/othertopic"  
            ]  
        }  
    ]  
}
```

```
{  
    "Effect": "Allow",  
    "Action": [  
        "iot:Subscribe"  
    ],  
    "Resource": [  
        "arn:aws:iot:us-east-1:123456789012:topicfilter/my/topic",  
        "arn:aws:iot:us-east-1:123456789012:topicfilter/my/othersTopic"  
    ]  
}  
}
```

registered devices (8)

Per i dispositivi registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante il nome dell'oggetto del dispositivo come ID client ed effettuare la sottoscrizione a un argomento univoco per tale nome dell'oggetto/ID client:

```
{  
    "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:Thing.ThingName}"  
            ]  
        }  
    ]  
}
```

unregistered devices (8)

Per i dispositivi non registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante l'ID client `client1` e pubblicare in un argomento univoco per tale ID client:

```
{  
    "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}"
            ]
        }
    ]
}
```

registered devices (9)

Per i dispositivi registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante il nome dell'oggetto del dispositivo come ID client e pubblicare in qualsiasi argomento preceduto dal nome dell'oggetto/ID client, tranne che per un argomento che termina con bar.

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

unregistered devices (9)

Per i dispositivi non registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante gli ID client `client1` e `client2` e pubblicare in qualsiasi argomento preceduto dall'ID client utilizzato per connettersi, tranne che per un argomento che termina con bar:

```
{
```

```
"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"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "iot:Publish"
        ],
        "Resource": [
            "arn:aws:iot:us-east-1:123456789012:topic/${iot:ClientId}/*"
        ]
    },
    {
        "Effect": "Deny",
        "Action": [
            "iot:Publish"
        ],
        "Resource": [
            "arn:aws:iot:us-east-1:123456789012:topic/${iot:ClientId}/bar"
        ]
    }
]
```

registered devices (10)

Per i dispositivi registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante il nome dell'oggetto del dispositivo come ID client. Il dispositivo può effettuare la sottoscrizione all'argomento `my/topic`, ma non può pubblicare in `<thing-name> /bar` dove `<thing-name>` è il nome dell'oggetto IoT che si connette a AWS IoT:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:client/
${iot:Connection.Thing.ThingName}"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topicfilter/my/topic"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "iot:Publish"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/${iot:Connection.Thing.ThingName}/bar"
            ]
        }
    ]
}
```

```
        "Effect": "Deny",
        "Action": [
            "iot:Publish"
        ],
        "Resource": [
            "arn:aws:iot:us-east-1:123456789012:topic/${iot:Thing.ThingName}/bar"
        ]
    }
}
```

unregistered devices (10)

Per i dispositivi non registrati come oggetti nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT mediante l'ID client `client1` ed effettuare la sottoscrizione all'argomento `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:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topicfilter/my/topic"
            ]
        }
    ]
}
```

Le variabili delle policy di oggetto vengono sostituite anche quando un certificato o un'identità di Amazon Cognito autenticata viene collegato a un oggetto. La policy seguente concede l'autorizzazione per connettersi a AWS IoT con ID client `client1` e pubblicare e ricevere nell'argomento `iotmonitor/provisioning/987654321098`. Consente inoltre al titolare del certificato di effettuare la sottoscrizione a questo stesso argomento.

```
{
    "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",
        "iot:Receive"
    ],
    "Resource": [
        "arn:aws:iot:us-east-1:123456789012:topic/iotmonitor/
provisioning/987654321098"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "iot:Subscribe"
    ],
    "Resource": [
        "arn:aws:iot:us-east-1:123456789012:topicfilter/iotmonitor/
provisioning/987654321098"
    ]
}
]
```

Policy per client HTTP e WebSocket

Per le operazioni seguenti, AWS IoT usa policy AWS IoT collegate a identità di Amazon Cognito (tramite l'API `AttachPolicy`) per ridurre l'ambito delle autorizzazioni collegate al pool di identità di Amazon Cognito con identità autenticate. Questo significa che un'identità di Amazon Cognito deve disporre dell'autorizzazione dalla policy del ruolo IAM collegata al pool e dalla policy AWS IoT collegata all'identità di Amazon Cognito tramite l'API AWS IoT `AttachPolicy`.

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

Note

Per le altre operazioni AWS IoT o per le identità non autenticate, AWS IoT non riduce l'ambito fino alle autorizzazioni collegate al ruolo del pool di identità di Amazon Cognito. Per le identità autenticate e non autenticate, questa è la policy più permissiva che consigliamo di collegare al ruolo del pool Amazon Cognito.

HTTP

Per permettere alle identità di Amazon Cognito non autenticate di pubblicare messaggi tramite HTTP su un argomento specifico per l'identità Cognito, collega la policy seguente al ruolo del pool di identità di Amazon Cognito:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish",
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/iotmonitor/
provisioning/987654321098"
            ]
        }
    ]
}
```

```
        "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/${cognito-  
identity.amazonaws.com:sub}"]  
    }  
}
```

Per consentire utenti autenticati, collega la policy precedente al ruolo del pool di identità di Amazon Cognito e all'identità Cognito utilizzando l'API AWS IoT [AttachPrincipalPolicy](#).

Note

Durante l'autorizzazione delle identità Cognito, AWS IoT considererà entrambe queste policy e concederà i privilegi minimi specificati. Un'operazione è consentita solo se entrambe le policy consentono l'operazione richiesta e se una di tali policy impediscono un'operazione, tale operazione non sarà autorizzata.

MQTT

Per permettere alle identità di Amazon Cognito non autenticate di pubblicare messaggi MQTT tramite WebSocket su un argomento specifico per l'identità Cognito nell'account, collega la policy seguente al ruolo del pool di identità di Amazon Cognito:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "iot:Publish",  
            ],  
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/${cognito-  
identity.amazonaws.com:sub}"]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "iot:Connect",  
            ],  
            "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/${cognito-  
identity.amazonaws.com:sub}"]  
        }  
    ]  
}
```

Per consentire utenti autenticati, collega la policy precedente al ruolo del pool di identità di Amazon Cognito e all'identità Cognito utilizzando l'API AWS IoT [AttachPrincipalPolicy](#).

Note

Durante l'autorizzazione delle identità Cognito, AWS IoT considererà entrambe queste policy e concederà i privilegi minimi specificati. Un'operazione è consentita solo se entrambe le policy consentono l'operazione richiesta e se una di tali policy impediscono un'operazione, tale operazione non sarà autorizzata.

Esempi di policy di ricezione

registered devices (11)

Per i dispositivi registrati nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con un ID client che corrisponde al nome dell'oggetto ed effettuare la sottoscrizione e ricevere messaggi dall'argomento `my/topic`:

```
{
```

```
"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:Subscribe"
        ],
        "Resource": [
            "arn:aws:iot:us-east-1:123456789012:topicfilter/my/topic"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "iot:Receive"
        ],
        "Resource": [
            "arn:aws:iot:us-east-1:123456789012:topic/my/topic"
        ]
    }
]
```

unregistered devices (11)

Per i dispositivi non registrati nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con l'ID client `client1` ed effettuare la sottoscrizione e ricevere messaggi da un solo argomento:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": ["arn:aws:iot:us-east-1:123456789012:client/client1"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topicfilter/my/topic"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Receive"
            ],
            "Resource": [
                "arn:aws:iot:us-east-1:123456789012:topic/my/topic"
            ]
        }
]
```

```
        }
    ]  
}
```

Esempi di policy di certificato

registered devices (12)

Per i dispositivi registrati nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con un ID client che corrisponde a un nome dell'oggetto e pubblicare in un argomento il cui nome è identico al `certificateId` del certificato utilizzato dal dispositivo per effettuare l'autenticazione:

```
{
  "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}"]
    }
  ]
}
```

unregistered devices (12)

Per i dispositivi non registrati nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con l'ID client `client1`, `client2` e `client3` e pubblicare in un argomento il cui nome è identico al `certificateId` del certificato utilizzato dal dispositivo per effettuare l'autenticazione:

```
{
  "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"
      ]
    }
  ]
}
```

```
        "arn:aws:iot:us-east-1:123456789012:client/client3"
    ]
}
}
```

registered devices (13)

Per i dispositivi registrati nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con un ID client che corrisponde al nome dell'oggetto e pubblicare in un argomento il cui nome è identico al campo nome comune del certificato utilizzato dal dispositivo per effettuare l'autenticazione:

```
{
  "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 questo esempio, il nome comune dell'oggetto del certificato viene utilizzato come identificatore dell'argomento, presumendo che il nome comune dell'oggetto sia univoco per ogni certificato registrato. Se i certificati sono condivisi tra più dispositivi, il nome comune dell'oggetto sarà identico per tutti i dispositivi che condividono questo certificato, consentendo pertanto la pubblicazione di privilegi nello stesso argomento da più dispositivi (opzione non consigliata).

unregistered devices (13)

Per i dispositivi non registrati nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con gli ID client `client1`, `client2` e `client3` e pubblicare in un argomento il cui nome è identico al campo del nome comune dell'oggetto del certificato utilizzato dal dispositivo per effettuare l'autenticazione:

```
{
  "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 questo esempio, il nome comune dell'oggetto del certificato viene utilizzato come identificatore dell'argomento, presumendo che il nome comune dell'oggetto sia univoco per ogni certificato registrato. Se i certificati sono condivisi tra più dispositivi, il nome comune dell'oggetto sarà identico per tutti i dispositivi che condividono questo certificato, consentendo pertanto la pubblicazione di privilegi nello stesso argomento da più dispositivi (opzione non consigliata).

registered devices (14)

Per i dispositivi registrati nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con un ID client che corrisponde al nome dell'oggetto e pubblicare in un argomento il cui nome è preceduto da admin/ quando il campo `Subject.CommonName.2` del certificato utilizzato per autenticare il dispositivo è impostato su `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"
                }
            }
        }
    ]
}
```

unregistered devices (14)

Per i dispositivi non registrati nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con ID client `client1`, `client2` e `client3` e pubblicare in un argomento il

cui nome è preceduto da admin/ quando il campo `Subject.CommonName.2` del certificato utilizzato per autenticare il dispositivo è impostato su `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"  
                }  
            }  
        }  
    ]  
}
```

registered devices (15)

Per i dispositivi registrati nel registro AWS IoT, la policy seguente consente a un dispositivo di utilizzare il suo nome dell'oggetto per pubblicare su un argomento specifico costituito da `admin/` seguito da `ThingName` quando uno dei campi `Subject.CommonName` del certificato utilizzato per autenticare il dispositivo è impostato su `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"  
                }  
            }  
        }  
    ]  
}
```

```
        }
    ]  
}
```

unregistered devices (15)

Per i dispositivi non registrati nel registro AWS IoT, la policy seguente concede l'autorizzazione per connettersi a AWS IoT con ID client `client1`, `client2` e `client3` e pubblicare nell'argomento `admin` quando uno qualsiasi dei campi `Subject.CommonName` del certificato utilizzato per autenticare il dispositivo è impostato su `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"
        }
      }
    }
  ]
}
```

Esempi di policy di oggetto

La policy seguente permette a un dispositivo di connettersi se il certificato usato per l'autenticazione con AWS IoT è collegato all'oggetto per cui viene valutata la policy:

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

Policy IoT IAM

AWS Identity and Access Management definisce un'operazione di policy per ogni operazione definita da AWS IoT, tra cui le API control-plane e data-plane.

AWS IoT Autorizzazioni API

Nella tabella seguente vengono elencate le API di AWS IoT, le autorizzazioni IAM necessarie e la risorsa manipolata dall'API.

| API | Autorizzazione necessaria (operazioni di policy) | Risorse |
|---------------------------|--|--|
| AcceptCertificateTransfer | iot:AcceptCertificateTransfer | arn:aws:iot: regione:id-account:cert/id-certificato Note L'account AWS specificato nell'ARN deve essere l'account in cui viene trasferito il certificato. |
| AddThingToThingGroup | iot:AddThingToThingGroup | arn:aws:iot: regione:id-account:thinggroup/nome-gruppo-oggetti arn:aws:iot: regione:id-account:thing/nome-oggetto |
| AssociateTargetsWithJob | iot:AssociateTargetsWithJob | Nessuna |
| AttachPolicy | iot:AttachPolicy | arn:aws:iot: regione:id-account:thinggroup/nome-gruppo-oggetti oppure arn:aws:iot: regione:id-account:cert/id-certificato |
| AttachPrincipalPolicy | iot:AttachPrincipalPolicy | arn:aws:iot: regione:id-account:cert/id-certificato |
| AttachThingPrincipal | iot:AttachThingPrincipal | arn:aws:iot: regione:id-account:cert/id-certificato |
| CancelCertificateTransfer | iot:CancelCertificateTransfer | arn:aws:iot: regione:id-account:cert/id-certificato Note L'account AWS specificato nell'ARN deve essere l'account in cui viene trasferito il certificato. |
| CancelJob | iot:CancelJob | arn:aws:iot: regione:id-account:job/job-id |
| CancelJobExecution | iot:CancelJobExecution | arn:aws:iot: regione:id-account:job/job-id arn:aws:iot: regione:id-account:thing/nome-oggetto |
| ClearDefaultAuthorizer | iot:ClearDefaultAuthorizer | Nessuna |
| CreateAuthorizer | iot>CreateAuthorizer | arn:aws:iot: regione:id-account:authorizer/nome-funzione-autorizzazione |
| CreateCertificateFromCsr | iot>CreateCertificateFromCsr | |

| API | Autorizzazione necessaria (operazioni di policy) | Risorse |
|--------------------------|--|--|
| CreateJob | iot:CreateJob | arn:aws:iot: regione:id-account:job/job-id |
| CreateKeysAndCertificate | iot:CreateKeysAndCertificate | |
| CreatePolicy | iot:CreatePolicy | * |
| CreatePolicyVersion | iot:CreatePolicyVersion | arn:aws:iot: regione:id-account:policy/ nome-policy Note Deve essere una policy AWS IoT e non una policy IAM. |
| CreateRoleAlias | iot:CreateRoleAlias | (parametro: roleAlias) arn:aws:iot: regione:id-account:rolealias/ nome-alias-ruolo |
| CreateThing | iot:CreateThing | arn:aws:iot: regione:id-account:thing/ nome-oggetto |
| CreateThingGroup | iot:CreateThingGroup | arn:aws:iot: regione:id-account:thinggroup/ nome-gruppo-oggetti Per il gruppo in fase di creazione e per il gruppo padre, se usato |
| CreateThingType | iot:CreateThingType | arn:aws:iot: regione:id-account:thingtype/ nome-tipo-oggetto |
| CreateTopicRule | iot:CreateTopicRule | arn:aws:iot: regione:id-account:rule/ nome-regola |
| DeleteAuthorizer | iot:DeleteAuthorizer | arn:aws:iot: regione:id-account:authorizer/ nome-autorizzazione |
| DeleteCACertificate | iot:DeleteCACertificate | arn:aws:iot: regione:id-account:cacert/ id-certificato |
| DeleteCertificate | iot:DeleteCertificate | arn:aws:iot: regione:id-account:cert/ id-certificato |
| DeleteJob | iot:DeleteJob | arn:aws:iot: region:account-id:job/ job-id |
| DeleteJobExecution | iot:DeleteJobExecution | arn:aws:iot: region:account-id:job/ job-id arn:aws:iot: region:account-id:thing/ thing-name |
| DeletePolicy | iot:DeletePolicy | arn:aws:iot: regione:id-account:policy/ nome-policy |
| DeletePolicyVersion | iot:DeletePolicyVersion | arn:aws:iot: regione:id-account:policy/ nome-policy |
| DeleteRegistrationCode | iot:DeleteRegistrationCode | |
| DeleteRoleAlias | iot:DeleteRoleAlias | arn:aws:iot: regione:id-account:rolealias/ nome-alias-ruolo |
| DeleteThing | iot:DeleteThing | arn:aws:iot: regione:id-account:thing/ nome-oggetto |
| DeleteThingGroup | iot:DeleteThingGroup | arn:aws:iot: regione:id-account:thinggroup/ nome-gruppo-oggetti |

| API | Autorizzazione necessaria (operazioni di policy) | Risorse |
|-------------------------------|--|---|
| DeleteThingType | iot:DeleteThingType | arn:aws:iot: regione:id-account:thingtype/nome-tipo-oggetto |
| DeleteTopicRule | iot:DeleteTopicRule | arn:aws:iot: regione:id-account:rule/nome-regola |
| DeleteV2LoggingLevel | iot:DeleteV2LoggingLevel | arn:aws:iot: regione:id-account:thinggroup/nome-gruppo-oggetti |
| DeprecateThingType | iot:DeprecateThingType | arn:aws:iot: regione:id-account:thingtype/nome-tipo-oggetto |
| DescribeAuthorizer | iot:DescribeAuthorizer | arn:aws:iot: regione:id-account:authorizer/nome-funzione-autorizzazione (parametro: authorizerName) Nessuna |
| DescribeCACertificate | iot:DescribeCACertificate | arn:aws:iot: regione:id-account:cacert/id-certificato |
| DescribeCertificate | iot:DescribeCertificate | arn:aws:iot: regione:id-account:cert/id-certificato |
| DescribeDefaultAuth | iot:DescribeDefaultAuth | Nessuna |
| DescribeEndpoint | iot:DescribeEndpoint | * |
| DescribeEventConfig | iot:DescribeEventConfig | Nessuna |
| DescribeIndex | iot:DescribeIndex | arn:aws:iot: regione:id-account:index/nome-indice |
| DescribeJob | iot:DescribeJob | arn:aws:iot: regione:id-account:job/job-id |
| DescribeJobExecution | iot:DescribeJobExecution | Nessuna |
| DescribeRoleAlias | iot:DescribeRoleAlias | arn:aws:iot: regione:id-account:rolealias/nome-alias-ruolo |
| DescribeThing | iot:DescribeThing | arn:aws:iot: regione:id-account:thing/nome-oggetto |
| DescribeThingGroup | iot:DescribeThingGroup | arn:aws:iot: regione:id-account:thinggroup/nome-gruppo-oggetti |
| DescribeThingRegistrationTask | iot:DescribeThingRegistrationTask | Nessuna |
| DescribeThingType | iot:DescribeThingType | arn:aws:iot: regione:id-account:thingtype/nome-tipo-oggetto |
| DetachPolicy | iot:DetachPolicy | arn:aws:iot: regione:id-account:cert/id-certificato oppure arn:aws:iot: regione:id-account:thinggroup/nome-gruppo-oggetti |
| DetachPrincipalPolicy | iot:DetachPrincipalPolicy | arn:aws:iot: regione:id-account:cert/id-certificato |
| DetachThingPrincipal | iot:DetachThingPrincipal | arn:aws:iot: regione:id-account:cert/id-certificato |

| API | Autorizzazione necessaria (operazioni di policy) | Risorse |
|---------------------------|--|---|
| DisableTopicRule | iot:DisableTopicRule | arn:aws:iot: regione:id-account:rule/nome-regola |
| EnableTopicRule | iot:EnableTopicRule | arn:aws:iot: regione:id-account:rule/nome-regola |
| GetEffectivePolicies | iot:GetEffectivePolicies | arn:aws:iot: regione:id-account:cert/id-certificato |
| GetIndexingConfiguration | iot:GetIndexingConfiguration | Nessuna |
| GetJobDocument | iot:GetJobDocument | arn:aws:iot: regione:id-account:job/job-id |
| GetLoggingOptions | iot:GetLoggingOptions | |
| GetPolicy | iot:GetPolicy | arn:aws:iot: regione:id-account:policy/nome-policy |
| GetPolicyVersion | iot:GetPolicyVersion | arn:aws:iot: regione:id-account:policy/nome-policy |
| GetRegistrationCode | iot:GetRegistrationCode | |
| GetTopicRule | iot:GetTopicRule | arn:aws:iot: regione:id-account:rule/nome-regola |
| ListAttachedPolicies | iot>ListAttachedPolicies | arn:aws:iot: regione:id-account:thinggroup/nome-gruppo-oggetti oppure arn:aws:iot: regione:id-account:cert/id-certificato |
| ListAuthorizers | iot>ListAuthorizers | Nessuna |
| ListCACertificates | iot>ListCACertificates | * |
| ListCertificates | iot>ListCertificates | * |
| ListCertificatesByCA | iot>ListCertificatesByCA | |
| ListIndices | iot>ListIndices | Nessuna |
| ListJobExecutionsForThing | iot>ListJobExecutionsForThing | Nessuna |
| ListJobExecutionsForThing | iot>ListJobExecutionsForThing | Nessuna |
| ListJobs | iot>ListJobs | arn:aws:iot: regione:id-account:thinggroup/nome-gruppo-oggetti Se è usato il parametro thingGroupName |
| ListOutgoingCertificates | iot>ListOutgoingCertificates | |
| ListPolicies | iot>ListPolicies | * |
| ListPolicyPrincipals | iot>ListPolicyPrincipals | arn:aws:iot: regione:id-account:policy/nome-policy |
| ListPolicyVersions | iot>ListPolicyVersions | arn:aws:iot: regione:id-account:policy/nome-policy |
| ListPrincipalPolicies | iot>ListPrincipalPolicies | arn:aws:iot: regione:id-account:cert/id-certificato |
| ListPrincipalThings | iot>ListPrincipalThings | arn:aws:iot: regione:id-account:cert/id-certificato |

| API | Autorizzazione necessaria (operazioni di policy) | Risorse |
|----------------------------|--|--|
| ListRoleAliases | iot:ListRoleAliases | Nessuna |
| ListTargetsForPolicy | iot>ListTargetsForPolicyarn:aws:iot: <i>regione:id-account:policy/nome-policy</i> | |
| ListThingGroups | iot>ListThingGroupsarn:aws:iot: <i>regione:id-account:thinggroup/nome-gruppo-oggetti</i> | |
| ListThingGroupsForThing | iot>ListThingGroupsForThingarn:aws:iot: <i>regione:id-account:thing/nome-oggetto</i> | |
| ListThingPrincipals | iot>ListThingPrincipalsarn:aws:iot: <i>regione:id-account:thing/nome-oggetto</i> | |
| ListThingRegistrationTasks | iot>ListThingRegistrationTasksarn:aws:iot: <i>regione:id-account:task/nome-task</i> | |
| ListThingRegistrations | iot>ListThingRegistrationsarn:aws:iot: <i>regione:id-account:thing/nome-oggetto</i> | |
| ListThingTypes | iot>ListThingTypes | * |
| ListThings | iot>ListThings | * |
| ListThingsInThingGroup | iot>ListThingsInThingGrouparn:aws:iot: <i>regione:id-account:thinggroup/nome-gruppo-oggetti</i> | |
| ListTopicRules | iot>ListTopicRules | * |
| ListV2LoggingLevels | iot>ListV2LoggingLevels | Nessuna |
| RegisterCACertificate | iot:RegisterCACertificate | |
| RegisterCertificate | iot:RegisterCertificate* | |
| RegisterThing | iot:RegisterThing | Nessuna |
| RejectCertificateTransfer | iot>RejectCertificateTransferarn:aws:iot: <i>regione:id-account:cert/id-certificato</i> | |
| RemoveThingFromThingGroup | iot>RemoveThingFromThingGrouparn:aws:iot: <i>regione:id-account:thinggroup/nome-gruppo-oggetti</i> | |
| ReplaceTopicRule | iot>ReplaceTopicRulearn:aws:iot: <i>regione:id-account:rule/nome-regola</i> | |
| SearchIndex | iot>SearchIndex | arn:aws:iot: <i>regione:id-account:index/id-indice</i> |
| SetDefaultAuthorizer | iot>SetDefaultAuthorizerarn:aws:iot: <i>regione:id-account:authorizer/nome-funzione-autorizzazione</i> | |
| SetDefaultPolicyVersion | iot>SetDefaultPolicyVersionarn:aws:iot: <i>regione:id-account:policy/nome-policy</i> | |
| SetLoggingOptions | iot>SetLoggingOptionsarn:aws:iot: <i>regione:id-account:role/nome-ruolo</i> | |
| SetV2LoggingLevel | iot>SetV2LoggingLevelarn:aws:iot: <i>regione:id-account:thinggroup/nome-gruppo-oggetti</i> | |
| SetV2LoggingOptions | iot>SetV2LoggingOptionsarn:aws:iot: <i>regione:id-account:role/nome-ruolo</i> | |
| StartThingRegistration | iot>StartThingRegistrationarn:aws:iot: <i>regione:id-account:task/nome-task</i> | |
| StopThingRegistration | iot>StopThingRegistrationarn:aws:iot: <i>regione:id-account:task/nome-task</i> | |

| API | Autorizzazione necessaria (operazioni di policy) | Risorse |
|------------------------------|--|--|
| TestAuthorization | iot:TestAuthorization | arn:aws:iot: <i>regione:id-account:cert/id-certificato</i> |
| TestInvokeAuthorizer | iot:TestInvokeAuthorizer | Nessuna |
| TransferCertificate | iot:TransferCertificate | arn:aws:iot: <i>regione:id-account:cert/id-certificato</i> |
| UpdateAuthorizer | iot:UpdateAuthorizer | arn:aws:iot: <i>regione:id-account:authorizerfunction/nome-funzione-autorizzazione</i> |
| UpdateCACertificate | iot:UpdateCACertificate | arn:aws:iot: <i>regione:id-account:cacert/id-certificato</i> |
| UpdateCertificate | iot:UpdateCertificate | arn:aws:iot: <i>regione:id-account:cert/id-certificato</i> |
| UpdateEventConfigurations | iot:UpdateEventConfigurations | Nessuna |
| UpdateIndexingConfigurations | iot:UpdateIndexingConfigurations | Nessuna |
| UpdateRoleAlias | iot:UpdateRoleAlias | arn:aws:iot: <i>regione:id-account:rolealias/nome-alias-ruolo</i> |
| UpdateThing | iot:UpdateThing | arn:aws:iot: <i>regione:id-account:thing/nome-oggetto</i> |
| UpdateThingGroup | iot:UpdateThingGroup | arn:aws:iot: <i>regione:id-account:thinggroup/nome-gruppo-oggetti</i> |
| UpdateThingGroupsForThing | iot:UpdateThingGroupsForThing | arn:aws:iot: <i>regione:id-account:thing/nome-oggetto</i> |

Modelli di policy IAM

AWS IoT offre un set di modelli di policy IAM che puoi usare senza apportarvi o come punto di partenza per la creazione di policy IAM personalizzate. Questi modelli permettono di accedere a operazioni di configurazione e sui dati. Le operazioni di configurazione ti permettono di creare oggetti, certificati, policy e regole. Le operazioni sui dati inviano dati tramite il protocollo MQTT o HTTP. La tabella seguente descrive questi modelli.

| Modello di policy | Descrizione |
|----------------------------|---|
| AWSIoTLogging | Permette all'identità associata di configurare il logging di CloudWatch. Questa policy è collegata al ruolo di logging di CloudWatch. |
| AWSIoTConfigAccess | Permette all'identità associata di accedere a tutte le operazioni di configurazione di AWS IoT. Questa policy può influenzare l'elaborazione e lo storage dei dati. |
| AWSIoTConfigReadOnlyAccess | Permette all'identità associata di chiamare operazioni di configurazione di sola lettura. |
| AWSIoTDataAccess | Concede all'identità associata l'accesso completo a tutte le operazioni sui dati di AWS IoT. Le operazioni sui dati inviano dati tramite il protocollo MQTT o HTTP. |

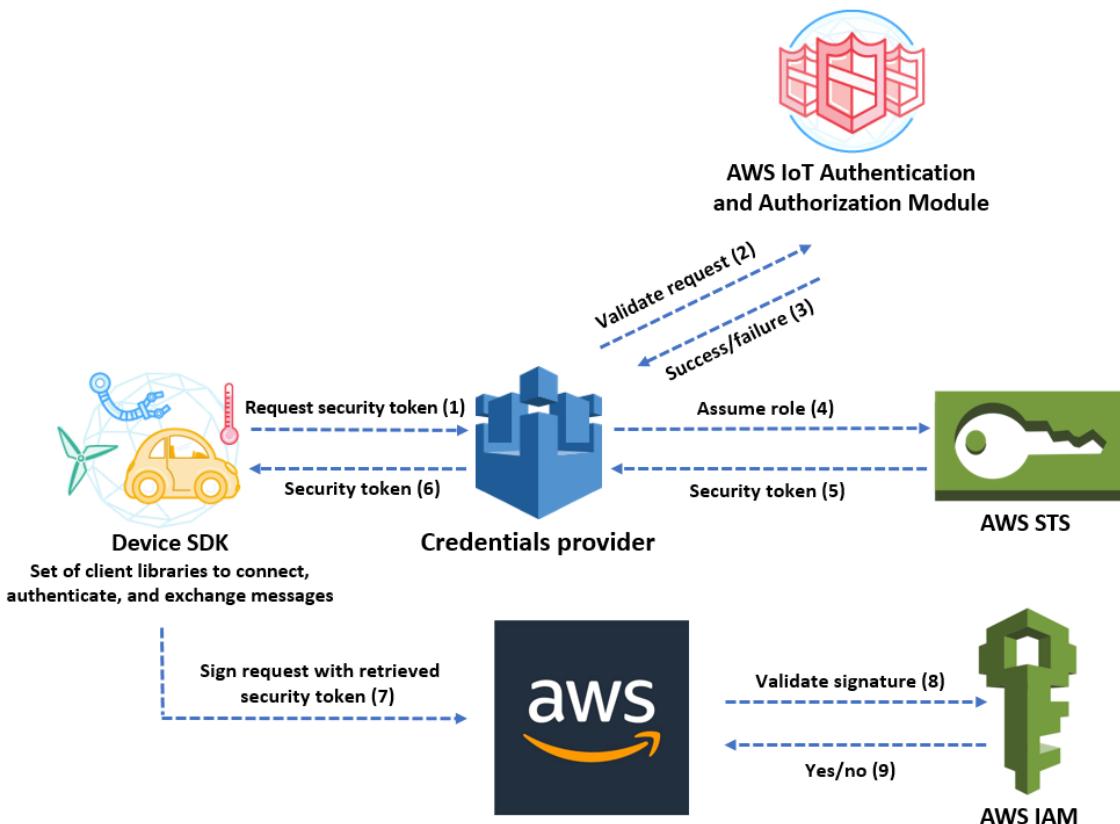
| Modello di policy | Descrizione |
|--------------------------|--|
| AWSIoTFullAccess | Concede all'identità associata l'accesso completo a tutte le operazioni di configurazione e sui dati di AWS IoT. |
| AWSIoTOTUpdate | Concede all'identità associata l'accesso per creare processi di AWS IoT e processi di firma del codice di AWS IoT. |
| AWSIoTRuleActions | Concede all'identità associata l'accesso a tutti i servizi AWS supportati nelle operazioni delle regole di AWS IoT. |
| AWSIoTThingsRegistration | Permette all'identità associata di registrare oggetti in blocco utilizzando StartThingRegistrationTask . Questa policy può influenzare l'elaborazione e lo storage dei dati. |

Autorizzazione di chiamate dirette a servizi AWS

I dispositivi possono usare i certificati X.509 per connettersi a AWS IoT tramite protocolli di autenticazione reciproca TLS. Altri servizi AWS non supportano l'autenticazione basata su certificati, ma possono essere chiamati tramite credenziali AWS in [formato AWS Signature Version 4](#). L'algoritmo [Signature Version 4](#) in genere richiede che l'autore della chiamata disponga di un ID chiave di accesso e di una chiave di accesso segreta. AWS IoT dispone di un fornitore di credenziali che ti permette di utilizzare il [certificato X.509](#) integrato come identità del dispositivo univoca per l'autenticazione delle richieste AWS. Ciò elimina la necessità di archiviare un ID chiave di accesso e la chiave di accesso segreta sul dispositivo.

Il fornitore di credenziali autentica un intermediario usando un certificato X.509 ed emette un token temporaneo di sicurezza con privilegi limitati. Il token può essere utilizzato per effettuare l'accesso e autenticare qualsiasi richiesta AWS. Questa modalità di autenticazione delle richieste AWS richiede di creare e configurare un [ruolo AWS Identity and Access Management \(IAM\)](#) e di collegarvi policy IAM appropriate, in modo che il fornitore di credenziali possa assumere il ruolo per tuo conto.

Lo schema seguente illustra il flusso di lavoro del fornitore di credenziali.



- Il dispositivo AWS IoT invia una richiesta HTTPS al fornitore di credenziali per un token di sicurezza. La richiesta include il certificato X.509 del dispositivo per l'autenticazione.
- Il fornitore di credenziali inoltra la richiesta al modulo di autenticazione e autorizzazione di AWS IoT per convalidare il certificato e verificare che disponga dell'autorizzazione per richiedere il token di sicurezza.
- Se il certificato è valido e dispone dell'autorizzazione per richiedere il token di sicurezza, il modulo di autenticazione e autorizzazione di AWS IoT indica che l'operazione è stata eseguita correttamente. In caso contrario, invia un'eccezione al dispositivo.
- Una volta completata la convalida del certificato, il fornitore di credenziali richiama il [AWS Security Token Service \(AWS STS\)](#) per usare il ruolo IAM creato.
- AWS STS restituisce al fornitore di credenziali un token di sicurezza temporaneo con privilegi limitati.
- Il fornitore di credenziali restituisce il token di sicurezza al dispositivo.
- Il dispositivo usa il token di sicurezza per firmare una richiesta AWS con AWS Signature Version 4.
- Il servizio richiesto richiama IAM per convalidare la firma e autorizzare la richiesta in base alle policy di accesso collegate al ruolo IAM creato per il fornitore di credenziali.
- Se IAM convalida la firma correttamente e autorizza la richiesta, questa va a buon fine. In caso contrario, IAM invia un'eccezione.

La sezione seguente descrive come utilizzare un certificato per ottenere un token di sicurezza. Si presuppone che sia stato già [registrato un dispositivo](#) e [creato e attivato il relativo certificato](#).

Come utilizzare un certificato per ottenere un token di sicurezza

1. Configura il ruolo IAM che il fornitore di credenziali assume per conto del tuo dispositivo. Collega la seguente policy di attendibilità al ruolo.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Effect": "Allow",  
         "Principal": {"Service": "credentials.iot.amazonaws.com"},  
         "Action": "sts:AssumeRole"}  
    ]  
}
```

Per ogni servizio AWS che desideri chiamare, collega al ruolo una policy di accesso. Il fornitore di credenziali supporta le seguenti variabili di policy:

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

Quando il dispositivo fornisce il nome dell'oggetto nella richiesta di un servizio AWS, il fornitore di credenziali aggiunge `credentials-iot:ThingName` e `credentials-iot:ThingTypeName` come variabili di contesto al token di sicurezza. Il fornitore di credenziali fornisce `credentials-iot:AwsCertificateId` come variabile di contesto, anche se il dispositivo non fornisce il nome dell'oggetto nella richiesta. Il nome dell'oggetto viene passato come valore dell'intestazione di richiesta HTTP `x-amzn-iot-thingname`.

Queste tre variabili funzionano solo con le policy IAM, non con le policy AWS IoT.

2. Assicurati che l'utente che esegue la fase successiva (creando un alias del ruolo) disponga dell'autorizzazione per trasferire questo ruolo appena creato a AWS IoT. La policy seguente fornisce entrambe le autorizzazioni `iam:GetRole` e `iam:PassRole` a un utente AWS. L'autorizzazione `iam:GetRole` consente all'utente di ottenere informazioni sul ruolo appena creato. L'autorizzazione `iam:PassRole` consente all'utente di trasferire il ruolo a un altro servizio AWS.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {"Effect": "Allow",  
         "Action": ["iam:GetRole",  
                   "iam:PassRole"],  
         "Resource": "arn:aws:iam::your aws account id:role/your role name"}  
    ]  
}
```

3. Crea un alias del ruolo AWS IoT. Il dispositivo che effettuerà chiamate dirette ai servizi AWS deve sapere quale ARN del ruolo usare durante la connessione a AWS IoT. L'impostazione hardcoded dell'ARN del ruolo non è una buona soluzione, perché richiede di aggiornare il dispositivo ogni volta che l'ARN del ruolo cambia. Una soluzione migliore consiste nell'utilizzare l'API `CreateRoleAlias` per creare un alias del ruolo che punti all'ARN del ruolo. Se l'ARN del ruolo viene modificato, è sufficiente aggiornare l'alias del ruolo. Non è richiesta alcuna modifica sul dispositivo. Questa API accetta i parametri seguenti:

roleAlias

Obbligatorio. Stringa arbitraria che identifica l'alias del ruolo. Opera come chiave primaria nel modello di dati dell'alias del ruolo. Contiene da 1 a 128 caratteri e deve includere solo caratteri alfanumerici e i simboli =,@ e -. Sono consentite le lettere maiuscole e minuscole.

roleArn

Obbligatorio. ARN del ruolo cui fa riferimento l'alias del ruolo.

credentialDurationInSeconds

Opzionale. Tempo di validità (in secondi) della credenziale. Il valore minimo è di 900 secondi (15 minuti). Il valore massimo è di 3.600 secondi (60 minuti). Il valore predefinito è 3.600 secondi.

Per ulteriori informazioni su questa API, consulta [CreateRoleAlias](#).

- Collega una policy al certificato del dispositivo. La policy collegata al certificato del dispositivo deve concedere al dispositivo l'autorizzazione necessaria per assumere il ruolo. A questo scopo, devi concedere l'autorizzazione per l'operazione `iot:AssumeRoleWithCertificate` sull'alias del ruolo, come indicato nel seguente esempio.

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

- Effettuare una richiesta HTTPS al fornitore di credenziali per ottenere un token di sicurezza. Fornire le seguenti informazioni.

- Certificato: poiché questa è una richiesta HTTP tramite autenticazione reciproca TLS, durante la richiesta devi fornire al client il certificato e la chiave privata corrispondente. Usa lo stesso certificato e la chiave privata utilizzati per registrare il certificato con AWS IoT.

Per avere la certezza che il dispositivo stia comunicando con AWS IoT (e non un servizio che lo rappresenta), fare riferimento alla documentazione in [Autenticazione del server in AWS IoT Core](#), seguire i collegamenti per scaricare i relativi certificati CA, quindi copiarli sul dispositivo.

- RoleAlias: il nome dell'alias del ruolo creato per il fornitore di credenziali.
- ThingName: il nome dell'oggetto creato al momento della registrazione dell'oggetto AWS IoT. Viene trasferito come valore dell'intestazione HTTP `x-amzn-iot-thingname`. Questo valore è obbligatorio solo se usi attributi di oggetto come le variabili di policy in AWS IoT o le policy IAM.

Esegui il comando seguente in AWS CLI per ottenere l'endpoint del fornitore di credenziali per l'account AWS. Per ulteriori informazioni su questa API, consulta [DescribeEndpoint](#).

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

Il seguente oggetto JSON è l'output di esempio del comando `describe-endpoint`. Contiene il valore `endpointAddress` utilizzato per richiedere un token di sicurezza.

```
{  
    "endpointAddress": "<your aws account specific prefix>.credentials.iot.<your region>.amazonaws.com"
```

}

Utilizza l'endpoint per effettuare una richiesta HTTPS al fornitore di credenziali per restituire un token di sicurezza. L'esempio seguente usa curl ma è possibile usare qualsiasi client HTTP.

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

Questo comando restituisce un oggetto token di sicurezza che contiene `accessKeyId`, `secretAccessKey`, `sessionToken` e una scadenza. Il seguente oggetto JSON è l'output di esempio del comando curl.

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

È possibile utilizzare i valori `accessKeyId`, `secretAccessKey` e `sessionToken` per firmare le richieste ai servizi AWS. Per una dimostrazione end-to-end di un caso d'uso specifico, consulta [Come eliminare la necessità di credenziali AWS hardcoded nei dispositivi usando il provider di credenziali AWS IoT](#).

Accesso tra account

In AWS IoT puoi consentire a un'entità principale di pubblicare o sottoscrivere un argomento definito in un account AWS non di proprietà dell'entità principale. Per configurare l'accesso tra account, crea una policy IAM e un ruolo IAM e quindi collega la policy al ruolo.

Innanzitutto, crea una policy IAM gestita dal cliente come descritto in [Creazione di policy IAM](#), come faresti per altri utenti e certificati nell'account AWS.

registered devices (16)

Per i dispositivi registrati nel registro AWS IoT, la policy seguente concede l'autorizzazione ai dispositivi per connettersi a AWS IoT mediante un ID client che corrisponde al nome dell'oggetto del dispositivo e pubblicare in `my/topic/<thing-name>` dove `<thing-name>` è il nome dell'oggetto del dispositivo:

```
{
  "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}"],  
    }  
}  
}
```

unregistered devices (16)

Per i dispositivi non registrati nel registro AWS IoT, la policy seguente concede a un dispositivo l'autorizzazione per utilizzare il nome dell'oggetto `client1` registrato nel registro AWS IoT (123456789012) dell'account per connettersi a AWS IoT e pubblicare in un argomento specifico dell'ID client il cui nome è preceduto da `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}"]  
        }  
    ]  
}
```

Quindi, segui le fasi nella pagina [Creazione di un ruolo per delegare le autorizzazioni a un utente IAM](#). Immetti l'ID account dell'account AWS con cui desideri condividere l'accesso. Quindi, nella fase finale, collega la policy appena creata al ruolo. Se in un secondo momento devi modificare l'ID account AWS cui desideri concedere l'accesso, potrai usare il formato di policy di trust seguente a questo scopo.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": { "AWS": "arn:aws:iam:us-east-1:567890123456:user:MyUser" },  
            "Action": "sts:AssumeRole",  
        }  
    ]  
}
```

Sicurezza del trasporto

Il broker di messaggi AWS IoT e il servizio Device Shadow crittografano tutta la comunicazione con [TLS versione 1.2](#). TLS viene usato per garantire la riservatezza dei protocolli applicativi (MQTT, HTTP) supportati da AWS IoT. TLS è disponibile in diversi linguaggi di programmazione e sistemi operativi.

Per MQTT, TLS crittografa la connessione tra il dispositivo e il broker. L'autenticazione client TLS viene usata da AWS IoT per identificare i dispositivi. Per HTTP, TLS crittografa la connessione tra il dispositivo e il broker. L'autenticazione viene delegata ad AWS Signature Version 4.

Supporto per i pacchetti di crittografia TLS

AWS IoT supporta i pacchetti di crittografia seguenti:

- ECDHE-ECDSA-AES128-GCM-SHA256 (consigliato)
- ECDHE-RSA-AES128-GCM-SHA256 (consigliato)
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA

Broker di messaggi per AWS IoT

Il broker di messaggi AWS IoT è un servizio broker di pubblicazione/sottoscrizione che permette di inviare e ricevere messaggi da e verso AWS IoT. Durante la comunicazione con AWS IoT, un client invia un messaggio indirizzato a un argomento, ad esempio `Sensor/temp/room1`.

Note

Non è consigliabile utilizzare informazioni di identificazione personale negli argomenti.

Il broker di messaggi, a sua volta, invia il messaggio a tutti i client registrati per la ricezione di messaggi per l'argomento. L'azione di invio del messaggio viene definita pubblicazione. L'azione di registrazione per la ricezione di messaggi per un filtro di argomenti è definita sottoscrizione.

Il namespace dell'argomento è isolato per ogni account AWS e coppia di regioni. Ad esempio, l'argomento `Sensor/temp/room1` per un account AWS è indipendente dall'argomento `Sensor/temp/room1` per un altro account AWS. Questo vale anche per le regioni. L'argomento `Sensor/temp/room1` nello stesso account AWS in us-east-1 è indipendente dallo stesso argomento in us-east-2. AWS IoT non supporta l'invio e la ricezione di messaggi tra più account AWS e regioni.

Il broker di messaggi mantiene un elenco di tutte le sessioni client e delle sottoscrizioni per ogni sessione. Quando viene pubblicato un messaggio in un argomento, il broker controlla le sessioni e le sottoscrizioni mappate all'argomento. Il broker inoltra quindi il messaggio di pubblicazione a tutte le sessioni che hanno un client attualmente connesso.

Se il caso d'uso specifico non richiede IoT, consulta [Messaggistica in AWS](#) per informazioni su altri servizi di messaggistica di AWS che meglio soddisfano le esigenze.

Protocolli

Il broker di messaggi supporta l'uso del protocollo MQTT per la pubblicazione e la sottoscrizione e del protocollo HTTPS per la pubblicazione. Entrambi i protocolli sono supportati tramite IP versione 4 e IP versione 6. Il broker di messaggi supporta anche MQTT tramite il protocollo WebSocket.

Associazioni tra protocolli e porte

La tabella seguente indica ogni protocollo supportato da AWS IoT, il metodo di autenticazione e la porta usata per ogni protocollo.

Associazioni tra protocolli, autenticazione e porte

| Protocollo | Autenticazione | Porta | ALPN ProtocolName |
|------------|--------------------------|------------------------|-------------------|
| MQTT | Certificato client X.509 | 8883, 443 [†] | x-amzn-mqtt-ca |
| HTTPS | Certificato client X.509 | 8443, 443 [†] | x-amzn-http-ca |
| HTTPS | SigV4 | 443 | N/D |

| Protocollo | Autenticazione | Porta | ALPN ProtocolName |
|-----------------------------------|----------------|-------|-------------------|
| MQTT tramite protocollo WebSocket | SigV4 | 443 | N/D |

[†]Client che si connettono sulla porta 443 con l'autenticazione del certificato client X.509 devono implementare l'estensione TLS [Application Layer Protocol Negotiation \(ALPN\)](#) e usare l'elemento [ALPN ProtocolName](#) elencato in precedenza nell'elemento [ALPN ProtocolNameList](#) inviato dal client come parte del messaggio `ClientHello`.

MQTT

MQTT è un protocollo di messaggistica leggero molto diffuso, progettato per dispositivi vincolati. Per ulteriori informazioni, consulta [MQTT](#). Il broker di messaggi AWS IoT supporta i livelli 0 e 1 della qualità del servizio (QoS).

Anche se l'implementazione del broker di messaggi AWS IoT è basata su MQTT versione 3.1.1, devia dalla specifica per quanto riguarda le considerazioni seguenti:

- In AWS IoT la sottoscrizione di un argomento con QoS livello 0 significa che un messaggio viene recapitato zero o più volte. È possibile che un messaggio venga recapitato più di una volta. I messaggi recapitati più di una volta potrebbero essere inviati con un ID pacchetto diverso. In questi casi, il flag DUP non è impostato.
- AWS IoT non supporta la pubblicazione e la sottoscrizione con livello QoS 2. Il broker di messaggi AWS IoT non invia un messaggio PUBACK o SUBACK quando è richiesto un livello QoS 2.
- Nel rispondere a una richiesta di connessione, il broker di messaggi invia un messaggio CONNACK. Questo messaggio contiene un flag per indicare se la connessione sta riprendendo una sessione precedente. Il valore di questo flag potrebbe non essere corretto se due client MQTT si connettono contemporaneamente con lo stesso ID client.
- Quando un client sottoscrive un argomento, può verificarsi un ritardo tra il momento in cui il broker di messaggi invia un messaggio SUBACK e il momento in cui il client inizia a ricevere nuovi messaggi corrispondenti.
- La specifica MQTT fornisce un clausola che permette all'entità di pubblicazione di richiedere che il broker conservi l'ultimo messaggio inviato a un argomento e che lo invii a tutti i futuri sottoscrittori dell'argomento. AWS IoT non supporta la conservazione dei messaggi. Se viene inviata una richiesta di conservazione dei messaggi, la connessione viene interrotta.
- Il broker di messaggi usa l'ID client per identificare ogni client. L'ID client viene passato dal client al broker di messaggi come parte del payload MQTT. Due client con lo stesso ID client non possono essere connessi contemporaneamente al broker di messaggi. Quando un client si connette al broker di messaggi tramite un ID client usato da un altro client, viene inviato un messaggio CONNACK a entrambi i client e il client connesso viene disconnesso.
- In rari casi, il broker di messaggi può inviare di nuovo lo stesso messaggio PUBLISH logico con un ID pacchetto diverso.
- Il broker di messaggi non garantisce l'ordine di ricezione dei messaggi e delle conferme.

Argomenti

Il broker di messaggi usa argomenti per instradare messaggi dai client di pubblicazione ai client di sottoscrizione. La barra (/) viene usata per separare la gerarchia degli argomenti.

Note

Non è consigliabile utilizzare informazioni di identificazione personale negli argomenti.

La tabella seguente elenca i caratteri jolly che possono essere usati nel filtro di argomenti quando esegui la sottoscrizione.

Caratteri jolly per gli argomenti

| Carattere jolly | Descrizione |
|-----------------|--|
| # | Deve essere l'ultimo carattere nell'argomento che stai sottoscrivendo. Opera come carattere jolly associando la struttura corrente e tutte le sottostrutture. Ad esempio, una sottoscrizione di Sensor/# riceve i messaggi pubblicati in Sensor/, Sensor/temp e Sensor/temp/room1, ma non i messaggi pubblicati in Sensor. |
| + | Corrisponde esattamente a un elemento nella gerarchia degli argomenti. Ad esempio, una sottoscrizione di Sensor/+/room1 riceve i messaggi pubblicati in Sensor/temp/room1, Sensor/moisture/room1 e così via. |

Argomenti riservati

Ad eccezione degli argomenti elencati di seguito, tutti quelli che iniziano con \$ sono considerati riservati e non sono supportati per la pubblicazione e la sottoscrizione. Qualsiasi tentativo di pubblicare o sottoscrivere argomenti che inizino con \$ terminerà la connessione.

Argomenti di eventi

| Argomento | Operazioni consentite | Descrizione |
|--|-----------------------|--|
| \$aws/events/presence/connected/ <i>IDclient</i> | Sottoscrivi | AWS IoT pubblica in questo argomento quando un client MQTT con l'ID client specificato si connette ad AWS IoT. Per ulteriori informazioni, consulta Eventi di connessione/disconnessione (p. 637) . |
| \$aws/events/presence/disconnected/ <i>IDclient</i> | Sottoscrivi | AWS IoT pubblica in questo argomento quando un client MQTT con l'ID client specificato si disconnette da AWS IoT. Per ulteriori informazioni, consulta Eventi di connessione/disconnessione (p. 637) . |
| \$aws/events/subscriptions/subscribed/ <i>IDclient</i> | Sottoscrivi | AWS IoT pubblica in questo argomento quando un client MQTT con l'ID client specificato sottoscrive un argomento MQTT. Per ulteriori informazioni, consulta Eventi di sottoscrizione/annullamento della sottoscrizione (p. 639) . |

| Argomento | Operazioni consentite | Descrizione |
|--|-----------------------|---|
| \$aws/events/subscriptions/unsubscribed/ <i>IDclient</i> | Sottoscrivi | AWS IoT pubblica in questo argomento quando un client MQTT con l'ID client specificato annulla la sottoscrizione di un argomento MQTT. Per ulteriori informazioni, consulta Eventi di sottoscrizione/annullamento della sottoscrizione (p. 639) . |

Argomenti di regole

| Argomento | Operazioni consentite | Descrizione |
|------------------------------|-----------------------|---|
| \$aws/rules/ <i>ruleName</i> | Pubblicazione | Un dispositivo o un'applicazione pubblica su questo argomento per arrivare le regole direttamente. Per ulteriori informazioni, consulta Basic Ingest (p. 333) . |

Argomenti Thing Shadow

| Argomento | Operazioni consentite | Descrizione |
|--|------------------------------|--|
| \$aws/things/< <i>thingName</i> >/shadow/delete | Pubblicazione/Sottoscrizione | Un dispositivo o un'applicazione pubblica in questo argomento per eliminare una copia shadow. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#delete-pub-sub-topic . |
| \$aws/things/< <i>thingName</i> >/shadow/delete/accepted | Sottoscrizione | Il servizio Device Shadow invia messaggi a questo argomento quando viene eliminata una copia shadow. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#delete-accepted-pub-sub-topic . |
| \$aws/things/< <i>thingName</i> >/shadow/delete/rejected | Sottoscrizione | Il servizio Device Shadow invia messaggi a questo argomento quando viene rifiutata una richiesta di eliminazione di una copia shadow. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#delete-rejected-pub-sub-topic . |

| Argomento | Operazioni consentite | Descrizione |
|--|------------------------------|--|
| | | shadow-mqtt.html#delete-rejected-pub-sub-topic . |
| \$aws/things/< <i>thingName</i> >/shadow/get | Pubblicazione/Sottoscrizione | Un'applicazione o un oggetto pubblica un messaggio vuoto in questo argomento per ottenere una copia shadow. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html . |
| \$aws/things/< <i>thingName</i> >/shadow/get/accepted | Sottoscrizione | Il servizio Device Shadow invia messaggi a questo argomento quando viene effettuata correttamente una richiesta di una copia shadow. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#get-accepted-pub-sub-topic . |
| \$aws/things/< <i>thingName</i> >/shadow/get/rejected | Sottoscrizione | Il servizio Device Shadow invia messaggi a questo argomento quando viene rifiutata una richiesta di una copia shadow. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#get-rejected-pub-sub-topic . |
| \$aws/things/< <i>thingName</i> >/shadow/update | Pubblicazione/Sottoscrizione | Un oggetto o un'applicazione pubblica in questo argomento per aggiornare una copia shadow. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#update-pub-sub-topic . |
| \$aws/things/< <i>thingName</i> >/shadow/update/accepted | Sottoscrizione | Il servizio Device Shadow invia messaggi a questo argomento quando viene effettuato correttamente un aggiornamento di una copia shadow. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#update-accepted-pub-sub-topic . |

| Argomento | Operazioni consentite | Descrizione |
|--|-----------------------|--|
| \$aws/things/<thingName>/shadow/update/rejected | Sottoscrizione | Il servizio Device Shadow invia messaggi a questo argomento quando viene rifiutato un aggiornamento di una copia shadow. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#update-rejected-pub-sub-topic . |
| \$aws/things/<thingName>/shadow/update/delta | Sottoscrizione | Il servizio Device Shadow invia messaggi a questo argomento quando viene rilevata una differenza tra le sezioni sullo stato segnalato e sullo stato desiderato di una copia shadow. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#update-delta-pub-sub-topic . |
| \$aws/things/<thingName>/shadow/update/documents | Sottoscrizione | AWS IoT pubblica un documento sullo stato in questo argomento ogni volta che un aggiornamento nella copia shadow va a buon fine. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-mqtt.html#update-documents-pub-sub-topic . |

Argomenti di processi

| Argomento | Operazioni consentite | Descrizione |
|--|-----------------------|--|
| \$aws/things/<thingName>/jobs/get | Pubblicazione | I dispositivi pubblicano un messaggio in questo argomento per effettuare una richiesta GetPendingJobExecutions. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/things/<thingName>/jobs/get/accepted | Sottoscrizione | I dispositivi si sottoscrivono a questo argomento per ricevere risposte corrette da una richiesta |

| Argomento | Operazioni consentite | Descrizione |
|---|-----------------------|---|
| | | GetPendingJobExecutions. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/things/<thingName>/jobs/get/accepted | Sottoscrizione | I dispositivi si sottoscrivono a questo argomento per ricevere risposte corrette per una richiesta GetPendingJobExecutions. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/things/<thingName>/jobs/start-next | Pubblicazione | I dispositivi pubblicano un messaggio in questo argomento per effettuare una richiesta StartNextPendingJobExecution. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/things/<thingName>/jobs/start-next/accepted | Sottoscrizione | I dispositivi si sottoscrivono a questo argomento per ricevere risposte corrette per una richiesta StartNextPendingJobExecution. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/things/<thingName>/jobs/start-next/rejected | Sottoscrizione | I dispositivi si sottoscrivono a questo argomento per ricevere risposte corrette per una richiesta StartNextPendingJobExecution. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |

| Argomento | Operazioni consentite | Descrizione |
|---|-----------------------|---|
| \$aws/things/<thingName>/jobs/jobId/get | Pubblicazione | I dispositivi pubblicano un messaggio in questo argomento per effettuare una richiesta <code>DescribeJobExecution</code> . Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/things/<thingName>/jobs/<jobId>/get/accepted | Sottoscrizione | I dispositivi si sottoscrivono a questo argomento per ricevere risposte corrette per una richiesta <code>DescribeJobExecution</code> . Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/things/<thingName>/jobs/<jobId>/get/rejected | Sottoscrizione | I dispositivi si sottoscrivono a questo argomento per ricevere risposte corrette per una richiesta <code>DescribeJobExecution</code> . Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/things/<thingName>/jobs/<jobId>/update | Pubblicazione | I dispositivi pubblicano un messaggio in questo argomento per effettuare una richiesta <code>UpdateJobExecution</code> . Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/things/<thingName>/jobs/<jobId>/update/accepted | Sottoscrizione | I dispositivi si sottoscrivono a questo argomento per ricevere risposte corrette per una richiesta <code>UpdateJobExecution</code> . Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |

| Argomento | Operazioni consentite | Descrizione |
|---|-----------------------|--|
| \$aws/things/<thingName>/jobs/<jobId>/update/rejected | Sottoscrizione | I dispositivi si sottoscrivono a questo argomento per ricevere risposte corrette per una richiesta <code>UpdateJobExecution</code> . Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/things/<thingName>/jobs/notify | Sottoscrizione | I dispositivi si sottoscrivono a questo argomento per ricevere notifiche quando viene aggiunta o rimossa l'esecuzione di un lavoro nell'elenco di esecuzioni in sospeso per una cosa. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/things/<thingName>/jobs/notify-next | Sottoscrizione | I dispositivi si sottoscrivono a questo argomento per ricevere notifiche quando viene modificata la successiva esecuzione del processo in sospeso per la cosa. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/iot/latest/developerguide/jobs-api.html . |
| \$aws/events/job/<jobId>/completed | Sottoscrizione | Il servizio Jobs pubblica un evento in questo argomento al termine di un processo. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |
| \$aws/events/job/<jobId>/canceled | Sottoscrizione | Il servizio Jobs pubblica un evento in questo argomento quando un processo viene annullato. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |
| \$aws/events/job/<jobId>/deleted | Sottoscrizione | Il servizio Jobs pubblica un evento su questo argomento quando un lavoro viene cancellato. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |

| Argomento | Operazioni consentite | Descrizione |
|--|-----------------------|---|
| \$aws/events/job/< <i>jobId</i> >/cancellation_in_progress | Sottoscrizione | Il servizio Jobs pubblica un evento in questo argomento quando inizia l'annullamento del processo. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |
| \$aws/events/job/< <i>jobId</i> >/deletion_in_progress | Sottoscrizione | Il servizio Jobs pubblica un evento in questo argomento quando inizia l'eliminazione di un processo. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |
| \$aws/events/jobExecution/< <i>jobId</i> >/succeeded | Sottoscrizione | Il servizio Jobs pubblica un evento in questo argomento quando l'esecuzione del processo ha esito positivo. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |
| \$aws/events/jobExecution/< <i>jobId</i> >/failed | Sottoscrizione | Il servizio Jobs pubblica un evento in questo argomento quando l'esecuzione di un processo non riesce. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |
| \$aws/events/jobExecution/< <i>jobId</i> >/rejected | Sottoscrizione | Il servizio Jobs pubblica un evento in questo argomento quando viene respinta l'esecuzione di un processo. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |
| \$aws/events/jobExecution/< <i>jobId</i> >/canceled | Sottoscrizione | Il servizio Jobs pubblica un evento in questo argomento quando viene annullata l'esecuzione di un processo. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |
| \$aws/events/jobExecution/< <i>jobId</i> >/timed_out | Sottoscrizione | Il servizio Jobs pubblica un evento in questo argomento quando si verifica il timeout dell'esecuzione di un processo. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |

| Argomento | Operazioni consentite | Descrizione |
|--|-----------------------|---|
| \$aws/events/ jobExecution/< <i>jobId</i> >/ removed | Sottoscrizione | Il servizio Jobs pubblica un evento in questo argomento quando viene rimossa l'esecuzione di un processo. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |
| \$aws/events/ jobExecution/< <i>jobId</i> >/ deleted | Sottoscrizione | Il servizio Jobs pubblica un evento in questo argomento quando viene eliminata l'esecuzione di un processo. Per ulteriori informazioni, consulta l'argomento relativo agli eventi di processo . |

Sessioni persistenti MQTT

Una sessione persistente rappresenta una connessione continua a un broker di messaggi MQTT. Quando un client si connette a un broker di messaggi AWS IoT utilizzando una sessione persistente, il broker di messaggi salva tutte le sottoscrizioni che il client effettua durante la connessione. Quando il client si disconnette, il broker di messaggi archivia i messaggi QoS 1 non riconosciuti e i nuovi messaggi QoS 1 pubblicati in argomenti di cui il client ha eseguito la sottoscrizione. Quando il client si riconnette alla sessione persistente, tutte le sottoscrizioni vengono ripristinate e tutti i messaggi archiviati vengono inviati al client a una velocità massima di 10 messaggi al secondo.

Puoi creare una sessione persistente MQTT inviando un messaggio CONNECT per impostare il flag `cleanSession` su 0. Se non esiste alcuna sessione per il client che invia il messaggio CONNECT, viene creata una nuova sessione persistente. Se esiste, viene ripresa.

I dispositivi devono guardare l'attributo `sessionPresent` nel messaggio CONNACK (Connection Acknowledged) per determinare l'eventuale presenza di una sessione persistente. Se `sessionPresent` è impostato su 1, è presente una sessione persistente e i messaggi archiviati vengono recapitati al client. Se `sessionPresent` è impostato su 0, non è presente alcuna sessione persistente e il client deve effettuare nuovamente la sottoscrizione nei filtri degli argomenti.

Le sessioni persistenti hanno un periodo di scadenza predefinito di 1 ora. Il periodo di scadenza inizia quando il broker di messaggi rileva la disconnessione da parte di un client (disconnessione o timeout MQTT). Il periodo di scadenza della sessione persistente può essere aumentato tramite il processo di aumento del limite standard. Se un client non ha ripreso la propria sessione entro il periodo di scadenza, la sessione viene terminata e i relativi messaggi archiviati vengono eliminati. Il periodo di scadenza è approssimativo, il tempo massimo di persistenza delle sessioni potrebbe essere di 30 minuti in più (ma non meno) rispetto alla durata configurata. Per ulteriori informazioni, consulta [Restrizioni dei servizi AWS](#). Tutti i messaggi archiviati per le sessioni persistenti saranno fatturati alla tariffa standard per la messaggistica. Per ulteriori informazioni, consulta [Prezzi di AWS IoT](#).

HTTP

Il broker di messaggi supporta i client che si connettono con il protocollo HTTP tramite un'API REST. I client possono eseguire la pubblicazione inviando un messaggio POST a `<AWS IoT Endpoint>/topics/<url_encoded_topic_name>?qos=1`".

Ad esempio, puoi usare `curl` per emulare l'invio di un messaggio. Ad esempio:

```
curl --tlsv1.2 --cacert root-CA.crt --cert 4b7828d2e5-certificate.pem.crt --key  
4b7828d2e5-private.pem.key -X POST -d "{ \"message\": \"Hello, world\" }" "https://  
a1pn10j0v8htvw.iot.us-east-1.amazonaws.com:8443/topics/my/topic"
```

--tlsv1.2

Usa TLSv1.2 (SSL). curl deve essere installato con OpenSSL e devi usare la versione 1.2 di TLS.
--cacert <nome file>

Nome del file del certificato CA per verificare il peer.

--cert <nome file>

Nome del file del certificato client.

--key <nome file>

Nome del file della chiave privata.

-X POST

Tipo di richiesta (in questo caso POST).

-d <dati>

Dati HTTP POST che vuoi pubblicare.

"https://..."

URL. In questo caso, l'endpoint API REST per l'oggetto.

Per individuare l'endpoint per un oggetto, nella console AWS IoT scegliere Registry per espandere le opzioni. Scegli Things (Oggetti), scegli l'oggetto e quindi fai clic su Interact (Interagisci). Dopo l'endpoint aggiungere la porta (:8443) seguita dalla parola chiave "argomenti", l'argomento e, infine, specificare la qualità del servizio in una stringa di query (?qos=1).

MQTT tramite il protocollo WebSocket

AWS IoT supporta MQTT tramite il protocollo [WebSocket](#) per permettere ad applicazioni remote e basate su browser di inviare e ricevere dati da dispositivi connessi ad AWS IoT usando credenziali AWS. Le credenziali AWS vengono specificate usando il protocollo [AWS Signature Version 4](#). Il supporto per WebSocket è disponibile sulla porta TCP 443, che permette il passaggio dei messaggi attraverso la maggior parte dei firewall e dei Web proxy.

Una connessione WebSocket viene avviata in un client inviando una richiesta HTTP GET. L'URL usato ha il formato seguente:

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

wss

Specifica il protocollo WebSocket.

endpoint

Endpoint AWS IoT specifico dell'account AWS. Puoi usare il comando [describe-endpoint](#) dell'interfaccia a riga di comando (CLI) per AWS IoT per trovare questo endpoint.

region

Regione AWS dell'account AWS.

mqtt

Specifica che i messaggi MQTT vengono inviati tramite il protocollo WebSocket.

Quando il server risponde, il client invia una richiesta di aggiornamento per indicare al server che comunicherà tramite il protocollo WebSocket. Dopo che il server conferma la richiesta di aggiornamento, tutta la comunicazione viene eseguita tramite il protocollo WebSocket. L'implementazione WebSocket usata funge da protocollo di trasporto. I dati inviati tramite il protocollo WebSocket sono messaggi MQTT.

Uso del protocollo WebSocket in un'applicazione Web

Poiché l'implementazione WebSocket fornita dalla maggior parte dei browser Web non permette la modifica delle intestazioni HTTP, devi aggiungere le informazioni sul protocollo Signature Version 4 alla stringa di query. Per ulteriori informazioni, consulta la pagina relativa all'[aggiunta di informazioni sulla firma alla stringa di query](#).

Il codice JavaScript seguente definisce alcune funzioni di utilità usate per la generazione di una richiesta Signature Version 4.

```
/**  
 * utilities to do sigv4  
 * @class SigV4Utils  
 */  
function SigV4Utils() {}  
  
SigV4Utils.getSignatureKey = function (key, date, region, service) {  
    var kDate = AWS.util.crypto.hmac('AWS4' + key, date, 'buffer');  
    var kRegion = AWS.util.crypto.hmac(kDate, region, 'buffer');  
    var kService = AWS.util.crypto.hmac(kRegion, service, 'buffer');  
    var kCredentials = AWS.util.crypto.hmac(kService, 'aws4_request', 'buffer');  
    return kCredentials;  
};  
  
SigV4Utils.getSignedUrl = function(host, region, credentials) {  
    var datetime = AWS.util.date.iso8601(new Date()).replace(/[:\-\]\|\.\d{3}]/g, '');  
    var date = datetime.substr(0, 8);  
  
    var method = 'GET';  
    var protocol = 'wss';  
    var uri = '/mqtt';  
    var service = 'iotdevicegateway';  
    var algorithm = 'AWS4-HMAC-SHA256';  
  
    var credentialScope = date + '/' + region + '/' + service + '/' + 'aws4_request';  
    var canonicalQueryString = 'X-Amz-Algorithm=' + algorithm;  
    canonicalQueryString += '&X-Amz-Credential=' +  
    encodeURIComponent(credentials.accessKeyId + '/' + credentialScope);  
    canonicalQueryString += '&X-Amz-Date=' + datetime;  
    canonicalQueryString += '&X-Amz-SignedHeaders=host';  
  
    var canonicalHeaders = 'host:' + host + '\n';  
    var payloadHash = AWS.util.crypto.sha256('', 'hex')  
    var canonicalRequest = method + '\n' + uri + '\n' + canonicalQueryString + '\n' +  
    canonicalHeaders + '\nhost\n' + payloadHash;  
  
    var stringToSign = algorithm + '\n' + datetime + '\n' + credentialScope + '\n' +  
    AWS.util.crypto.sha256(canonicalRequest, 'hex');  
    var signingKey = SigV4Utils.getSignatureKey(credentials.secretAccessKey, date, region,  
    service);  
    var signature = AWS.util.crypto.hmac(signingKey, stringToSign, 'hex');  
  
    canonicalQueryString += '&X-Amz-Signature=' + signature;  
    if (credentials.sessionToken) {  
        canonicalQueryString += '&X-Amz-Security-Token=' +  
        encodeURIComponent(credentials.sessionToken);  
    }  
}
```

```
    var requestUrl = protocol + '://' + host + uri + '?' + canonicalQueryString;
    return requestUrl;
};
```

Per creare una richiesta Signature Version 4

1. Crea una richiesta canonica Signature Version 4.

Il codice JavaScript seguente crea una richiesta canonica:

```
var datetime = AWS.util.date.iso8601(new Date()).replace(/[:\ -]|\\.d{3}/g, '');
var date = datetime.substr(0, 8);

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

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

var canonicalHeaders = 'host:' + host + '\n';
var payloadHash = AWS.util.crypto.sha256('', 'hex')
var canonicalRequest = method + '\n' + uri + '\n' + canonicalQueryString + '\n' +
  canonicalHeaders + '\nhost\n' + payloadHash;
```

2. Crea una stringa per firmare, generare una chiave di firma e firmare la stringa.

Assembra l'URL canonico creato nella fase precedente in una stringa da firmare. A questo scopo, crea una stringa costituita dall'algoritmo hash, la data, l'ambito delle credenziali e l'SHA della richiesta canonica. Genera quindi la chiave di firma e firma la stringa, come mostrato nel codice JavaScript seguente.

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

3. Aggiungi le informazioni sulla firma alla richiesta.

Il codice JavaScript seguente mostra come aggiungere le informazioni sulla firma alla stringa di query.

```
canonicalQueryString += '&X-Amz-Signature=' + signature;
```

4. Se hai credenziali per la sessione (da un server STS, AssumeRole o Amazon Cognito), aggiungi il token della sessione alla fine della stringa dell'URL dopo la firma:

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

5. Aggiungi come prefisso il protocollo, l'host e l'URI a canonicalQueryString:

```
var requestUrl = protocol + '://' + host + uri + '?' + canonicalQueryString;
```

6. Apri il WebSocket.

Il codice JavaScript seguente mostra come creare un client MQTT Paho e chiamare CONNECT in AWS IoT. L'argomento endpoint è il tuo endpoint specifico dell'account AWS. clientId è un identificatore di testo univoco tra tutti i client connessi contemporaneamente nell'account AWS.

```
var client = new Paho.MQTT.Client(requestUrl, clientId);
var connectOptions = {
    onSuccess: function(){
        // connect succeeded
    },
    useSSL: true,
    timeout: 3,
    mqttVersion: 4,
    onFailure: function() {
        // connect failed
    }
};
client.connect(connectOptions);
```

Uso del protocollo WebSocket in un'applicazione per dispositivi mobili

Ti consigliamo di usare uno degli SDK di dispositivo AWS IoT per connettere il dispositivo ad AWS IoT quando stabilisci una connessione WebSocket. Gli SDK di dispositivo AWS IoT indicati di seguito supportano le connessioni MQTT basate su WebSocket ad AWS IoT:

- [Node.js](#)
- [iOS](#)
- [Android](#)

Per un'implementazione di riferimento per connettere un'applicazione Web ad AWS IoT usando MQTT tramite il protocollo WebSocket, consulta l'[esempio WebSocket per AWS Labs](#).

Se usi un linguaggio di programmazione o di scripting che non è attualmente supportato, puoi utilizzare qualsiasi libreria WebSocket esistente, purché la richiesta di aggiornamento WebSocket iniziale (HTTP POST) sia firmata tramite Signature Version 4. Alcuni client MQTT, come [Eclipse Paho per JavaScript](#), supportano il protocollo WebSocket in modo nativo.

Regole per AWS IoT

Le regole permettono ai dispositivi di interagire con i servizi AWS. Le regole vengono analizzate e vengono eseguite operazioni in base al flusso di argomenti MQTT. È possibile usare le regole a supporto di attività come le seguenti:

- Aumentare o filtrare i dati ricevuti da un dispositivo.
- Scrivere i dati ricevuti da un dispositivo in un database Amazon DynamoDB.
- Salvare un file in Amazon S3.
- Inviare una notifica push a tutti gli utenti usando Amazon SNS.
- Pubblicare dati in una coda Amazon SQS.
- Richiamare una funzione Lambda per estrarre i dati.
- Elaborare i messaggi da un numero elevato di dispositivi con Amazon Kinesis.
- Inviare dati ad Amazon Elasticsearch Service.
- Acquisire un parametro CloudWatch.
- Modificare un allarme CloudWatch.
- Inviare i dati da un messaggio MQTT ad Amazon Machine Learning per effettuare previsioni in base a un modello Amazon ML.
- Inviare un messaggio a un flusso di input Salesforce IoT.
- Inviare dati dei messaggi a un canale AWS IoT Analytics.
- Avviare l'esecuzione di una macchina a stati Step Functions.
- Inviare i dati del messaggio a un messaggio di input AWS IoT Events.

Le regole possono utilizzare i messaggi MQTT che passano attraverso la pubblicazione/sottoscrizione [Broker di messaggi per AWS IoT \(p. 239\)](#) oppure, utilizzando la caratteristica [Basic Ingest \(p. 333\)](#), è possibile inviare in modo sicuro i dati del dispositivo ai servizi AWS elencati sopra, senza dover sostenere i [costi di messaggistica](#). La caratteristica [Basic Ingest \(p. 333\)](#) ottimizza il flusso di dati rimuovendo il broker di messaggi di pubblicazione/sottoscrizione dal percorso di inserimento per una maggiore efficacia in termini di costi, pur mantenendo la sicurezza e le caratteristiche di elaborazione dei dati di AWS IoT.

Affinché AWS IoT possa eseguire queste operazioni, deve disporre dell'autorizzazione di accesso alle risorse AWS per tuo conto. Quando le operazioni vengono eseguite, vengono addebitati i costi standard per i servizi AWS usati.

Concessione dell'accesso richiesto ad AWS IoT

Puoi usare i ruoli IAM per controllare le risorse AWS a cui ogni regola può accedere. Prima di creare una regola, devi creare un ruolo IAM con una policy che permette l'accesso alle risorse AWS necessarie. AWS IoT assume questo ruolo durante l'esecuzione di una regola.

Per creare un ruolo IAM (AWS CLI)

1. Salva il documento di policy di trust seguente, che concede ad AWS IoT l'autorizzazione ad assumere il ruolo, in un file denominato `iot-role-trust.json`:

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

```
        "Effect": "Allow",
        "Principal": [
            "Service": "iot.amazonaws.com"
        ],
        "Action": "sts:AssumeRole"
    }]
}
```

Usa il comando [create-role](#) per creare un ruolo IAM specificando il file iot-role-trust.json:

```
aws iam create-role --role-name my-iot-role --assume-role-policy-document file://iot-role-trust.json
```

L'output di questo comando è simile al seguente:

```
{
  "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. Salva il codice JSON seguente in un file denominato iot-policy.json.

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

Questo codice JSON rappresenta un esempio di documento di policy che concede all'amministratore di AWS IoT l'accesso a DynamoDB.

Usa il comando [create-policy](#) per concedere ad AWS IoT l'accesso alle risorse AWS dopo l'assunzione del ruolo, passando il file iot-policy.json:

```
aws iam create-policy --policy-name my-iot-policy --policy-document file://my-iot-policy.json
```

Per ulteriori informazioni su come concedere l'accesso ai servizi AWS nelle policy per AWS IoT, consulta [Creazione di una regola AWS IoT \(p. 256\)](#).

L'output del comando [create-policy](#) contiene l'ARN della policy. È necessario collegare la policy a un ruolo.

```
{
  "Policy": {
    "PolicyName": "my-iot-policy",
    "CreateDate": "2015-09-30T19:31:18.620Z",
    "AttachmentCount": 0,
    "IsAttachable": true,
    "PolicyId": "ZXR6A36LTYANPAI7NJ5UV",
    "Arn": "arn:aws:iam::123456789012:policy/my-iot-policy"
  }
}
```

```
        "DefaultVersionId": "v1",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:policy/my-iot-policy",
        "UpdateDate": "2015-09-30T19:31:18.620Z"
    }
}
```

3. Usa il comando [attach-role-policy](#) per collegare la policy a un ruolo:

```
aws iam attach-role-policy --role-name my-iot-role --policy-arn
"arn:aws:iam::123456789012:policy/my-iot-policy"
```

Passaggio delle autorizzazioni di un ruolo

Parte di una definizione di regola è costituita da un ruolo IAM che concede l'autorizzazione di accesso alle risorse specificate nell'operazione della regola. Il motore di regole presuppone l'uso del ruolo quando l'operazione della regola viene attivata. Il ruolo deve essere definito nello stesso account AWS della regola.

Quando crei o sostituisci una regola, in realtà passi un ruolo al motore di regole. L'utente che esegue questa operazione deve disporre dell'autorizzazione `iam:PassRole`. Per assicurarti di disporre di questa autorizzazione, crea una policy che concede l'autorizzazione `iam:PassRole` e collegala al tuo utente IAM. La policy seguente mostra come concedere l'autorizzazione `iam:PassRole` per un ruolo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::123456789012:role/myRole"
            ]
        }
    ]
}
```

In questa policy di esempio viene concessa l'autorizzazione `iam:PassRole` al ruolo `myRole`. Il ruolo viene specificato usando l'ARN del ruolo. È necessario collegare questa policy all'utente IAM o al ruolo a cui l'utente appartiene. Per ulteriori informazioni, consulta la sezione relativa all'[utilizzo di policy gestite](#).

Note

Le funzioni Lambda usano una policy basata sulle risorse, in cui la policy è collegata direttamente alla funzione Lambda stessa. Quando crei una regola che invoca una funzione Lambda, non trasferisci un ruolo; pertanto, l'utente che crea la regola non richiede l'autorizzazione `iam:PassRole`. Per ulteriori informazioni sull'autorizzazione per la funzione Lambda, consulta la pagina relativa alla [concessione di autorizzazioni usando una policy per le risorse](#).

Creazione di una regola AWS IoT

È possibile configurare regole per instradare i dati dagli oggetti connessi. Le regole sono costituite dagli elementi seguenti:

Nome regola

Nome della regola.

Note

Non è consigliabile utilizzare informazioni di identificazione personale nei nomi delle regole.

Descrizione facoltativa

Descrizione di testo della regola.

Note

Non è consigliabile utilizzare informazioni di identificazione personale nelle descrizioni delle regole.

Istruzione SQL

Sintassi SQL semplificata per filtrare i messaggi ricevuti in un argomento MQTT ed effettuare il push dei dati in un'altra posizione. Per ulteriori informazioni, consulta [Documentazione di riferimento su SQL per AWS IoT \(p. 279\)](#).

Versione SQL

Versione del motore di regole SQL da usare durante la valutazione della regola. Anche se questa proprietà è facoltativa, è consigliabile specificare la versione SQL. Se questa proprietà non è impostata, viene usato il valore predefinito 2015-10-08. Per ulteriori informazioni, consulta [Versioni SQL \(p. 330\)](#).

Una o più operazioni

Le operazioni che AWS IoT esegue quando esegue la regola. Puoi ad esempio inserire i dati in una tabella DynamoDB, scrivere i dati in un bucket Amazon S3, eseguire la pubblicazione in un argomento Amazon SNS o richiamare una funzione Lambda.

Un'operazione in caso di errore

L'operazione che AWS IoT esegue quando non è in grado di eseguire un'operazione di una regola.

Quando crei una regola, fai attenzione alla quantità di dati pubblicati negli argomenti. Se crei regole che includono un modello di argomento con caratteri jolly che potrebbe corrispondere a una elevata percentuale di messaggi, potrebbe essere necessario aumentare la capacità delle risorse AWS usate dalle operazioni target. Se inoltre crei una regola di ripubblicazione che include un modello di argomento con caratteri jolly, si potrebbe creare una regola circolare che provoca un ciclo infinito.

Note

La creazione e l'aggiornamento di regole sono operazioni a livello di amministratore. Qualsiasi utente che abbia l'autorizzazione per creare o aggiornare regole potrà accedere ai dati elaborati dalle regole.

Per creare una regola AWS CLI

Usa il comando [create-topic-rule](#) per creare una regola:

```
aws iot create-topic-rule --rule-name my-rule --topic-rule-payload file://my-rule.json
```

Di seguito è riportato un esempio di file di payload con una regola che inserisce tutti i messaggi inviati all'argomento `iot/test` nella tabella DynamoDB specificata. L'istruzione SQL filtra i messaggi e l'ARN del ruolo concede ad AWS IoT l'autorizzazione di scrittura nella tabella DynamoDB.

```
{
```

```
"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()}"  
        }  
    }  
]
```

Di seguito è riportato un esempio di file di payload con una regola che inserisce tutti i messaggi inviati all'argomento `iot/test` nel bucket S3 specificato. L'istruzione SQL filtra i messaggi e l'ARN del ruolo concede ad AWS IoT l'autorizzazione di scrittura nella bucket Amazon S3.

```
{  
    "awsIotSqlVersion": "2016-03-23",  
    "sql": "SELECT * FROM 'iot/test'",  
    "ruleDisabled": false,  
    "actions": [  
        {  
            "s3": {  
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_s3",  
                "bucketName": "my-bucket",  
                "key": "myS3Key"  
            }  
        }  
    ]  
}
```

Di seguito è riportato un esempio di file di payload con una regola che effettua il push dei dati ad Amazon Elasticsearch Service:

```
{  
    "sql": "SELECT *, timestamp() as timestamp FROM 'iot/test'",  
    "ruleDisabled": false,  
    "awsIotSqlVersion": "2016-03-23",  
    "actions": [  
        {  
            "elasticsearch": {  
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_es",  
                "endpoint": "https://my-endpoint",  
                "index": "my-index",  
                "type": "my-type",  
                "id": "${newuuid()}"  
            }  
        }  
    ]  
}
```

Di seguito è riportato un esempio di file di payload con una regola che richiama una funzione Lambda:

```
{  
    "sql": "expression",  
    "ruleDisabled": false,  
    "awsIotSqlVersion": "2016-03-23",  
    "actions": [  
        {"lambda": {  
            "functionArn": "arn:aws:lambda:eu-west-1:123456789012:function:my-lambda-function"  
        }}  
    ]  
}
```

```
        "functionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-lambda-
function"
    }
}
}
```

Di seguito è riportato un esempio di file di payload con una regola che esegue la pubblicazione in un argomento Amazon SNS:

```
{
  "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"
      }
    }
  ]
}
```

Di seguito è riportato un esempio di file di payload con una regola che esegue la ripubblicazione in un argomento MQTT diverso:

```
{
  "sql": "expression",
  "ruleDisabled": false,
  "awsIotSqlVersion": "2016-03-23",
  "actions": [
    {
      "republish": {
        "topic": "my-mqtt-topic",
        "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"
      }
    }
  ]
}
```

Di seguito è riportato un esempio di file di payload con una regola che effettua il push dei dati in un flusso Amazon Kinesis Data Firehose:

```
{
  "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"
      }
    }
  ]
}
```

Di seguito è riportato un esempio di file di payload con una regola che usa la funzione Amazon Machine Learning di `machinelearning_predict` per eseguire la ripubblicazione in un argomento se i dati contenuti nel payload MQTT vengono classificati con valore 1.

```
{
  "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"}}, {"actions": [{"salesforce": {"token": "ABCDEFGHI123456789abcdefghi123456789", "url": "https://ingestion-cluster-id.my-env.sfdcnow.com/streams/stream-id/connection-id/my-event"}]}]}
```

Di seguito è riportato un esempio di file di payload con una regola che pubblica messaggi in un flusso di input Salesforce IoT Cloud.

```
{ "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"}]}]}
```

Di seguito è riportato un esempio di file di payload con una regola che avvia un'esecuzione di una macchina a stati Step Functions.

```
{ "sql": "expression", "ruleDisabled": false, "awsIotSqlVersion": "2016-03-23", "actions": [{"stepFunctions": {"stateMachineName": "myCoolStateMachine", "executionNamePrefix": "coolRunning", "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"}]}]}
```

Visualizzazione delle regole

Usa il comando [list-topic-rules](#) per elencare le regole:

```
aws iot list-topic-rules
```

Usa il comando [get-topic-rule](#) per ottenere informazioni su una regola:

```
aws iot get-topic-rule --rule-name my-rule
```

Eliminazione di una regola

Quando una regola non è più necessaria, è possibile eliminarla.

Per eliminare una regola (AWS CLI)

Usa il comando [delete-topic-rule](#) per eliminare una regola:

```
aws iot delete-topic-rule --rule-name my-rule
```

Operazioni delle regole AWS IoT

Le operazioni delle regole AWS IoT vengono usate per specificare cosa fare quando viene attivata una regola. È possibile definire operazioni per scrivere i dati in un database DynamoDB o in un flusso Kinesis oppure per richiamare una funzione Lambda e molto altro. Sono supportate le operazioni seguenti:

- `cloudwatchAlarm` per modificare un allarme CloudWatch.
- `cloudwatchMetric` per acquisire un parametro CloudWatch.
- `dynamoDB` per scrivere i dati in un database DynamoDB.
- `dynamoDBv2` per scrivere i dati in un database DynamoDB.
- `elasticsearch` per scrivere i dati in un dominio Amazon Elasticsearch Service.
- `firehose` per scrivere i dati in un flusso Amazon Kinesis Data Firehose.
- `iotAnalytics` per inviare dati a un canale AWS IoT Analytics.
- `iotEvents` per inviare dati a un input AWS IoT Events.
- `kinesis` per scrivere i dati in un flusso Kinesis.
- `lambda` per richiamare una funzione Lambda.
- `republish` per ripubblicare il messaggio in un altro argomento MQTT.
- `s3` per scrivere i dati in un bucket Amazon S3.
- `salesforce` per scrivere un messaggio in un flusso di input Salesforce IoT.
- `sns` per scrivere i dati come notifiche push.
- `sqs` per scrivere i dati in una coda SQS.
- `stepFunctions` per avviare l'esecuzione di una macchina a stati Step Functions.

Note

Il motore di regole AWS IoT potrebbe eseguire più tentativi di esecuzione di un'operazione in caso di errori intermittenti. Se tutti i tentativi hanno esito negativo, il messaggio viene eliminato e l'errore viene riportato nei log CloudWatch. È possibile specificare un'operazione di errore per ciascuna regola che viene invocata quando si verifica un errore. Per ulteriori informazioni, consulta [Gestione degli errori \(operazione in caso di errore\) \(p. 277\)](#).

Ogni operazione viene descritta in modo dettagliato.

Operazione per gli allarmi CloudWatch

CloudWatch Alarm Action

L'operazione relativa agli allarmi CloudWatch permette di modificare lo stato di un allarme CloudWatch.

In questa chiamata è possibile specificare il motivo della modifica dello stato e il valore.

[more info \(1\)](#)

Quando crei una regola AWS IoT con un'operazione relativa agli allarmi CloudWatch, devi specificare le informazioni seguenti:

roleArn

Ruolo IAM che permette l'accesso all'allarme CloudWatch.

alarmName

Nome dell'allarme CloudWatch.

stateReason

Motivo della modifica dell'allarme.

stateValue

Valore dello stato dell'allarme. I valori accettabili sono OK, ALARM, INSUFFICIENT_DATA.

Note

Verifica che il ruolo associato alla regola disponga di una policy che concede l'autorizzazione cloudwatch:SetAlarmState.

L'esempio JSON seguente illustra come definire un'operazione relativa agli allarmi CloudWatch in una regola AWS IoT:

```
{  
    "topicRulePayload": {  
        "sql": "SELECT * FROM 'some/topic'",  
        "ruleDisabled": false,  
        "awsIotSqlVersion": "2016-03-23",  
        "actions": [  
            {  
                "cloudwatchAlarm": {  
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_cw",  
                    "alarmName": "IoTAlarm",  
                    "stateReason": "Temperature stabilized.",  
                    "stateValue": "OK"  
                }  
            }  
        ]  
    }  
}
```

Per ulteriori informazioni, consulta [Allarmi CloudWatch](#).

Operazione per i parametri CloudWatch

CloudWatch Metric Action

L'operazione relativa ai parametri CloudWatch permette di acquisire un parametro CloudWatch. È possibile specificare namespace, nome, valore, unità e timestamp per il parametro.

[more info \(2\)](#)

Quando crei una regola AWS IoT con un'operazione relativa ai parametri CloudWatch, devi specificare le informazioni seguenti:

roleArn

Ruolo IAM che permette l'accesso al parametro CloudWatch.

metricNamespace

Nome del namespace parametro CloudWatch.

metricName

Nome del parametro CloudWatch.

metricValue

Valore del parametro CloudWatch.

metricUnit

Unità di misura del parametro supportata da CloudWatch.

metricTimestamp

Timestamp Unix opzionale.

Note

Verifica che il ruolo associato alla regola disponga di una policy che concede l'autorizzazione `cloudwatch:PutMetricData`.

L'esempio JSON seguente illustra come definire un'operazione relativa ai parametri CloudWatch in una regola AWS IoT:

```
{  
    "topicRulePayload": {  
        "sql": "SELECT * FROM 'some/topic'",  
        "ruleDisabled": false,  
        "awsIotSqlVersion": "2016-03-23",  
        "actions": [  
            {  
                "cloudwatchMetric": {  
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_cw",  
                    "metricNamespace": "IoTNamespace",  
                    "metricName": "IoTMetric",  
                    "metricValue": "1",  
                    "metricUnit": "Count",  
                    "metricTimestamp": "1456821314"  
                }  
            }  
        ]  
    }  
}
```

Per ulteriori informazioni, [Parametri CloudWatch](#).

Operazione DynamoDB

DynamoDB Action

L'operazione `dynamoDB` permette di scrivere, completamente o in parte, un messaggio MQTT in una tabella DynamoDB.

[more info \(3\)](#)

Quando crei una regola DynamoDB, devi specificare le informazioni seguenti:

hashKeyType

Tipo di dati della chiave hash (detta anche chiave di partizione). I valori validi sono: `"STRING"` e `"NUMBER"`.

hashKeyField

Nome della chiave hash (detta anche chiave di partizione).

hashKeyValue

Valore della chiave hash.

rangeKeyType

Opzionale. Tipo di dati della chiave di intervallo (detta anche chiave di ordinamento). I valori validi sono: "STRING" e "NUMBER".

rangeKeyField

Opzionale. Nome della chiave di intervallo (detta anche chiave di ordinamento).

rangeKeyValue

Opzionale. Valore della chiave di intervallo.

operation

Opzionale. Tipo di operazione da eseguire. Segue il modello di sostituzione, per cui può essere \${operation}, ma la sostituzione deve restituire uno dei risultati seguenti: INSERT, UPDATE o DELETE.

payloadField

Opzionale. Nome del campo in cui viene scritto il payload. Se questo valore viene omesso, il payload viene scritto nel campo `payload`.

tabella

Nome della tabella DynamoDB.

roleARN

Ruolo IAM che permette l'accesso alla tabella DynamoDB. Il ruolo deve permettere almeno l'operazione `AmazonDynamoDB:PutItem`.

I dati scritti nella tabella DynamoDB sono il risultato dell'istruzione SQL della regola. I campi `hashKeyValue` e `rangeKeyValue` sono in genere costituiti da espressioni (ad esempio `"${topic()}"` o `"${timestamp()}"`).

Note

I dati non JSON vengono scritti in DynamoDB come dati binari. La console DynamoDB mostra i dati come testo con codifica Base64.

Verifica che il ruolo associato alla regola disponga di una policy che conceda l'autorizzazione dynamodb:PutItem.

L'esempio JSON seguente illustra come definire un'operazione dynamodb in una regola AWS IoT:

```
{  
    "topicRulePayload": {  
        "ruleDisabled": false,  
        "sql": "SELECT * AS message FROM 'some/topic'",  
        "description": "A test Dynamo DB rule",  
        "awsIotSqlVersion": "2016-03-23",  
        "actions": [  
            "dynamoDB": {  
                "hashKeyField": "key",  
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_dynamoDB"
```

```
        "tableName": "my_ddb_table",
        "hashKeyValue": "${topic()}",
        "rangeKeyValue": "${timestamp()}",
        "rangeKeyField": "timestamp"
    }
}
}
```

Per ulteriori informazioni, consulta la [Guida alle operazioni di base di Amazon DynamoDB](#).

Operazione DynamoDBv2

DynamoDBv2 Action

L'operazione `dynamoDBv2` permette di scrivere, completamente o in parte, un messaggio MQTT in una tabella DynamoDB. Ogni attributo nel payload viene scritto in una colonna separata del database DynamoDB.

[more info \(4\)](#)

Quando crei una regola DynamoDB, devi specificare le informazioni seguenti:

`roleARN`

Ruolo IAM che permette l'accesso alla tabella DynamoDB. Il ruolo deve permettere almeno l'operazione IAM `dynamoDB:PutItem`.

`tableName`

Nome della tabella DynamoDB.

`Note`

Il payload del messaggio MQTT deve contenere una chiave di livello root corrispondente alla chiave di partizione primaria della tabella e una chiave di livello root corrispondente alla chiave di ordinamento primaria della tabella, se definita.

I dati scritti nella tabella DynamoDB sono il risultato dell'istruzione SQL della regola.

`Note`

Verifica che il ruolo associato alla regola disponga di una policy che concede l'autorizzazione `dynamodb:PutItem`.

L'esempio JSON seguente illustra come definire un'operazione `dynamoDB` in una regola AWS IoT:

```
{
    "topicRulePayload": {
        "sql": "SELECT * AS message FROM 'some/topic'",
        "ruleDisabled": false,
        "description": "A test DynamoDBv2 rule",
        "awsIotSqlVersion": "2016-03-23",
        "actions": [
            "dynamoDBv2": {
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_dynamoDBv2",
                "putItem": {
                    "tableName": "my_ddb_table"
                }
            }
        ]
    }
}
```

```
        }
    }]
}
```

Per ulteriori informazioni, consulta la [Guida alle operazioni di base di Amazon DynamoDB](#).

Operazione Elasticsearch

Elasticsearch Action

L'operazione `elasticsearch` permette di scrivere i dati dai messaggi MQTT a un dominio Amazon Elasticsearch Service. È quindi possibile eseguire query sui dati in Elasticsearch e visualizzare tali dati usando strumenti come Kibana.

[more info \(5\)](#)

Quando crei una regola AWS IoT con un'operazione `elasticsearch`, devi specificare le informazioni seguenti:

`endpoint`

Endpoint del dominio Amazon Elasticsearch Service.

`index`

Indice Elasticsearch in cui archiviare i dati.

`type`

Tipo di documento che stai archiviando.

`id`

Identificatore univoco per ogni documento.

Note

Verifica che il ruolo associato alla regola disponga di una policy che concede l'autorizzazione `es:ESHttpPut`.

L'esempio JSON seguente illustra come definire un'operazione `elasticsearch` in una regola AWS IoT:

```
{
  "topicRulePayload": {
    "sql": "SELECT *, timestamp() as timestamp FROM 'iot/test'",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
      {
        "elasticsearch": {
          "roleArn": "arn:aws:iam::123456789012:role/aws_iot_es",
          "endpoint": "https://my-endpoint",
          "index": "my-index",
          "type": "my-type",
          "id": "${newuuid()}"
        }
      }
    ]
  }
}
```

Per ulteriori informazioni, consulta la [Guida per sviluppatori di Amazon Elasticsearch Service](#).

Operazione Firehose

Firehose Action

Un'operazione `firehose` invia i dati da un messaggio MQTT che ha attivato la regola a un flusso Kinesis Data Firehose.

[more info \(6\)](#)

Quando crei una regola con un'operazione `firehose`, devi specificare le informazioni seguenti:

`deliveryStreamName`

Flusso Kinesis Data Firehose in cui scrivere i dati del messaggio.

`roleArn`

Ruolo IAM che permette l'accesso a Kinesis Data Firehose.

`separator`

Separatore di caratteri usato per separare i record scritti nel flusso Kinesis Data Firehose. I valori validi sono: '\n' (nuova riga), '\t' (tabulazione), '\r\n' (nuova riga Windows), ',' (virgola).

Note

Verifica che il ruolo associato alla regola disponga di una policy che concede l'autorizzazione `firehose:PutRecord`.

L'esempio JSON seguente illustra come creare una regola AWS IoT con un'operazione `firehose`:

```
{  
    "topicRulePayload": {  
        "sql": "SELECT * FROM 'some/topic'",  
        "ruleDisabled": false,  
        "awsIotSqlVersion": "2016-03-23",  
        "actions": [  
            {"  
                "firehose": {  
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_firehose",  
                    "deliveryStreamName": "my_firehose_stream"  
                }  
            }  
        ]  
    }  
}
```

Per ulteriori informazioni, consulta la [Guida per sviluppatori di Kinesis Data Firehose](#).

Operazione IoT Analytics

IoT Analytics Action

Un'operazione `iotAnalytics` invia i dati dal messaggio MQTT che ha attivato la regola a un canale AWS IoT Analytics.

[more info \(7\)](#)

Quando crei una regola con un'operazione `iotAnalytics`, devi specificare le informazioni seguenti:

channelName

Il nome del canale AWS IoT Analytics in cui scrivere i dati.

roleArn

Ruolo IAM che permette l'accesso al canale AWS IoT Analytics.

La policy associata al ruolo specificato sarà simile alla seguente:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "iotanalytics:BatchPutMessage",  
            "Resource": [  
                "arn:aws:iotanalytics:us-west-2:<your-account-number>:channel/  
mychannel"  
            ]  
        }  
    ]  
}
```

e avrà una relazione di trust simile alla seguente:

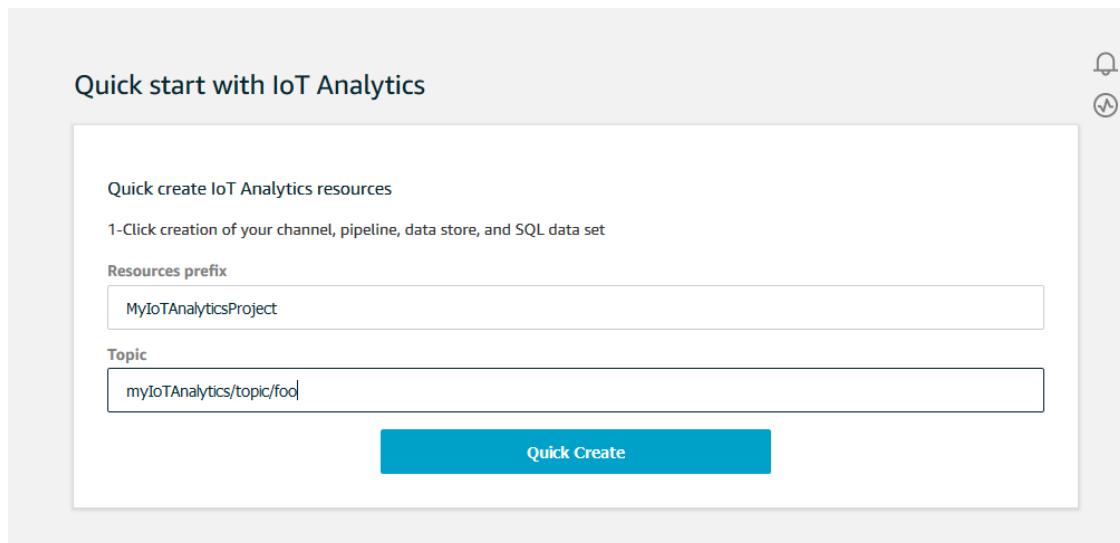
```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "iot.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole",  
        }  
    ]  
}
```

L'esempio JSON seguente illustra come creare una regola AWS IoT con un'operazione `iotAnalytics`:

```
{  
    "topicRulePayload": {  
        "sql": "SELECT * FROM 'some/topic'",  
        "ruleDisabled": false,  
        "awsIotSqlVersion": "2016-03-23",  
        "actions": [  
            {  
                "iotAnalytics": {  
                    "channelName": "mychannel",  
                    "roleArn": "arn:aws:iam::123456789012:role/analyticsRole",  
                }  
            }  
        ]  
    }  
}
```

Per ulteriori informazioni, consulta la [Guida per l'utente AWS IoT Analytics](#).

La console AWS IoT Analytics offre anche una funzione Quick Start che consente di creare un canale, i dati archiviati, pipeline e dati con un solo clic. Cerca questa pagina quando immetti la console di AWS IoT Analytics:



Operazione IoT Events

IoT Events Action

Un'operazione `iotEvents` invia i dati dal messaggio MQTT che ha attivato la regola a un input AWS IoT Events.

[more info \(8\)](#)

Quando crei una regola con un'operazione `iotEvents`, devi specificare le informazioni seguenti:

`inputName`

Nome dell'input AWS IoT Events.

`messageId`

Opzionale. Da utilizzare per essere certi che il rilevatore AWS IoT Events elabori un solo messaggio di input con un determinato `messageId`.

`roleArn`

ARN del ruolo che concede l'autorizzazione AWS IoT per l'invio di un input a un rilevatore AWS IoT Events. ("Action": "iotevents:BatchPutMessage").

Di seguito è riportato un esempio di policy di attendibilità che dovrebbe essere collegata al ruolo:

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

L'esempio JSON seguente illustra come creare una regola AWS IoT con un'operazione `iotEvents`:

```
{
```

```
"topicRulePayload": {  
    "sql": "expression",  
    "ruleDisabled": false,  
    "description": "An AWS IoT Events test rule",  
    "awsIotSqlVersion": "2016-03-23",  
    "actions": [  
        {"  
            "iotEvents": {  
                "inputName": "MyIoTEventsInput",  
                "messageId": "1234567890",  
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_events"  
            },  
        }  
    ]  
}
```

Per ulteriori informazioni, consulta il documento [Guida per sviluppatori di AWS IoT Events](#).

Operazione Kinesis

Kinesis Action

L'operazione `kinesis` permette di scrivere i dati dai messaggi MQTT in un flusso Kinesis.

[more info \(9\)](#)

Quando crei una regola AWS IoT con un'operazione `kinesis`, devi specificare le informazioni seguenti:

stream

Flusso Kinesis in cui scrivere i dati.

partitionKey

Chiave di partizione usata per determinare in quale shard vengono scritti i dati. La chiave di partizione è in genere composta da un'espressione (ad esempio, "\${topic()}" o "\${timestamp()}").

Note

Verifica che la policy associata alla regola disponga dell'autorizzazione `kinesis:PutRecord`.

L'esempio JSON seguente illustra come definire un'operazione `kinesis` in una regola AWS IoT:

```
{  
    "topicRulePayload": {  
        "sql": "SELECT * FROM 'some/topic'",  
        "ruleDisabled": false,  
        "awsIotSqlVersion": "2016-03-23",  
        "actions": [  
            {"  
                "kinesis": {  
                    "roleArn": "arn:aws:iam::123456789012:role/aws_iot_kinesis",  
                    "streamName": "my_kinesis_stream",  
                    "partitionKey": "${topic()}"  
                },  
            }  
        ]  
    }  
}
```

Per ulteriori informazioni, consulta la [Guida per sviluppatori di Kinesis](#).

Operazione Lambda

Lambda Action

Un'operazione lambda chiama una funzione Lambda passando il messaggio MQTT che ha attivato la regola.

[more info \(10\)](#)

Affinché AWS IoT possa chiamare una funzione Lambda, è necessario configurare una policy che conceda l'autorizzazione `lambda:InvokeFunction` a AWS IoT. Le funzioni Lambda usano policy basate sulle risorse, quindi è necessario collegare la policy alla funzione Lambda. Usa il comando dell'interfaccia a riga di comando seguente per collegare una policy che concede l'autorizzazione `lambda:InvokeFunction`:

```
aws lambda add-permission --function-name "function_name" --region "region" --principal iot.amazonaws.com --source-arn arn:aws:iot:us-east-2:account_id:rule/rule_name --source-account "account_id" --statement-id "unique_id" --action "lambda:InvokeFunction"
```

Di seguito sono illustrati gli argomenti per il comando `add-permission`:

`--function-name`

Nome della funzione Lambda di cui viene aggiornata la policy per le risorse aggiungendo una nuova autorizzazione.

`--region`

Regione AWS dell'account.

`--principal`

Entità principale che riceve l'autorizzazione. Deve trattarsi di `iot.amazonaws.com` per concedere ad AWS IoT l'autorizzazione per chiamare una funzione Lambda.

`--source-arn`

ARN della regola. Usa il comando `get-topic-rule` dell'interfaccia a riga di comando per ottenere l'ARN di una regola.

`--source-account`

Account AWS in cui la regola è definita.

`--statement-id`

Identificatore univoco di un'istruzione.

`--action`

Operazione Lambda da consentire nell'istruzione. Per consentire a AWS IoT di invocare una funzione Lambda, specificare `lambda:InvokeFunction`.

Note

Se si aggiunge un'autorizzazione per un'entità principale AWS IoT senza fornire l'ARN di origine, qualsiasi account AWS che crea una regola con l'operazione Lambda può attivare regole per invocare la funzione Lambda da AWS IoT.

Per ulteriori informazioni, consulta la pagina relativa al [modello di autorizzazioni Lambda](#).

Quando crei una regola con un'operazione `lambda`, devi specificare la funzione Lambda da richiamare quando la regola viene attivata.

L'esempio JSON seguente illustra una regola che chiama una funzione Lambda:

```
{  
    "topicRulePayload": {  
        "sql": "SELECT * FROM 'some/topic'",  
        "ruleDisabled": false,  
        "awsIotSqlVersion": "2016-03-23",  
        "actions": [  
            {"  
                "lambda": {  
                    "functionArn": "arn:aws:lambda:us-  
east-2:123456789012:function:myLambdaFunction"  
                }  
            }  
        ]  
    }  
}
```

Se non si specifica una versione o un alias per la funzione Lambda, viene eseguita la versione più recente della funzione. È possibile specificare una versione o un alias se si desidera eseguire una versione specifica della funzione Lambda. Per specificare una versione o un alias, aggiungere la versione o l'alias all'ARN della funzione Lambda. Ad esempio:

```
"arn:aws:lambda:us-east-2:123456789012:function:myLambdaFunction:someAlias"
```

Per ulteriori informazioni sulla funzione Versioni multiple e sugli alias, consulta [Funzione Versioni multiple e alias nella AWS Lambda](#). Per ulteriori informazioni su AWS Lambda, consulta la [Guida per gli sviluppatori di AWS Lambda](#).

Operazione Republish

Republish Action

L'operazione `republish` permette di ripubblicare il messaggio che ha attivato il ruolo in un altro argomento MQTT.

[more info \(11\)](#)

Quando crei una regola con un'operazione `republish`, devi specificare le informazioni seguenti:

argomento

Argomento MQTT in cui ripubblicare il messaggio. Se stai ripubblicando in un argomento riservato, per quello che inizia con \$ utilizza invece \$\$. Ad esempio, se si sta ripubblicando in un argomento Device Shadow come `$aws/things/MyThing/shadow/update`, è necessario specificare l'argomento come `$$aws/things/MyThing/shadow/update`.

roleArn

Ruolo IAM che permette la pubblicazione nell'argomento MQTT.

Note

Verifica che il ruolo associato alla regola disponga di una policy che concede l'autorizzazione `iot:Publish`.

```
{  
    "topicRulePayload": {  
        "sql": "SELECT * FROM 'some/topic'",  
        "ruleDisabled": false,  
        "awsIotSqlVersion": "2016-03-23",  
        "actions": [  
            {"  
                "lambda": {  
                    "functionArn": "arn:aws:lambda:us-  
east-2:123456789012:function:myLambdaFunction"  
                }  
            }  
        ]  
    }  
}
```

```
    "ruleDisabled": false,  
    "awsIotSqlVersion": "2016-03-23",  
    "actions": [  
        {  
            "republish": {  
                "topic": "another/topic",  
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_republish"  
            }  
        }  
    ]  
}
```

Operazione S3

S3 Action

Un'operazione s3 scrive i dati provenienti dal messaggio MQTT che ha attivato la regola in un bucket Amazon S3.

[more info \(12\)](#)

Quando si crea una regola AWS IoT con un'operazione s3, è necessario specificare le informazioni seguenti (ad eccezione di cannedacl, che è opzionale):

bucket

Bucket Amazon S3 in cui scrivere i dati.

cannedacl

Opzionale. Lista di controllo degli accessi predefinita di Amazon S3 che controlla l'accesso all'oggetto identificato dalla chiave dell'oggetto. Per ulteriori informazioni, inclusi i valori consentiti, consulta la pagina relativa alle [liste di controllo degli accessi predefinite S3](#).

key

Percorso del file in cui vengono scritti i dati. Ad esempio, se il valore dell'argomento è "\${topic()}/ \${timestamp()}", l'argomento al quale è stato inviato il messaggio è "this/is/my/topic,". Se il timestamp corrente è 1460685389, i dati vengono scritti in un file denominato "1460685389" nella cartella "this/is/my/topic" in Amazon S3.

Note

Se si usa una chiave statica, viene sovrascritto un singolo file in Amazon S3 per ogni chiamata della regola. Altri casi di utilizzo comuni includono l'uso del timestamp di un messaggio o un altro identificatore univoco del messaggio in modo che, per ogni messaggio ricevuto, venga salvato un nuovo file in Amazon S3.

roleArn

Ruolo IAM che permette l'accesso al bucket Amazon S3.

Note

Verifica che il ruolo associato alla regola disponga di una policy che concede l'autorizzazione s3:PutObject.

L'esempio JSON seguente illustra come definire un'operazione s3 in una regola AWS IoT:

```
{
```

```
"topicRulePayload": {  
    "sql": "SELECT * FROM 'some/topic'",  
    "ruleDisabled": false,  
    "awsIotSqlVersion": "2016-03-23",  
    "actions": [  
        {"  
            "s3": {  
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_s3",  
                "bucketName": "my-bucket",  
                "key": "${topic()}/${timestamp()}"  
                "cannedAcl": "public-read"  
            }  
        }  
    ]  
}
```

Per ulteriori informazioni, consulta la [Guida per sviluppatori di Amazon S3](#).

Operazione Salesforce

Salesforce Action

Un'operazione salesforce invia i dati dal messaggio MQTT che ha attivato la regola a un flusso di input Salesforce IoT.

[more info \(13\)](#)

Quando crei una regola con un'operazione salesforce, devi specificare le informazioni seguenti:

url

URL esposto dal flusso di input Salesforce IoT. L'URL è disponibile dalla piattaforma Salesforce IoT durante la creazione di un flusso di input. Per ulteriori informazioni, consulta la documentazione di Salesforce IoT.

token

Token usato per autenticare l'accesso al flusso di input Salesforce IoT specificato. Il token è disponibile dalla piattaforma Salesforce IoT durante la creazione di un flusso di input. Per ulteriori informazioni, consulta la documentazione di Salesforce IoT.

Note

Questi parametri non supportano la sostituzione.

L'esempio JSON seguente illustra come creare una regola AWS IoT con un'operazione salesforce:

```
{  
    "topicRulePayload": {  
        "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"  
                }  
            }  
        ]  
    }  
}
```

}

Per ulteriori informazioni, consulta la documentazione di Salesforce IoT.

Operazione SNS

SNS Action

Un'operazione sns invia i dati dal messaggio MQTT che ha attivato la regola come notifica push SNS.
[more info \(14\)](#)

Quando crei una regola con un'operazione sns, devi specificare le informazioni seguenti:

messageFormat

Formato del messaggio. I valori accettati sono "JSON" e "RAW". Il valore predefinito dell'attributo è "RAW". SNS usa questa impostazione per determinare se il payload deve essere analizzato e se le parti specifiche della piattaforma rilevanti del payload devono essere estratte.

roleArn

Ruolo IAM che permette l'accesso a SNS.

targetArn

Argomento SNS o singolo dispositivo a cui viene inviata la notifica push.

Note

Verifica che la policy associata alla regola disponga dell'autorizzazione sns:Publish.

L'esempio JSON seguente illustra come definire un'operazione sns in una regola AWS IoT:

```
{  
    "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"  
            }  
        }]  
    }  
}
```

Per ulteriori informazioni, consulta la [Guida per sviluppatori di Amazon SNS](#).

Operazione SQS

SQS Action

Un'operazione sqs invia i dati dal messaggio MQTT che ha attivato la regola a una coda SQS.
[more info \(15\)](#)

Quando crei una regola con un'operazione sqs, devi specificare le informazioni seguenti:

queueUrl

URL della coda SQS in cui scrivere i dati.

useBase64

Imposta il valore su `true` se vuoi che ai dati del messaggio MQTT venga applicata la codifica Base64 prima della scrittura nella coda SQS. In caso contrario, imposta il valore su `false`.

roleArn

Ruolo IAM che permette l'accesso alla coda SQS.

Note

Verifica che il ruolo associato alla regola disponga di una policy che conceda l'autorizzazione `sqs:SendMessage`.

L'esempio JSON seguente illustra come creare una regola AWS IoT con un'operazione `sqs`:

```
{  
    "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_sq",  
                    "useBase64": false  
                }  
            }  
        ]  
    }  
}
```

L'operazione SQS non supporta le [code FIFO di SQS](#). Poiché il motore di regole è un servizio completamente distribuito, non vi è alcuna garanzia in merito all'ordine dei messaggi quando viene attivata l'operazione SQS.

Per ulteriori informazioni, consulta la [Guida per sviluppatori di Amazon SQS](#).

Step Functions Action

Step Functions Action

Un'operazione `stepFunctions` avvia l'esecuzione di una macchina a stati Step Functions.

[more info \(16\)](#)

Quando crei una regola con un'operazione `stepFunctions`, devi specificare le informazioni seguenti:

executionNamePrefix

Opzionale. Il nome assegnato all'esecuzione della macchina a stati è formato da questo prefisso seguito da un UUID. Step Functions crea un nome univoco per ogni esecuzione di macchina a stati, se non viene fornito.

stateMachineName

Nome della macchina a stati Step Functions di cui verrà avviata l'esecuzione.

roleArn

ARN del ruolo che concede a AWS IoT l'autorizzazione per avviare l'esecuzione di una macchina a stati ("Action":"states:StartExecution").

Di seguito è riportato un esempio di policy di attendibilità che dovrebbe essere collegata al ruolo:

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

L'esempio JSON seguente illustra come creare una regola AWS IoT con un'operazione stepFunctions:

```
{  
    "topicRulePayload": {  
        "sql": "expression",  
        "ruleDisabled": false,  
        "description": "A step functions test rule",  
        "awsIoTSqlVersion": "2016-03-23",  
        "actions": [{  
            "stepFunctions": {  
                "executionNamePrefix": "myExecution",  
                "stateMachineName": "myStateMachine",  
                "roleArn": "arn:aws:iam::123456789012:role/aws_iot_step_functions"  
            }  
        }]  
    }  
}
```

Per ulteriori informazioni, consulta la [Guida per sviluppatori Step Functions](#).

Risoluzione dei problemi relativi a una regola

Se si verifica un problema con le regole, abilita CloudWatch Logs. Analizzando i log, è possibile determinare se il problema riguarda l'autorizzazione o, ad esempio, una condizione della clausola WHERE non corrispondente. Per ulteriori informazioni, consulta la sezione relativa alla [configurazione di CloudWatchLogs](#).

Gestione degli errori (operazione in caso di errore)

Quando AWS IoT riceve un messaggio da un dispositivo, il motore di regole controlla se il messaggio corrisponde a una regola. In tal caso, l'istruzione SQL della regola viene valutata e vengono attivate le operazioni della regola, passando il risultato dell'istruzione SQL.

Se si verifica un problema quando si attiva un'operazione, il motore di regole attiva un'operazione da eseguire in caso di errore, se ne è stata specificata una per la regola. Questo può accadere quando:

- Una regola non dispone dell'autorizzazione per l'accesso a un bucket Amazon S3.
- Un errore dell'utente causa il superamento del throughput di DynamoDB di cui è stato effettuato il provisioning.

Formato del messaggio dell'operazione da eseguire in caso di errore

Viene generato un singolo messaggio per ogni regola e messaggio. Se, ad esempio, si verifica un errore per due operazioni nella stessa regola, l'operazione da eseguire in caso di errore riceve un messaggio contenente entrambi gli errori.

Il messaggio dell'operazione da eseguire in caso di errore è simile al seguente:

```
{  
  "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:  
yMah1cwPhqTH267QLPhTKeVPKJB8B05ndBHzOmWtxLTM6uAvwYYuqieAKyb6qRPTxP1tHXCoR4Y=).  
Message arrived on: error/action, Action: s3, Bucket: us-  
east-1-s3-verify-user, Key: \"aaa\". Value of x-amz-id-2:  
yMah1cwPhqTH267QLPhTKeVPKJB8B05ndBHzOmWtxLTM6uAvwYYuqieAKyb6qRPTxP1tHXCoR4Y="  
    }  
  ]  
}
```

ruleName

Nome della regola che ha attivato l'operazione da eseguire in caso di errore.

argomento

Argomento dove è stato ricevuto il messaggio originale.

cloudwatchTraceld

Identità univoca che fa riferimento ai log di errore in CloudWatch.

clientId

ID client di chi ha pubblicato il messaggio.

base64OriginalPayload

Payload del messaggio originale con codifica Base64.

failures

failedAction

Nome dell'operazione che non è stato possibile completare, ad esempio "S3Action".

failedResource

Nome della risorsa, ad esempio il nome di un bucket S3.

errorMessage

Descrizione e spiegazione dell'errore.

Esempio di operazione in caso di errore

Di seguito è illustrato un esempio di una regola a cui è stata aggiunta un'operazione da eseguire in caso di errore. La regola seguente include un'operazione di scrittura dei dati dei messaggi in una tabella DynamoDB e un'operazione da eseguire in caso di errore di scrittura dei dati in un bucket Amazon S3:

```
{  
    "sql" : "SELECT * FROM ..."  
    "actions" : [  
        "dynamoDB" : {  
            "table" : "PoorlyConfiguredTable",  
            "hashKeyField" : "AConstantString",  
            "hashKeyValue" : "AHashKey"}  
    ],  
    "errorAction" : {  
        "s3" : {  
            "roleArn": "arn:aws:iam::123456789012:role/aws_iot_s3",  
            "bucket" : "message-processing-errors",  
            "key" : "${replace(topic(), '/', '-') + '-' + timestamp() + '-' + newuuid()}"  
        }  
    }  
}
```

È possibile usare qualsiasi funzione o sostituzione in un'istruzione SQL per l'operazione da eseguire in caso di errore, ad eccezione delle funzioni esterne (ad esempio `get_thing_shadow`, `aws_lambda` e `machinelearning_predict`).

Per ulteriori informazioni sulle regole e su come specificare un'operazione da eseguire in caso di errore, consulta la pagina relativa alla [creazione di una regola AWS IoT](#).

Per ulteriori informazioni sull'uso di CloudWatch per monitorare l'esito delle regole, consulta [Parametri e dimensioni di AWS IoT \(p. 646\)](#).

Documentazione di riferimento su SQL per AWS IoT

In AWS IoT le regole vengono definite usando una sintassi di tipo SQL. Le istruzioni SQL sono costituite da tre tipi di clausole:

SELECT

Campo obbligatorio. Estraie le informazioni dal payload del messaggio in ingresso ed esegue le trasformazioni.

FROM

Il filtro dell'argomento del messaggio MQTT. La regola viene attivata per ogni messaggio inviato a un argomento MQTT che corrisponde al filtro specificato qui. Obbligatorio per le regole che vengono attivate da messaggi che attraversano il broker di messaggi. Facoltativo per le regole che vengono attivate solo utilizzando la caratteristica [Basic Ingest \(p. 333\)](#).

WHERE

Opzionale. Aggiunge una logica condizionale che determina se le operazioni specificate da una regola vengono eseguite.

Un'istruzione SQL di esempio è simile a quanto segue:

```
SELECT color AS rgb FROM 'a/b' WHERE temperature > 50
```

Un messaggio MQTT di esempio (detto anche payload in ingresso) è simile a quanto segue:

```
{  
    "color": "red",  
    "temperature": 100  
}
```

Se questo messaggio viene pubblicato nell'argomento 'a/b', la regola viene attivata e l'istruzione SQL viene valutata. L'istruzione SQL estrae il valore della proprietà `color` se la proprietà "temperature" è superiore a 50. La clausola WHERE specifica la condizione `temperature > 50`. La parola chiave AS rinomina la proprietà "color" in "rgb". Il risultato (detto anche payload in uscita) è simile al seguente:

```
{  
    "rgb": "red"  
}
```

Questi dati vengono quindi inoltrati all'operazione della regola, che invia i dati per l'ulteriore elaborazione. Per ulteriori informazioni sulle operazioni delle regole, consulta [Operazioni delle regole AWS IoT \(p. 261\)](#).

Tipi di dati

Il motore di regole AWS IoT supporta tutti i tipi di dati JSON.

Tipi di dati supportati

| Tipo | Significato |
|----------------------|--|
| <code>Int</code> | Tipo <code>Int</code> discreto. Composto al massimo da 34 cifre. |
| <code>Decimal</code> | Tipo <code>Decimal</code> con una precisione di 34 cifre, con grandezza minima diversa da zero corrispondente a 1E-999 e grandezza massima di 9.999...E999. Note Alcune funzioni restituiscono tipi <code>Decimal</code> a precisione doppia invece che con 34 cifre di precisione. |
| <code>Boolean</code> | <code>True</code> oppure <code>False</code> . |
| <code>String</code> | Stringa UTF-8. |
| <code>Array</code> | Serie di valori non necessariamente dello stesso tipo. |
| <code>Object</code> | Valore JSON costituito da una chiave e un valore. Le chiavi devono essere stringhe. I valori possono essere di qualsiasi tipo. |
| <code>Null</code> | <code>Null</code> come definito da JSON. Si tratta di un valore effettivo che rappresenta l'assenza di un valore. È possibile creare in modo esplicito un valore <code>Null</code> usando la parola chiave <code>Null</code> nell'istruzione SQL. |

| Tipo | Significato |
|------------------------|---|
| | <p>Ad esempio: "SELECT NULL AS n FROM 'a/b'"</p> |
| <code>Undefined</code> | <p>Non un valore. Non si tratta di un tipo rappresentabile in modo esplicito in JSON, se non omettendo il valore. Ad esempio, nell'oggetto <code>{"foo": null}</code> la chiave "foo" restituisce <code>NULL</code>, ma la chiave "bar" restituisce <code>Undefined</code>. Internamente, il linguaggio SQL tratta <code>Undefined</code> come un valore, ma questo tipo non è rappresentabile in JSON, quindi quando viene serializzato in JSON i risultati sono <code>Undefined</code>.</p> <pre>{"foo":null, "bar":undefined}</pre> <p>viene serializzato in JSON come:</p> <pre>{"foo":null}</pre> <p>Analogamente, <code>Undefined</code> viene convertito in una stringa vuota quando serializzato. Le funzioni chiamate con argomenti non validi (ad esempio tipi errati, numero errato di argomenti e così via) restituiscono <code>Undefined</code>.</p> |

Conversioni

La tabella seguente elenca i risultati quando un valore di un tipo viene convertito in un altro tipo (quando un valore del tipo non corretto viene fornito a una funzione). Se, ad esempio, alla funzione di valore assoluto "abs" (che richiede un tipo `Int` o `Decimal`) viene passato un tipo `String`, viene eseguito un tentativo di convertire `String` in `Decimal`, seguendo queste regole. In questo caso, `'abs("-5.123")'` viene trattato come `'abs(-5.123)'`.

Note

Non vengono eseguiti tentativi di conversione in un tipo `ArrayObject`, `Null` o `Undefined`.

Nel tipo `Decimal`

| Tipo di argomento | Risultato |
|----------------------|---|
| <code>Int</code> | Tipo <code>Decimal</code> senza separatore decimale. |
| <code>Decimal</code> | Valore di origine. |
| <code>Boolean</code> | <code>Undefined</code> . È possibile usare in modo esplicito la funzione cast per trasformare <code>true = 1.0</code> , <code>false = 0.0</code> . |
| <code>String</code> | Il motore SQL cerca di analizzare la stringa come <code>Decimal</code> . AWS IoT tenta di analizzare le stringhe che corrispondono all'espressione regolare: <code>^-?\d+(\.\d+)?((?i)E-?\d+)?\$. "0", "-1.2", "5E-12"</code> sono tutti esempi di stringhe che vengono convertite automaticamente in tipi <code>Decimal</code> . |

| Tipo di argomento | Risultato |
|------------------------|-------------------------|
| Array | <code>Undefined.</code> |
| Oggetto | <code>Undefined.</code> |
| Null | <code>Null.</code> |
| <code>Undefined</code> | <code>Undefined.</code> |

Nel tipo Int

| Tipo di argomento | Risultato |
|------------------------|--|
| <code>Int</code> | Valore di origine. |
| <code>Decimal</code> | Valore di origine arrotondato al valore <code>Int</code> più vicino. |
| <code>Boolean</code> | <code>Undefined.</code> È possibile usare in modo esplicito la funzione <code>cast</code> per trasformare <code>true = 1.0</code> , <code>false = 0.0</code> . |
| <code>String</code> | Il motore SQL cerca di analizzare la stringa come <code>Decimal</code> . AWS IoT tenta di analizzare le stringhe che corrispondono all'espressione regolare: <code>^-?\d+(\.\d+)?((?i)E-?\d+)?\$. "0", "-1.2", "5E-12"</code> sono tutti esempi di stringhe che verrebbero convertite automaticamente in tipi <code>Decimal</code> . AWS IoT esegue un tentativo di convertire il tipo <code>String</code> in <code>Decimal</code> e quindi tronca le posizioni decimali di <code>Decimal</code> per creare un tipo <code>Int</code> . |
| Array | <code>Undefined.</code> |
| Oggetto | <code>Undefined.</code> |
| Null | <code>Null.</code> |
| <code>Undefined</code> | <code>Undefined.</code> |

Nel tipo Boolean

| Tipo di argomento | Risultato |
|----------------------|---|
| <code>Int</code> | <code>Undefined.</code> È possibile usare in modo esplicito la funzione <code>cast</code> per trasformare <code>0 = False</code> , <code>qualsiasi_valore_diverso_da_zero = True</code> . |
| <code>Decimal</code> | <code>Undefined.</code> È possibile usare in modo esplicito la funzione <code>cast</code> per trasformare <code>0 = False</code> , <code>qualsiasi_valore_diverso_da_zero = True</code> . |
| <code>Boolean</code> | Valore originale. |
| <code>String</code> | "true"= <code>True</code> e "false"= <code>False</code> (senza distinzione tra maiuscole e minuscole). Altri valori stringa sono <code>Undefined</code> . |

| Tipo di argomento | Risultato |
|------------------------|-------------------------|
| Array | <code>Undefined.</code> |
| Oggetto | <code>Undefined.</code> |
| Null | <code>Undefined.</code> |
| <code>Undefined</code> | <code>Undefined.</code> |

Nel tipo String

| Tipo di argomento | Risultato |
|------------------------|--|
| <code>Int</code> | Rappresentazione di stringa del tipo <code>Int</code> in notazione standard. |
| <code>Decimal</code> | Stringa che rappresenta il valore <code>Decimal</code> , possibilmente in notazione scientifica. |
| <code>Boolean</code> | "true" o "false". Tutto in caratteri minuscoli. |
| <code>String</code> | Valore originale. |
| <code>Array</code> | Tipo <code>Array</code> serializzato in JSON. La stringa risultante è un elenco separato da virgolette, racchiuso tra parentesi quadre. I tipi <code>String</code> sono racchiusi tra virgolette. I tipi <code>Decimal</code> , <code>Int</code> , <code>Boolean</code> e <code>Null</code> non sono racchiusi tra virgolette. |
| Oggetto | Oggetto serializzato in JSON. La stringa risultante è un elenco separato da virgolette di coppie chiave-valore e inizia e termina con parentesi graffe. I tipi <code>String</code> sono racchiusi tra virgolette. I tipi <code>Decimal</code> , <code>Int</code> , <code>Boolean</code> e <code>Null</code> non sono racchiusi tra virgolette. |
| <code>Null</code> | <code>Undefined.</code> |
| <code>Undefined</code> | <code>Undefined.</code> |

Operatori

Gli operatori seguenti possono essere usati nelle clausole SELECT e WHERE.

Operatore AND

Restituisce un risultato Boolean. Esegue un'operazione AND logica. Restituisce true se gli operandi sinistro e destro sono true. In caso contrario, restituisce false. Sono necessari operandi di tipo Boolean o operandi di tipo String "true" o "false" che non facciano distinzione tra maiuscole e minuscole.

Sintassi: `expression AND expression`.

Operatore AND

| Operando sinistro | Operando destro | Output |
|-------------------|-----------------|--|
| Boolean | Boolean | Boolean. True se entrambi gli operandi sono true. In caso contrario, false. |
| String/Boolean | String/Boolean | Se tutte le stringhe sono "true" o "false" (senza distinzione tra maiuscole e minuscole), vengono convertite in Boolean ed elaborate normalmente come tipi <code>boolean</code> AND <code>boolean</code> . |
| Altro valore | Altro valore | Undefined. |

Operatore OR

Restituisce un risultato Boolean. Esegue un'operazione OR logica. Restituisce true se l'operando sinistro o quello destro è true. In caso contrario, restituisce false. Sono necessari operandi di tipo Boolean o operandi di tipo String "true" o "false" che non facciano distinzione tra maiuscole e minuscole.

Sintassi: `expression` OR `expression`.

Operatore OR

| Operando sinistro | Operando destro | Output |
|-------------------|-----------------|--|
| Boolean | Boolean | Boolean. True se uno degli operandi è true. In caso contrario, false. |
| String/Boolean | String/Boolean | Se tutte le stringhe sono "true" o "false" (senza distinzione tra maiuscole e minuscole), vengono convertite in tipi Boolean ed elaborate normalmente come tipi <code>boolean</code> OR <code>boolean</code> . |
| Altro valore | Altro valore | Undefined. |

Operatore NOT

Restituisce un risultato Boolean. Esegue un'operazione NOT logica. Restituisce true se l'operando è false. In caso contrario, restituisce true. È necessario un operando di tipo Boolean o un operando di tipo String "true" o "false" senza distinzione tra maiuscole e minuscole.

Sintassi: NOT `expression`.

Operatore NOT

| Operando | Output |
|--------------|--|
| Boolean | Boolean. True se l'operando è false. In caso contrario, true. |
| String | Se stringa è "true" o "false" (senza distinzione tra maiuscole e minuscole), viene convertita nel valore booleano corrispondente e viene restituito il valore opposto. |
| Altro valore | Undefined. |

Operatore >

Restituisce un risultato Boolean. Restituisce true se l'operando sinistro è maggiore dell'operando destro. Entrambi gli operandi vengono convertiti in un tipo Decimal e quindi confrontati.

Sintassi: *expression* > *expression*.

Operatore >

| Operando sinistro | Operando destro | Output |
|------------------------|------------------------|--|
| Int/Decimal | Int/Decimal | Boolean. True se l'operando sinistro è maggiore dell'operando destro. In caso contrario, false. |
| String/Int/ Decimal | String/Int/ Decimal | Se tutte le stringhe possono essere convertite in Decimal, restituisce un valore Boolean. Restituisce true se l'operando sinistro è maggiore dell'operando destro. In caso contrario, false. |
| Altro valore | Undefined. | Undefined. |

Operatore >=

Restituisce un risultato Boolean. Restituisce true se l'operando sinistro è maggiore o uguale all'operando destro. Entrambi gli operandi vengono convertiti in un tipo Decimal e quindi confrontati.

Sintassi: *expression* >= *expression*.

Operatore >=

| Operando sinistro | Operando destro | Output |
|------------------------|------------------------|--|
| Int/Decimal | Int/Decimal | Boolean. True se l'operando sinistro è maggiore o uguale all'operando destro. In caso contrario, false. |
| String/Int/ Decimal | String/Int/ Decimal | Se tutte le stringhe possono essere convertite in Decimal, restituisce un valore Boolean. Restituisce true se l'operando sinistro è maggiore o uguale all'operando destro. In caso contrario, false. |
| Altro valore | Undefined. | Undefined. |

Operatore <

Restituisce un risultato Boolean. Restituisce true se l'operando sinistro è minore dell'operando destro. Entrambi gli operandi vengono convertiti in un tipo Decimal e quindi confrontati.

Sintassi: *expression* < *expression*.

Operatore <

| Operando sinistro | Operando destro | Output |
|-------------------|-----------------|---|
| Int/Decimal | Int/Decimal | Boolean. True se l'operando sinistro è minore dell'operando destro. In caso contrario, false. |

| Operando sinistro | Operando destro | Output |
|------------------------|------------------------|--|
| String/Int/ Decimal | String/Int/ Decimal | Se tutte le stringhe possono essere convertite in Decimal, restituisce un valore Boolean. Restituisce true se l'operando sinistro è minore dell'operando destro. In caso contrario, false. |
| Altro valore | Undefined | Undefined |

Operatore <=

Restituisce un risultato Boolean. Restituisce true se l'operando sinistro è minore o uguale all'operando destro. Entrambi gli operandi vengono convertiti in un tipo Decimal e quindi confrontati.

Sintassi: *expression* <= *expression*.

Operatore >=

| Operando sinistro | Operando destro | Output |
|------------------------|------------------------|--|
| Int/Decimal | Int/Decimal | Boolean. True se l'operando sinistro è minore o uguale all'operando destro. In caso contrario, false. |
| String/Int/ Decimal | String/Int/ Decimal | Se tutte le stringhe possono essere convertite in Decimal, restituisce un valore Boolean. Restituisce true se l'operando sinistro è minore o uguale all'operando destro. In caso contrario, false. |
| Altro valore | Undefined | Undefined |

Operatore <>

Restituisce un risultato Boolean. Restituisce true se gli operandi sinistro e destro non sono uguali. In caso contrario, restituisce false.

Sintassi: *expression* <> *expression*.

Operatore <>

| Operando sinistro | Operando destro | Output |
|-------------------|-----------------|--|
| Int | Int | True se l'operando sinistro non è uguale all'operando destro. In caso contrario, false. |
| Decimal | Decimal | True se l'operando sinistro non è uguale all'operando destro. In caso contrario, false. Int viene convertito in Decimal prima di essere confrontato. |
| String | String | True se l'operando sinistro non è uguale all'operando destro. In caso contrario, false. |
| Array | Array | True se gli elementi di ogni operando non sono uguali e non sono nello stesso ordine. In caso contrario, false |
| Oggetto | Oggetto | True se le chiavi e i valori di ogni operando non sono uguali. In caso contrario, false. L'ordine delle chiavi e dei valori non è importante. |

| Operando sinistro | Operando destro | Output |
|-------------------------|-------------------------|------------|
| Null | Null | False. |
| qualsiasi valore | Undefined | Undefined. |
| Undefined | qualsiasi valore | Undefined. |
| Tipo non corrispondente | Tipo non corrispondente | True. |

Operatore =

Restituisce un risultato Boolean. Restituisce true se gli operandi sinistro e destro sono uguali. In caso contrario, restituisce false.

Sintassi: *expression* = *expression*.

Operatore =

| Operando sinistro | Operando destro | Output |
|-------------------------|-------------------------|--|
| Int | Int | True se l'operando sinistro è uguale all'operando destro. In caso contrario, false. |
| Decimal | Decimal | True se l'operando sinistro è uguale all'operando destro. In caso contrario, false. Int viene convertito in Decimal prima di essere confrontato. |
| String | String | True se l'operando sinistro è uguale all'operando destro. In caso contrario, false. |
| Array | Array | True se gli elementi di ogni operando sono uguali e sono nello stesso ordine. In caso contrario, false. |
| Oggetto | Oggetto | True se le chiavi e i valori di ogni operando sono uguali. In caso contrario, false. L'ordine delle chiavi e dei valori non è importante. |
| qualsiasi valore | Undefined | Undefined. |
| Undefined | qualsiasi valore | Undefined. |
| Tipo non corrispondente | Tipo non corrispondente | False. |

Operatore +

L'operatore "+" è un operatore di overload. Può essere usato per la concatenazione di stringhe o la somma.

Sintassi: *expression* + *expression*.

Operatore +

| Operando sinistro | Operando destro | Output |
|-------------------|------------------|--|
| String | qualsiasi valore | Converte l'operando destro in una stringa e lo concatena alla fine dell'operando sinistro. |

| Operando sinistro | Operando destro | Output |
|-------------------|-----------------|---|
| qualsiasi valore | String | Converte l'operando sinistro in una stringa e lo concatena all'operando destro alla fine dell'operando sinistro convertito. |
| Int | Int | Int value. Somma gli operandi. |
| Int/Decimal | Int/Decimal | Decimal value. Somma gli operandi. |
| Altro valore | Altro valore | Undefined. |

Operatore -

Sottrae l'operando destro dall'operando sinistro.

Sintassi: *expression* - *expression*.

Operatore -

| Operando sinistro | Operando destro | Output |
|------------------------|------------------------|--|
| Int | Int | Int value. Sottrae l'operando destro dall'operando sinistro. |
| Int/Decimal | Int/Decimal | Decimal value. Sottrae l'operando destro dall'operando sinistro. |
| String/Int/ Decimal | String/Int/ Decimal | Se tutte le stringhe possono essere convertite in valori decimali, viene restituito un valore Decimal. Sottrae l'operando destro dall'operando sinistro. In caso contrario, restituisce Undefined. |
| Altro valore | Altro valore | Undefined. |
| Altro valore | Altro valore | Undefined. |

Operatore *

Moltiplica l'operando sinistro per l'operando destro.

Sintassi: *expression* * *expression*.

Operatore *

| Operando sinistro | Operando destro | Output |
|------------------------|------------------------|--|
| Int | Int | Int value. Moltiplica l'operando sinistro per l'operando destro. |
| Int/Decimal | Int/Decimal | Decimal value. Moltiplica l'operando sinistro per l'operando destro. |
| String/Int/ Decimal | String/Int/ Decimal | Se tutte le stringhe possono essere convertite in valori decimali, viene restituito un valore Decimal. Moltiplica l'operando sinistro per l'operando destro. In caso contrario, restituisce Undefined. |
| Altro valore | Altro valore | Undefined. |

Operatore /

Divide l'operando sinistro per l'operando destro.

Sintassi: `expression / expression`.

Operatore /

| Operando sinistro | Operando destro | Output |
|------------------------|------------------------|--|
| Int | Int | Int value. Divide l'operando sinistro per l'operando destro. |
| Int/Decimal | Int/Decimal | Decimal value. Divide l'operando sinistro per l'operando destro. |
| String/Int/ Decimal | String/Int/ Decimal | Se tutte le stringhe possono essere convertite in valori decimali, viene restituito un valore Decimal. Divide l'operando sinistro per l'operando destro. In caso contrario, restituisce Undefined. |
| Altro valore | Altro valore | Undefined. |

Operatore %

Restituisce il resto della divisione dell'operando sinistro per l'operando destro.

Sintassi: `expression % expression`.

Operatore %

| Operando sinistro | Operando destro | Output |
|------------------------|------------------------|---|
| Int | Int | Int value. Restituisce il resto della divisione dell'operando sinistro per l'operando destro. |
| String/Int/ Decimal | String/Int/ Decimal | Se tutte le stringhe possono essere convertite in valori decimali, viene restituito un valore Decimal. Restituisce il resto della divisione dell'operando sinistro per l'operando destro. In caso contrario, Undefined. |
| Altro valore | Altro valore | Undefined. |

Funzioni

È possibile usare le seguenti funzioni predefinite nelle clausole SELECT o WHERE delle espressioni SQL.

abs(Decimal)

Restituisce il valore assoluto di un numero. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `abs(-5)` restituisce 5.

| Tipo di argomento | Risultato |
|-------------------|---|
| Int | Int, il valore assoluto dell'argomento. |

| Tipo di argomento | Risultato |
|-------------------|---|
| Decimal | Decimal, il valore assoluto dell'argomento. |
| Boolean | Undefined. |
| String | Decimal. Il risultato è il valore assoluto dell'argomento. Se la stringa non può essere convertita, il risultato è Undefined. |
| Array | Undefined. |
| Oggetto | Undefined. |
| Null | Undefined. |
| Undefined | Undefined. |

accountid()

Restituisce l'ID dell'account proprietario della regola come `String`. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:

```
accountid() = "123456789012"
```

acos(Decimal)

Restituisce il coseno inverso di un numero in radianti. Gli argomenti `Decimal` vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `acos(0) = 1.5707963267948966`

| Tipo di argomento | Risultato |
|-------------------|---|
| Int | Decimal (a precisione doppia), il coseno inverso dell'argomento. I risultati immaginari vengono restituiti come <code>Undefined</code> . |
| Decimal | Decimal (a precisione doppia), il coseno inverso dell'argomento. I risultati immaginari vengono restituiti come <code>Undefined</code> . |
| Boolean | Undefined. |
| String | Decimal, il coseno inverso dell'argomento. Se la stringa non può essere convertita, il risultato è <code>Undefined</code> . I risultati immaginari vengono restituiti come <code>Undefined</code> . |
| Array | Undefined. |
| Oggetto | Undefined. |
| Null | Undefined. |
| Undefined | Undefined. |

asin(Decimal)

Restituisce il seno inverso di un numero in radianti. Gli argomenti `Decimal` vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `asin(0) = 0.0`

| Tipo di argomento | Risultato |
|------------------------|--|
| <code>Int</code> | <code>Decimal</code> (a precisione doppia), il seno inverso dell'argomento. I risultati immaginari vengono restituiti come <code>Undefined</code> . |
| <code>Decimal</code> | <code>Decimal</code> (a precisione doppia), il seno inverso dell'argomento. I risultati immaginari vengono restituiti come <code>Undefined</code> . |
| <code>Boolean</code> | <code>Undefined</code> . |
| <code>String</code> | <code>Decimal</code> (a precisione doppia), il seno inverso dell'argomento. Se la stringa non può essere convertita, il risultato è <code>Undefined</code> . I risultati immaginari vengono restituiti come <code>Undefined</code> . |
| <code>Array</code> | <code>Undefined</code> . |
| Oggetto | <code>Undefined</code> . |
| <code>Null</code> | <code>Undefined</code> . |
| <code>Undefined</code> | <code>Undefined</code> . |

atan(Decimal)

Restituisce la tangente inversa di un numero in radianti. Gli argomenti `Decimal` vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `atan(0) = 0.0`

| Tipo di argomento | Risultato |
|----------------------|---|
| <code>Int</code> | <code>Decimal</code> (a precisione doppia), la tangente inversa dell'argomento. I risultati immaginari vengono restituiti come <code>Undefined</code> . |
| <code>Decimal</code> | <code>Decimal</code> (a precisione doppia), la tangente inversa dell'argomento. I risultati immaginari vengono restituiti come <code>Undefined</code> . |
| <code>Boolean</code> | <code>Undefined</code> . |
| <code>String</code> | <code>Decimal</code> , la tangente inversa dell'argomento. Se la stringa non può essere convertita, il risultato è <code>Undefined</code> . I risultati immaginari vengono restituiti come <code>Undefined</code> . |

| Tipo di argomento | Risultato |
|-------------------|------------|
| Array | Undefined. |
| Oggetto | Undefined. |
| Null | Undefined. |
| Undefined | Undefined. |

atan2(Decimal, Decimal)

Restituisce l'angolo in radianti, tra l'asse X positivo e il punto (x, y) definito nei due argomenti. L'angolo è positivo per gli angoli in senso antiorario (semipiano superiore, $y > 0$) e negativo per gli angoli in senso orario (semipiano inferiore, $y < 0$). Gli argomenti Decimal vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `atan2(1, 0) = 1.5707963267948966`

| Tipo di argomento | Tipo di argomento | Risultato |
|--------------------|--------------------|--|
| Int/Decimal | Int/Decimal | Decimal (a precisione doppia) del punto (x, y) specificato. |
| Int/Decimal/String | Int/Decimal/String | Decimal, la tangente del punto (x, y). Una stringa non può essere convertita in Decimal. |
| Altro valore | Altro valore | Undefined. |

aws_lambda(functionArn, inputJson)

Chiama la funzione Lambda specificata passando `inputJson` alla funzione Lambda e restituisce il codice JSON generato dalla funzione Lambda.

Argomenti

| Argomento | Descrizione |
|--------------------------|--|
| <code>functionArn</code> | ARN della funzione Lambda da chiamare. La funzione Lambda deve restituire dati JSON. |
| <code>inputJson</code> | Input JSON passato alla funzione Lambda. |

È necessario concedere ad AWS IoT le autorizzazioni `lambda:InvokeFunction` per richiamare la funzione Lambda specificata. L'esempio seguente illustra come concedere l'autorizzazione `lambda:InvokeFunction` usando l'interfaccia a riga di comando di AWS:

```
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"
```

Di seguito sono illustrati gli argomenti per il comando add-permission:

--function-name

Nome della funzione Lambda di cui viene aggiornata la policy per le risorse aggiungendo una nuova autorizzazione.

--region

Regione AWS dell'account.

--principal

Entità principale che riceve l'autorizzazione. Deve trattarsi di `iot.amazonaws.com` per concedere ad AWS IoT l'autorizzazione per chiamare una funzione Lambda.

--source-arn

ARN della regola. Usa il comando `get-topic-rule` dell'interfaccia a riga di comando per ottenere l'ARN di una regola.

--source-account

Account AWS in cui la regola è definita.

--statement-id

Identificatore univoco di un'istruzione.

--action

Operazione Lambda da consentire nell'istruzione. Per consentire a AWS IoT di invocare una funzione Lambda, specificare `lambda:InvokeFunction`.

Note

Se si aggiunge un'autorizzazione per un'entità principale AWS IoT senza fornire l'ARN di origine, qualsiasi account AWS che crea una regola con l'operazione Lambda può attivare regole per invocare la funzione Lambda da AWS IoT. Per ulteriori informazioni, consulta la pagina relativa al [modello di autorizzazioni Lambda](#).

Dato un payload di messaggio JSON, ad esempio:

```
{  
    "attribute1": 21,  
    "attribute2": "value"  
}
```

È possibile utilizzare la funzione `aws_lambda` per chiamare la funzione Lambda come segue:

```
SELECT  
aws_lambda("arn:aws:lambda:us-east-1:account_id:function:lambda_function",  
{"payload":attribute1} as output FROM 'a/b'
```

Se si desidera passare il payload di messaggio MQTT completo, è possibile specificare il payload JSON utilizzando `**`. Ad esempio:

```
SELECT
```

```
aws_lambda("arn:aws:lambda:us-east-1:account_id:function:lambda_function", *) as output
FROM 'a/b'
```

`payload.inner.element` seleziona i dati dal messaggio pubblicato nell'argomento 'a/b'.

`some.value` seleziona i dati dall'output generato dalla funzione Lambda.

Note

Il motore di regole limita la durata dell'esecuzione delle funzioni Lambda. Le chiamate alle funzioni Lambda dalle regole devono essere completate entro 2000 millisecondi.

bitand(Int, Int)

Esegue un'operazione AND bit per bit sulle rappresentazioni in bit dei due argomenti `Int` (convertiti). Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `bitand(13, 5) = 5`

| Tipo di argomento | Tipo di argomento | Risultato |
|---------------------------------|---------------------------------|--|
| <code>Int</code> | <code>Int</code> | <code>Int</code> , un'operazione AND bit per bit. |
| <code>Int/Decimal</code> | <code>Int/Decimal</code> | <code>Int</code> , un'operazione AND bit per bit. I numeri non di tipo <code>Int</code> vengono convertiti in <code>Int</code> al valore <code>Int</code> più vicino. Se non è possibile convertire il numero, il risultato è <code>Undefined</code> . |
| <code>Int/Decimal/String</code> | <code>Int/Decimal/String</code> | <code>Int</code> , un'operazione AND bit per bit. Tutte le stringhe vengono convertite in <code>Int</code> . Se non è possibile convertire la stringa, il risultato è <code>Undefined</code> . |
| Altro valore | Altro valore | <code>Undefined</code> . |

bitor(Int, Int)

Esegue un'operazione OR bit per bit sulle rappresentazioni in bit dei due argomenti. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `bitor(8, 5) = 13`

| Tipo di argomento | Tipo di argomento | Risultato |
|---------------------------------|---------------------------------|--|
| <code>Int</code> | <code>Int</code> | <code>Int</code> , l'operazione OR bit per bit. |
| <code>Int/Decimal</code> | <code>Int/Decimal</code> | <code>Int</code> , l'operazione OR bit per bit. I numeri non di tipo <code>Int</code> vengono convertiti in <code>Int</code> al valore <code>Int</code> più vicino. Se non è possibile convertire il numero, il risultato è <code>Undefined</code> . |
| <code>Int/Decimal/String</code> | <code>Int/Decimal/String</code> | <code>Int</code> , l'operazione OR bit per bit. Tutte le stringhe vengono convertite in <code>Int</code> . Se non è possibile convertire la stringa, il risultato è <code>Undefined</code> . |
| Altro valore | Altro valore | <code>Undefined</code> . |

bitxor(Int, Int)

Esegue un'operazione XOR bit per bit sulle rappresentazioni in bit dei due argomenti `Int` (convertiti). Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:`bitor(13, 5) = 8`

| Tipo di argomento | Tipo di argomento | Risultato |
|---------------------------------|---------------------------------|---|
| <code>Int</code> | <code>Int</code> | <code>Int</code> , un'operazione XOR |
| <code>Int/Decimal</code> | <code>Int/Decimal</code> | <code>Int</code> , un'operazione XOR sui numeri non di tipo <code>Int</code> . Il valore <code>Int</code> più vicino. |
| <code>Int/Decimal/String</code> | <code>Int/Decimal/String</code> | <code>Int</code> , un'operazione XOR. Le stringhe vengono convertite in decimali e arrotondate per difetto al valore <code>Int</code> più vicino. Se la conversione non riesce, il risultato è <code>Undefined</code> . |
| Altro valore | Altro valore | <code>Undefined</code> . |

bitnot(Int)

Esegue un'operazione NOT bit per bit sulle rappresentazioni in bit dell'argomento `Int` (convertito). Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:`bitnot(13) = 2`

| Tipo di argomento | Risultato |
|----------------------|--|
| <code>Int</code> | <code>Int</code> , un'operazione NOT bit per bit sull'argomento. |
| <code>Decimal</code> | <code>Int</code> , un'operazione NOT bit per bit sull'argomento. Il valore <code>Decimal</code> viene arrotondato per difetto al valore <code>Int</code> più vicino. |
| <code>String</code> | <code>Int</code> , un'operazione NOT bit per bit sull'argomento. Le stringhe vengono convertite in decimali e arrotondate per difetto al valore <code>Int</code> più vicino. Se la conversione non riesce, il risultato è <code>Undefined</code> . |
| Altro valore | Altro valore. |

cast()

Converte un valore da un tipo di dati a un altro. Le operazioni di cast hanno un comportamento per lo più simile alle conversioni standard, con in più la possibilità di eseguire il cast dei numeri da e verso tipi booleani. Se AWS IoT non è in grado di determinare come eseguire il cast di un tipo in un altro, il risultato è `Undefined`. Supportata da SQL versione 2015-10-8 e versioni successive. Formato: `cast(valore as tipo)`.

Esempio:

`cast(true as Decimal) = 1.0`

Di seguito sono indicate le parole chiave che potrebbero seguire la parola "as" quando si chiama cast:

Per la versione SQL 2015-10-8 e 2016-03-23

| Parola chiave | Risultato |
|---------------|---|
| Decimal | Esegue il cast del valore nel tipo Decimal. |
| Bool | Esegue il cast del valore nel tipo Boolean. |
| Boolean | Esegue il cast del valore nel tipo Boolean. |
| String | Esegue il cast del valore nel tipo String. |
| Nvarchar | Esegue il cast del valore nel tipo String. |
| Text | Esegue il cast del valore nel tipo String. |
| Ntext | Esegue il cast del valore nel tipo String. |
| varchar | Esegue il cast del valore nel tipo String. |
| Int | Esegue il cast del valore nel tipo Int. |
| Numero intero | Esegue il cast del valore nel tipo Int. |

Inoltre, per la versione SQL 2016-03-23

| Parola chiave | Risultato |
|---------------|---|
| Decimal | Esegue il cast del valore nel tipo Decimal. |
| Bool | Esegue il cast del valore nel tipo Boolean. |
| Boolean | Esegue il cast del valore nel tipo Boolean. |

Regole per il cast:

Cast nel tipo Decimal

| Tipo di argomento | Risultato |
|-------------------|--|
| Int | Tipo Decimal senza separatore decimale. |
| Decimal | Valore di origine. |
| Boolean | true = 1.0, false = 0.0. |
| String | Cerca di analizzare la stringa come Decimal. AWS IoT tenta di analizzare le stringhe che corrispondono all'espressione regolare: ^-?[d+](\.\d+)?((?i)E-?[d+])?\$. "0", "-1.2", "5E-12" sono tutti esempi di stringhe che vengono convertite automaticamente in decimali. |
| Array | Undefined. |
| Oggetto | Undefined. |
| Null | Undefined. |

| Tipo di argomento | Risultato |
|-------------------|------------|
| Undefined | Undefined. |

Cast nel tipo Int

| Tipo di argomento | Risultato |
|-------------------|--|
| Int | Valore di origine. |
| Decimal | Valore di origine, arrotondato per difetto al valore Int più vicino. |
| Boolean | true = 1.0, false = 0.0. |
| String | Cerca di analizzare la stringa come Decimal. AWS IoT tenta di analizzare le stringhe che corrispondono all'espressione regolare: ^-?d+(\.\d+)?((?i)E-?d+)?\$. "0", "-1.2", "5E-12" sono tutti esempi di stringhe che vengono convertite automaticamente in decimali. AWS IoT prova a convertire la stringa in un tipo Decimal e ad arrotondarla per difetto al valore Int più vicino. |
| Array | Undefined. |
| Oggetto | Undefined. |
| Null | Undefined. |
| Undefined | Undefined. |

Cast nel tipo Boolean

| Tipo di argomento | Risultato |
|-------------------|--|
| Int | 0 = False, qualsiasi_valore_diverso_da_zero = True. |
| Decimal | 0 = False, qualsiasi_valore_diverso_da_zero = True. |
| Boolean | Valore di origine. |
| String | "true" = True e "false" = False (senza distinzione tra maiuscole e minuscole). Altri valori stringa = Undefined. |
| Array | Undefined. |
| Oggetto | Undefined. |
| Null | Undefined. |
| Undefined | Undefined. |

Cast nel tipo String

| Tipo di argomento | Risultato |
|-------------------|--|
| Int | Rappresentazione di stringa del tipo Int, in notazione standard. |

| Tipo di argomento | Risultato |
|-------------------|---|
| Decimal | Stringa che rappresenta il valore Decimal, possibilmente in notazione scientifica. |
| Boolean | "true" o "false", tutto in caratteri minuscoli. |
| String | "true"=True e "false"=False (senza distinzione tra maiuscole e minuscole). Altri valori stringa = Undefined. |
| Array | Matrice serializzata in JSON. La stringa risultante è un elenco separato da virgolette racchiuso tra parentesi quadre. I tipi String sono racchiusi tra virgolette. I tipi Decimal, Int e Boolean non sono racchiusi tra virgolette. |
| Oggetto | Oggetto serializzato in JSON. La stringa JSON è un elenco separato da virgolette di coppie chiave-valore e inizia e termina con parentesi graffe. Il tipo String è racchiuso tra virgolette. I tipi Decimal, Int, Boolean e Null non sono racchiusi tra virgolette. |
| Null | Undefined. |
| Undefined | Undefined. |

ceil(Decimal)

Arrotonda per eccesso il tipo Decimal specificato al valore Int più vicino. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
ceil(1.2) = 2
ceil(11.2) = -1
```

| Tipo di argomento | Risultato |
|-------------------|---|
| Int | Int, il valore dell'argomento. |
| Decimal | Int, il valore Decimal arrotondato per eccesso al valore Int più vicino. |
| String | Int. La stringa viene convertita in Decimal e arrotondata per eccesso al valore Int più vicino. Se la stringa non può essere convertita in un tipo Decimal, il risultato è Undefined. |
| Altro valore | Undefined. |

chr(String)

Restituisce il carattere ASCII corrispondente all'argomento Int specificato. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
chr(65) = "A".
chr(49) = "1".
```

| Tipo di argomento | Risultato |
|-------------------|--|
| Int | Carattere corrispondente al valore ASCII specificato. Se l'argomento non è un valore ASCII valido, il risultato è <code>Undefined</code> . |
| Decimal | Carattere corrispondente al valore ASCII specificato. L'argomento <code>Decimal</code> viene arrotondato per difetto al valore <code>Int</code> più vicino. Se l'argomento non è un valore ASCII valido, il risultato è <code>Undefined</code> . |
| Boolean | <code>Undefined</code> . |
| String | Se il tipo <code>String</code> può essere convertito in <code>Decimal</code> , viene arrotondato per difetto al valore <code>Int</code> più vicino. Se l'argomento non è un valore ASCII valido, il risultato è <code>Undefined</code> . |
| Array | <code>Undefined</code> . |
| Oggetto | <code>Undefined</code> . |
| Null | <code>Undefined</code> . |
| Altro valore | <code>Undefined</code> . |

clientid()

Restituisce l'ID del client MQTT che invia il messaggio oppure `n/a` se il messaggio non è stato inviato tramite MQTT. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:

```
clientid() = "123456789012"
```

concat()

Concatena matrici o stringhe. Questa funzione accetta qualsiasi numero di argomenti e restituisce un tipo `String` o `Array`. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
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]`

| Numero di argomenti | Risultato |
|---------------------|--|
| 0 | <code>Undefined.</code> |
| 1 | L'argomento viene restituito non modificato. |
| 2+ | <p>Se un argomento è un tipo <code>Array</code>, il risultato è una singola matrice contenente tutti gli argomenti. Se nessun argomento è un array e almeno un argomento è di tipo <code>String</code>, il risultato è la concatenazione delle rappresentazioni <code>String</code> di tutti gli argomenti. Gli argomenti vengono convertiti in stringhe usando le conversioni standard illustrate in precedenza.</p> <p>.</p> |

cos(Decimal)

Restituisce il coseno di un numero in radianti. Gli argomenti `Decimal` vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:

`cos(0) = 1.`

| Tipo di argomento | Risultato |
|------------------------|---|
| <code>Int</code> | <code>Decimal</code> (a precisione doppia), il coseno dell'argomento. I risultati immaginari vengono restituiti come <code>Undefined</code> . |
| <code>Decimal</code> | <code>Decimal</code> (a precisione doppia), il coseno dell'argomento. I risultati immaginari vengono restituiti come <code>Undefined</code> . |
| <code>Boolean</code> | <code>Undefined.</code> |
| <code>String</code> | <code>Decimal</code> (a precisione doppia), il coseno dell'argomento. Se la stringa non può essere convertita in un tipo <code>Decimal</code> , il risultato è <code>Undefined</code> . I risultati immaginari vengono restituiti come <code>Undefined</code> . |
| <code>Array</code> | <code>Undefined.</code> |
| Oggetto | <code>Undefined.</code> |
| <code>Null</code> | <code>Undefined.</code> |
| <code>Undefined</code> | <code>Undefined.</code> |

cosh(Decimal)

Restituisce il coseno iperbolico di un numero in radianti. Gli argomenti `Decimal` vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: $\cosh(2.3) = 5.037220649268761$.

| Tipo di argomento | Risultato |
|-------------------|---|
| Int | Decimal (a precisione doppia), il coseno iperbolico dell'argomento. I risultati immaginari vengono restituiti come Undefined. |
| Decimal | Decimal (a precisione doppia), il coseno iperbolico dell'argomento. I risultati immaginari vengono restituiti come Undefined. |
| Boolean | Undefined. |
| String | Decimal (a precisione doppia), il coseno iperbolico dell'argomento. Se la stringa non può essere convertita in un tipo Decimal, il risultato è Undefined. I risultati immaginari vengono restituiti come Undefined. |
| Array | Undefined. |
| Oggetto | Undefined. |
| Null | Undefined. |
| Undefined | Undefined. |

encode(value, encodingScheme)

Usa la funzione `encode` per codificare il payload, che potenzialmente può essere costituito da dati non JSON, nella rappresentazione di stringa in base allo schema di codifica. Supportata da SQL versione 2016-03-23 e versioni successive.

`value`

Qualsiasi espressioni valida, in base a quanto definito in [Documentazione di riferimento su SQL per AWS IoT \(p. 279\)](#). È possibile specificare * per codificare l'intero payload, indipendentemente dal fatto che sia in formato JSON. Se si fornisce un'espressione, il risultato della valutazione verrà prima convertito in una stringa e quindi codificato.

`encodingScheme`

Stringa letterale che rappresenta lo schema di codifica da usare. Attualmente è supportato solo 'base64'.

endswith(String, String)

Restituisce un tipo Boolean che indica se il primo argomento String termina con il secondo argomento String. Se uno degli argomenti è Null oppure Undefined, il risultato è Undefined. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `endswith("cat", "at") = true.`

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|------------------|------------------|---|
| String | String | True se il primo argomento. In caso contrario, False. |

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|------------------|------------------|---|
| Altro valore | Altro valore | Entrambi gli argomenti sono di tipo <code>String</code> . Se un argomento termina con <code>NaN</code> o <code>infinity</code> , il risultato è <code>NaN</code> . Se un argomento termina con <code>false</code> , il risultato è <code>false</code> . Se un argomento termina con <code>true</code> , il risultato è <code>true</code> . Se un argomento termina con <code>undefined</code> , il risultato è <code>undefined</code> . |

exp(Decimal)

Restituisce il valore e elevato all'argomento `Decimal`. Gli argomenti `Decimal` vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `exp(1) = e.`

| Tipo di argomento | Risultato |
|----------------------|---|
| <code>Int</code> | <code>Decimal</code> (a precisione doppia), argomento <code>e ^</code> . |
| <code>Decimal</code> | <code>Decimal</code> (a precisione doppia), argomento <code>e ^</code> . |
| <code>String</code> | <code>Decimal</code> (a precisione doppia), argomento <code>e ^</code> . Se il tipo <code>String</code> non può essere convertito in <code>Decimal</code> , il risultato è <code>undefined</code> . |
| Altro valore | <code>undefined</code> . |

get

Estrae un valore da un tipo di raccolta (Array, String, Object). Al primo argomento non viene applicata alcuna conversione. La conversione viene applicata al secondo argomento come illustrato nella tabella. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
get(["a", "b", "c"], 1) = "B USD"
get({"a": "b"}, "a") = "B USD"
get("abc", 1) = "B USD"
```

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|------------------|--|---|
| Array | qualsiasi tipo (convertito in <code>Int</code>) | Elemento con indice <code>i</code> nel <code>Array</code> . Se <code>i</code> è maggiore del numero di elementi nell' <code>Array</code> o se <code>i</code> è di tipo <code>String</code> e non riesce a convertirsi in <code>Int</code> , il risultato è <code>undefined</code> . |
| Stringa | qualsiasi tipo (convertito in <code>Int</code>) | Carattere con indice <code>i</code> nella stringa. Se <code>i</code> è maggiore del numero di caratteri nella stringa o se <code>i</code> è di tipo <code>String</code> e non riesce a convertirsi in <code>Int</code> , il risultato è <code>undefined</code> . |

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|------------------|---|--|
| Oggetto | String (non viene applicata alcuna conversione) | Valore archiviato nell'corrispondente alla chiamata di funzione. |
| Altro valore | qualsiasi valore | Undefined. |

get_thing_shadow(thingName, roleARN)

Restituisce la copia shadow dell'oggetto specificato. Supportata da SQL versione 2016-03-23 e versioni successive.

thingName

String: nome della copia shadow dell'oggetto da recuperare.

roleArn

String: ARN di un ruolo con autorizzazione `iot:GetThingShadow`.

Esempio:

```
SELECT * from 'a/b'
WHERE get_thing_shadow("MyThing", "arn:aws:iam::123456789012:role/
AllowsThingShadowAccess") .state.reported.alarm = 'ON'
```

Funzioni di hashing

AWS IoT fornisce le funzioni di hashing seguenti:

- md2
- md5
- sha1
- sha224
- sha256
- sha384
- sha512

Tutte le funzioni hash richiedono un argomento stringa. Il risultato è il valore della stringa sottoposta ad hashing. Agli argomenti non di tipo String si applicano le conversioni standard nel tipo String. Tutte le funzioni hash sono supportate da SQL versione 2015-10-8 e successive.

Esempi:

`md2("hello") = "a9046c73e00331af68917d3804f70655"`

`md5("hello") = "5d41402abc4b2a76b9719d911017c592"`

indexof(String, String)

Restituisce il primo indice (base 0) del secondo argomento come sottostringa nel primo argomento. Entrambi gli argomenti devono essere stringhe. Gli argomenti non di tipo String sono soggetti alle regole

di conversione standard nel tipo String. Questa funzione non si applica alle matrici, ma solo alle stringhe. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
indexof("abcd", "bc") = 1
```

isNull()

Restituisce true se l'argomento è il valore Null. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
isNull(5) = false.
```

```
isNull(null) = true.
```

| Tipo di argomento | Risultato |
|-------------------|-----------|
| Int | false |
| Decimal | false |
| Boolean | false |
| String | false |
| Array | false |
| Object | false |
| Null | true |
| Undefined | false |

isUndefined()

Restituisce true se l'argomento è Undefined. Supportata da SQL versione 2016-03-23 e versioni successive.

Esempi:

```
isUndefined(5) = false.
```

```
isUndefined(floor([1,2,3])) = true.
```

| Tipo di argomento | Risultato |
|-------------------|-----------|
| Int | false |
| Decimal | false |
| Boolean | false |
| String | false |

| Tipo di argomento | Risultato |
|-------------------|-----------|
| Array | false |
| Object | false |
| Null | false |
| Undefined | true |

length(String)

Restituisce il numero di caratteri della stringa fornita. Agli argomenti non di tipo `String` si applicano le regole di conversione standard. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
length("hi") = 2
length(false) = 5
```

ln(Decimal)

Restituisce il logaritmo naturale dell'argomento. Gli argomenti `Decimal` vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `ln(e) = 1`.

| Tipo di argomento | Risultato |
|------------------------|---|
| <code>Int</code> | <code>Decimal</code> (a precisione doppia), il logaritmo naturale dell'argomento. |
| <code>Decimal</code> | <code>Decimal</code> (a precisione doppia), il logaritmo naturale dell'argomento. |
| <code>Boolean</code> | <code>Undefined</code> . |
| <code>String</code> | <code>Decimal</code> (a precisione doppia), il logaritmo naturale dell'argomento. Se la stringa non può essere convertita in un tipo <code>Decimal</code> , il risultato è <code>Undefined</code> . |
| <code>Array</code> | <code>Undefined</code> . |
| Oggetto | <code>Undefined</code> . |
| <code>Null</code> | <code>Undefined</code> . |
| <code>Undefined</code> | <code>Undefined</code> . |

log(Decimal)

Restituisce il logaritmo in base 10 dell'argomento. Gli argomenti `Decimal` vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `log(100) = 2.0.`

| Tipo di argomento | Risultato |
|------------------------|--|
| <code>Int</code> | <code>Decimal</code> (a precisione doppia), il logaritmo in base 10 dell'argomento. |
| <code>Decimal</code> | <code>Decimal</code> (a precisione doppia), il logaritmo in base 10 dell'argomento. |
| <code>Boolean</code> | <code>Undefined.</code> |
| <code>String</code> | <code>Decimal</code> (a precisione doppia), il logaritmo in base 10 dell'argomento. Se il tipo <code>String</code> non può essere convertito in <code>Decimal</code> , il risultato è <code>Undefined</code> . |
| <code>Array</code> | <code>Undefined.</code> |
| <code>Oggetto</code> | <code>Undefined.</code> |
| <code>Null</code> | <code>Undefined.</code> |
| <code>Undefined</code> | <code>Undefined.</code> |

lower(`String`)

Restituisce la versione con caratteri minuscoli del tipo `String` specificato. Gli argomenti non di tipo `String` vengono convertiti in stringhe usando le regole di conversione standard. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
lower("HELLO") = "hello".
lower(["HELLO"]) = ["hello"].
```

lpad(`String`, `Int`)

Restituisce l'argomento `String` con spaziatura sul lato sinistro, con il numero di spazi specificato dal secondo argomento. L'argomento `Int` deve essere compreso tra 0 e 1.000. Se il valore fornito è al di fuori di questo intervallo valido, l'argomento viene impostato sul valore valido più vicino (0 o 1000). Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
lpad("hello", 2) = " hello".
lpad(1, 3) = " 1"
```

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|---------------------|----------------------|--|
| <code>String</code> | <code>Int</code> | <code>String</code> , il tipo <code>String</code> sinistro, con un numero di spazi aggiuntivi a destra. |
| <code>String</code> | <code>Decimal</code> | L'argomento <code>Decimal</code> viene convertito in un <code>String</code> con lo stesso numero di spazi aggiuntivi a sinistra. |

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|------------------|--------------------|---|
| String | String | Il secondo argomento arrotondato per difetto. String viene aggiunto al numero di spazi specificati. Se il numero non può essere convertito in un numero intero, il risultato è Undefined. |
| Altro valore | Int/Decimal/String | Il primo valore viene convertito in un numero intero. Le conversioni standard sono applicate alla funzione Int. Se non è possibile, il risultato è Undefined. |
| qualsiasi valore | Altro valore | Undefined. |

Itrim(String)

Rimuove tutti gli spazi vuoti iniziali (tabulazioni e spazi) dal tipo String fornito. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:

```
Itrim(" h i ") = "hi".
```

| Tipo di argomento | Risultato |
|-------------------|--|
| Int | Rappresentazione String del tipo Int con tutti gli spazi vuoti iniziali rimossi. |
| Decimal | Rappresentazione String del tipo Decimal con tutti gli spazi vuoti iniziali rimossi. |
| Boolean | Rappresentazione String del tipo Boolean ("true" o "false") con tutti gli spazi vuoti iniziali rimossi. |
| String | Argomento con tutti gli spazi vuoti iniziali rimossi. |
| Array | Rappresentazione String del tipo Array (usando le regole di conversione standard) con tutti gli spazi vuoti iniziali rimossi. |
| Oggetto | Rappresentazione String del tipo Object (usando le regole di conversione standard) con tutti gli spazi vuoti iniziali rimossi. |
| Null | Undefined. |
| Undefined | Undefined. |

machinelearning_predict(modelId)

Usa la funzione machinelearning_predict per effettuare previsioni usando i dati di un messaggio MQTT in base a un modello Amazon Machine Learning (Amazon ML). Supportata da SQL versione 2015-10-8 e versioni successive. Gli argomenti per la funzione machinelearning_predict sono i seguenti:

modelId

ID del modello in base a cui effettuare la previsione. L'endpoint in tempo reale del modello deve essere abilitato.

roleArn

Ruolo IAM che dispone di una policy con autorizzazioni `machinelearning:Predict` e `machinelearning:GetMLModel` e permette l'accesso al modello in base a cui viene effettuata la previsione.

record

Dati da passare all'API di previsione di Amazon ML. Questo elemento deve essere rappresentato come oggetto JSON a singolo livello. Se il record è un oggetto JSON multilivello, viene appiattito mediante la serializzazione dei rispettivi valori. Ad esempio, l'oggetto JSON seguente:

```
{ "key1": {"innerKey1": "value1"}, "key2": 0}
```

diventerebbe:

```
{ "key1": "{\"innerKey1\": \"value1\"}", "key2": 0}
```

La funzione restituisce un oggetto JSON con i campi seguenti:

`predictedLabel`

Classificazione dell'input in base al modello.

`details`

Contiene gli attributi seguenti:

`PredictiveModelType`

Tipo di modello. I valori validi sono REGRESSION, BINARY, MULTICLASS.

`Algorithm`

Algoritmo usato da Amazon ML per effettuare le previsioni. Il valore deve essere SGD.
`predictedScores`

Contiene il punteggio di classificazione non elaborato corrispondente a ogni etichetta.

`predictedValue`

Valore previsto da Amazon ML.

mod(Decimal, Decimal)

Restituisce il resto della divisione del primo argomento per il secondo argomento. Supportata da SQL versione 2015-10-8 e versioni successive. È anche possibile usare "%" come operatore infisso per la stessa funzionalità di modulo. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `mod(8, 3) = 2`.

| Operando sinistro | Operando destro | Output |
|-------------------|------------------|---|
| <code>Int</code> | <code>Int</code> | <code>Int</code> , il resto della divisione del primo argomento per il secondo argomento. |

| Operando sinistro | Operando destro | Output |
|--------------------|--------------------|--|
| Int/Decimal | Int/Decimal | Decimal, il resto dell'ultimo operando. |
| String/Int/Decimal | String/Int/Decimal | Se tutte le stringhe sono valide, il risultato è il resto della stringa del secondo argomento. In caso contrario, viene restituito il secondo argomento. |
| Altro valore | Altro valore | Undefined. |

nanvl(AnyValue, AnyValue)

Restituisce il primo argomento, se si tratta di un tipo Decimal valido. In caso contrario, viene restituito il secondo argomento. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `Nanvl(8, 3) = 8.`

| Tipo argomento 1 | Tipo argomento 2 | Output |
|-------------------------|------------------|--------------------|
| Undefined | qualsiasi valore | Secondo argomento. |
| Null | qualsiasi valore | Secondo argomento. |
| Decimal (non un numero) | qualsiasi valore | Secondo argomento. |
| Decimal (numero) | qualsiasi valore | Primo argomento. |
| Altro valore | qualsiasi valore | Primo argomento. |

newuuid()

Restituisce un valore UUID casuale a 16 byte. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `newuuid() = 123a4567-b89c-12d3-e456-789012345000`

numbytes(String)

Restituisce il numero di byte nella codifica UTF-8 della stringa fornita. Agli argomenti non di tipo String si applicano le regole di conversione standard. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

`numbytes("hi") = 2`

`numbytes("€") = 3`

principal()

Restituisce l'impronta del certificato X.509 o il nome dell'oggetto, a seconda dell'endpoint, MQTT o HTTP, che ha ricevuto la richiesta. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:

`principal() = "ba67293af50bf2506f5f93469686da660c7c844e7b3950fb16813e0d31e9373"`

parse_time(String, Long, [String])

Usa la funzione `parse_time` per formattare un timestamp in un formato di data/ora leggibile. Supportata da SQL versione 2016-03-23 e versioni successive. Gli argomenti per la funzione `parse_time` sono i seguenti:

pattern

(String) modello di data/ora conforme al formato standard [ISO 8601](#). Nello specifico, la funzione supporta i [formati Joda-Time](#).

timestamp

(Long) Ora da formattare in millisecondi dall'epoca (Unix epoch). Consulta la funzione [timestamp\(\)](#) (p. 322).

timezone

(String) [Opzionale] Fuso orario del valore di data/ora formattato. Il valore predefinito è "UTC". La funzione supporta i [fusi orari Joda-Time](#).

Esempi:

Quando questo messaggio viene pubblicato nell'argomento "A/B", il payload `{"ts": "1970.01.01 AD at 21:46:40 CST"}` viene inviato al bucket S3:

```
{  
    "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"}  
        ]  
    }  
}
```

Quando questo messaggio viene pubblicato nell'argomento "A/B", un payload simile a `{"ts": "2017.06.09 AD at 17:19:46 UTC"}` (ma con valore di data/ora corrente) viene inviato al bucket S3:

```
{  
    "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"}  
        ]  
    }  
}
```

```

        "key": "KEY_NAME"
    }
}
],
"ruleName": "RULE_NAME"
}
}
```

È anche possibile usare `parse_time()` come modello di sostituzione. Quando, ad esempio, questo messaggio viene pubblicato nell'argomento "A/B", il payload viene inviato al bucket S3 con key = "2017":

```
{
    "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:role:ROLE_NAME",
                    "bucketName": BUCKET_NAME,
                    "key": "${parse_time(\"yyyy\", timestamp(), \"UTC\")}"
                }
            }
        ],
        "ruleName": "RULE_NAME"
    }
}
```

power(Decimal, Decimal)

Restituisce il primo argomento elevato al secondo argomento. Gli argomenti `Decimal` vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `power(2, 5) = 32.0`.

| Tipo argomento 1 | Tipo argomento 2 | Output |
|---------------------------------|---------------------------------|---|
| <code>Int/Decimal</code> | <code>Int/Decimal</code> | <code>Tipo Decimal</code> (a precisione doppia) elevato alla potenza di <code>Int/Decimal</code> . |
| <code>Int/Decimal/String</code> | <code>Int/Decimal/String</code> | <code>Tipo Decimal</code> (a precisione doppia) elevato alla potenza di <code>String</code> . I valori stringa vengono convertiti in numeri decimali prima di essere convertito in <code>Decimal</code> . |
| Altro valore | Altro valore | <code>Undefined</code> . |

rand()

Restituisce un tipo `double` pseudocasuale, distribuito uniformemente e compreso tra 0,0 e 1,0. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:

`rand() = 0.8231909191640703`

regexp_matches(String, String)

Restituisce true se la stringa (primo argomento) contiene una corrispondenza dell'espressione regolare (secondo argomento).

Esempio:

```
Regexp_matches("aaaa", "a{2,}") = true.
```

```
Regexp_matches("aaaa", "b") = false.
```

Primo argomento:

| Tipo di argomento | Risultato |
|-------------------|---|
| Int | Rappresentazione String del tipo Int. |
| Decimal | Rappresentazione String del tipo Decimal. |
| Boolean | Rappresentazione String del tipo Boolean ("true" o "false"). |
| String | Tipo String. |
| Array | Rappresentazione String del tipo Array (usando le regole di conversione standard). |
| Oggetto | Rappresentazione String del tipo Object (usando le regole di conversione standard). |
| Null | Undefined. |
| Undefined | Undefined. |

Secondo argomento:

Deve essere un'espressione regex valida. I tipi non String vengono convertiti in tipi String usando le regole di conversione standard. A seconda del tipo, la stringa risultante potrebbe non essere un'espressione regolare valida. Se l'argomento (convertito) non è un valore regex valido, il risultato è Undefined.

Terzo argomento:

Deve essere una stringa di sostituzione regex valida. Può fare riferimento a gruppi Capture. I tipi non String vengono convertiti in tipi String usando le regole di conversione standard. Se l'argomento (convertito) non è una stringa di sostituzione regex valida, il risultato è Undefined.

regexp_replace(String, String, String)

Sostituisce tutte le occorrenze del secondo argomento (espressione regolare) nel primo argomento con il terzo argomento. Può fare riferimento a gruppi Capture con "\$". Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:

```
Regexp_replace("abcd", "bc", "x") = "axd".
```

```
Regexp_replace("abcd", "b(.*)d", "$1") = "ac".
```

Primo argomento:

| Tipo di argomento | Risultato |
|-------------------|---|
| Int | Rappresentazione String del tipo Int. |
| Decimal | Rappresentazione String del tipo Decimal. |
| Boolean | Rappresentazione String del tipo Boolean ("true" o "false"). |
| String | Valore di origine. |
| Array | Rappresentazione String del tipo Array (usando le regole di conversione standard). |
| Oggetto | Rappresentazione String del tipo Object (usando le regole di conversione standard). |
| Null | Undefined. |
| Undefined | Undefined. |

Secondo argomento:

Deve essere un'espressione regex valida. I tipi non String vengono convertiti in tipi String usando le regole di conversione standard. A seconda del tipo, la stringa risultante potrebbe non essere un'espressione regolare valida. Se l'argomento (convertito) non è un'espressione regex valida, il risultato è Undefined.

Terzo argomento:

Deve essere una stringa di sostituzione regex valida. Può fare riferimento a gruppi Capture. I tipi non String vengono convertiti in tipi String usando le regole di conversione standard. Se l'argomento (convertito) non è una stringa di sostituzione regex valida, il risultato è Undefined.

regexp_substr(String, String)

Trova la prima corrispondenza del secondo parametro (regex) nel primo parametro. Può fare riferimento a gruppi Capture con "\$". Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:

```
regexp_substr("hihihello", "hi") => "hi"
regexp_substr("hihihello", "(hi)*") => "hihi".
```

Primo argomento:

| Tipo di argomento | Risultato |
|-------------------|--|
| Int | Rappresentazione String del tipo Int. |
| Decimal | Rappresentazione String del tipo Decimal. |
| Boolean | Rappresentazione String del tipo Boolean ("true" o "false"). |
| String | Argomento String. |

| Tipo di argomento | Risultato |
|-------------------|---|
| Array | Rappresentazione <code>String</code> del tipo <code>Array</code> (usando le regole di conversione standard). |
| Oggetto | Rappresentazione <code>String</code> del tipo <code>Object</code> (usando le regole di conversione standard). |
| Null | <code>Undefined</code> . |
| Undefined | <code>Undefined</code> . |

Secondo argomento:

Deve essere un'espressione regex valida. I tipi non `String` vengono convertiti in tipi `String` usando le regole di conversione standard. A seconda del tipo, la stringa risultante potrebbe non essere un'espressione regolare valida. Se l'argomento (convertito) non è un'espressione regex valida, il risultato è `Undefined`.

Terzo argomento:

Deve essere una stringa di sostituzione regex valida. Può fare riferimento a gruppi Capture. I tipi non `String` vengono convertiti in tipi `String` usando le regole di conversione standard. Se l'argomento non è una stringa di sostituzione regex valida, il risultato è `Undefined`.

rpad(String, Int)

Restituisce l'argomento `String` con spaziatura sul lato destro, con il numero di spazi specificato nel secondo argomento. L'argomento `Int` deve essere compreso tra 0 e 1.000. Se il valore fornito è al di fuori di questo intervallo valido, l'argomento viene impostato sul valore valido più vicino (0 o 1000). Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

`rpad("hello", 2) = "hello "`.

`rpad(1, 3) = "1"`.

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|---------------------|------------------|--|
| <code>String</code> | <code>Int</code> | Al tipo <code>String</code> viene aggiunta una spaziatura sul lato destro, con un numero di spazi corrispondente al valore <code>Int</code> fornito. |

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|------------------|------------------|---|
| String | Decimal | L'argomento Decimal viene arrotondato per difetto al valore Int più vicino e alla stringa viene aggiunta una spaziatura sul lato destro, con un numero di spazi corrispondente al valore Int fornito. |

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|------------------|------------------|---|
| String | String | Il secondo argomento viene convertito in un tipo Decimal, arrotondato per difetto al valore Int più vicino. Al tipo String viene aggiunta una spaziatura sul lato destro, con un numero di spazi corrispondente al valore Int . |

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|------------------|--------------------|--|
| Altro valore | Int/Decimal/String | Il primo valore viene convertito in un tipo String usando le conversioni standard e quindi al tipo String viene applicata la funzione rpad. Se la conversione non è possibile, il risultato è Undefined. |
| qualsiasi valore | Altro valore | Undefined. |

round(Decimal)

Arrotonda il tipo Decimal specificato al valore Int più vicino. Se Decimal è equidistante da due valori Int (ad esempio, 0,5), il tipo Decimal viene arrotondato per eccesso. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `Round(1.2) = 1.`

`Round(1.5) = 2.`

`Round(1.7) = 2.`

`Round(-1.1) = -1.`

`Round(-1.5) = -2.`

| Tipo di argomento | Risultato |
|-------------------|---|
| Int | Argomento. |
| Decimal | Decimal viene arrotondato per difetto al valore Int più vicino. |

| Tipo di argomento | Risultato |
|-------------------|---|
| String | Decimal viene arrotondato per difetto al valore Int più vicino. Se la stringa non può essere convertita in un tipo Decimal, il risultato è Undefined. |
| Altro valore | Undefined. |

rtrim(String)

Rimuove tutti gli spazi vuoti finali (tabulazioni e spazi) dal tipo String fornito. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
rtrim(" h i ") = " h i"
```

| Tipo di argomento | Risultato |
|-------------------|---|
| Int | Rappresentazione String del tipo Int. |
| Decimal | Rappresentazione String del tipo Decimal. |
| Boolean | Rappresentazione String del tipo Boolean ("true" o "false"). |
| Array | Rappresentazione String del tipo Array (usando le regole di conversione standard). |
| Oggetto | Rappresentazione String del tipo Object (usando le regole di conversione standard). |
| Null | Undefined. |
| Undefined | Undefined |

sign(Decimal)

Restituisce il segno di un determinato numero. Quando il segno dell'argomento è positivo, viene restituito 1. Quando il segno dell'argomento è negativo, viene restituito -1. Se l'argomento è 0, viene restituito 0. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
sign(-7) = -1.
```

```
sign(0) = 0.
```

```
sign(13) = 1.
```

| Tipo di argomento | Risultato |
|-------------------|-----------------------------------|
| Int | Int, il segno del valore Int. |
| Decimal | Int, il segno del valore Decimal. |

| Tipo di argomento | Risultato |
|-------------------|--|
| String | Int, il segno del valore Decimal. La stringa viene convertita in un valore Decimal e viene restituito il segno del valore Decimal. Se il tipo String non può essere convertito in Decimal, il risultato è Undefined. Supportata da SQL versione 2015-10-8 e versioni successive. |
| Altro valore | Undefined. |

sin(Decimal)

Restituisce il seno di un numero in radianti. Gli argomenti Decimal vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: $\sin(0) = 0.0$

| Tipo di argomento | Risultato |
|-------------------|--|
| Int | Decimal (a precisione doppia), il seno dell'argomento. |
| Decimal | Decimal (a precisione doppia), il seno dell'argomento. |
| Boolean | Undefined. |
| String | Decimal (a precisione doppia), il seno dell'argomento. Se la stringa non può essere convertita in un tipo Decimal, il risultato è Undefined. |
| Array | Undefined. |
| Oggetto | Undefined. |
| Null | Undefined. |
| Undefined | Undefined. |

sinh(Decimal)

Restituisce il seno iperbolico di un numero. I valori Decimal vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Il risultato è un valore Decimal a precisione doppia. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: $\sinh(2.3) = 4.936961805545957$

| Tipo di argomento | Risultato |
|-------------------|---|
| Int | Decimal (a precisione doppia), il seno iperbolico dell'argomento. |
| Decimal | Decimal (a precisione doppia), il seno iperbolico dell'argomento. |

| Tipo di argomento | Risultato |
|-------------------|---|
| Boolean | Undefined. |
| String | Decimal (a precisione doppia), il seno iperbolico dell'argomento. Se la stringa non può essere convertita in un tipo Decimal, il risultato è Undefined. |
| Array | Undefined. |
| Oggetto | Undefined. |
| Null | Undefined. |
| Undefined | Undefined. |

substring(String, Int [, Int])

Richiede un tipo String seguito da uno o due valori Int. Per un tipo String e un singolo argomento Int, questa funzione restituisce la sottostringa del tipo String fornito dall'indice Int specificato (in base 0, incluso) fino alla fine di String. Per un tipo String e due argomenti Int, questa funzione restituisce la sottostringa del tipo String fornito dal primo argomento di indice Int specificato (in base 0, incluso) al secondo argomento di indice Int (in base 0, escluso). Gli indici inferiori a zero vengono impostati su zero. Gli indici superiori alla lunghezza di String vengono impostati sulla lunghezza di String. Per la versione con tre argomenti, se il primo indice è maggiore o uguale al secondo indice, il risultato è il tipo String vuoto.

Se gli argomenti forniti non sono (*String, Int*) o (*String, Int, Int*), viene effettuato il tentativo di convertirli nei tipi corretti applicando le conversioni standard. Se i tipi non possono essere convertiti, il risultato della funzione è Undefined. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
substring("012345", 0) = "012345".
substring("012345", 2) = "2345".
substring("012345", 2.745) = "2345".
substring(123, 2) = "3".
substring("012345", -1) = "012345".
substring(true, 1.2) = "rue".
substring(false, -2.411E247) = "false".
substring("012345", 1, 3) = "12".
substring("012345", -50, 50) = "012345".
substring("012345", 3, 1) = "".
```

sqrt(Decimal)

Restituisce la radice quadrata di un numero. Gli argomenti Decimal vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `sqrt(9) = 3.0.`

| Tipo di argomento | Risultato |
|------------------------|--|
| <code>Int</code> | Radice quadrata dell'argomento. |
| <code>Decimal</code> | Radice quadrata dell'argomento. |
| <code>Boolean</code> | <code>Undefined.</code> |
| <code>String</code> | Radice quadrata dell'argomento. Se la stringa non può essere convertita in un tipo <code>Decimal</code> , il risultato è <code>Undefined.</code> |
| <code>Array</code> | <code>Undefined.</code> |
| <code>Oggetto</code> | <code>Undefined.</code> |
| <code>Null</code> | <code>Undefined.</code> |
| <code>Undefined</code> | <code>Undefined.</code> |

startswith(String, String)

Restituisce un tipo `Boolean` che indica se il primo argomento `String` inizia con il secondo argomento `String`. Se uno degli argomenti è `Null` oppure `Undefined`, il risultato è `Undefined`. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:

`startswith("ranger", "ran") = true`

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|---------------------|---------------------|---|
| <code>String</code> | <code>String</code> | Indica se il primo argomento <code>String</code> . |
| Altro valore | Altro valore | Entrambi gli argomenti sono di tipo <code>String</code> . Il risultato è <code>true</code> se il primo argomento è una stringa che inizia con il secondo argomento <code>String</code> . Se uno degli argomenti è <code>Null</code> oppure <code>Undefined</code> , il risultato è <code>Undefined</code> . |

tan(Decimal)

Restituisce la tangente di un numero in radianti. I valori `Decimal` vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `tan(3) = -0.1425465430742778`

| Tipo di argomento | Risultato |
|-------------------|---|
| <code>Int</code> | <code>Decimal</code> (a precisione doppia), la tangente dell'argomento. |

| Tipo di argomento | Risultato |
|-------------------|--|
| Decimal | Decimal (a precisione doppia), la tangente dell'argomento. |
| Boolean | Undefined. |
| String | Decimal (a precisione doppia), la tangente dell'argomento. Se la stringa non può essere convertita in un tipo Decimal, il risultato è Undefined. |
| Array | Undefined. |
| Oggetto | Undefined. |
| Null | Undefined. |
| Undefined | Undefined. |

tanh(Decimal)

Restituisce la tangente iperbolica di un numero in radianti. I valori Decimal vengono arrotondati a un valore a precisione doppia prima dell'applicazione della funzione. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `tanh(2.3) = 0.9800963962661914`

| Tipo di argomento | Risultato |
|-------------------|---|
| Int | Decimal (a precisione doppia), la tangente iperbolica dell'argomento. |
| Decimal | Decimal (a precisione doppia), la tangente iperbolica dell'argomento. |
| Boolean | Undefined. |
| String | Decimal (a precisione doppia), la tangente iperbolica dell'argomento. Se la stringa non può essere convertita in un tipo Decimal, il risultato è Undefined. |
| Array | Undefined. |
| Oggetto | Undefined. |
| Null | Undefined. |
| Undefined | Undefined. |

timestamp()

Restituisce il timestamp corrente in millisecondi da giovedì, 1 gennaio 1970, 00:00:00 UTC (Coordinated Universal Time), come rilevato dal motore di regole AWS IoT. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio: `timestamp() = 1481825251155`

topic(Decimal)

Restituisce l'argomento a cui è stato inviato il messaggio che ha attivato la regola. Se non viene specificato alcun parametro, viene restituito l'intero argomento. Il parametro `Decimal` viene utilizzato per specificare un segmento di argomento specifico, con 1 che indica il primo segmento. Per l'argomento `foo/bar/baz`, `topic(1)` restituisce `foo`, `topic(2)` restituisce `bar` e così via. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
topic() = "things/myThings/thingOne"  
topic(1) = "things"
```

Quando viene utilizzato [Basic Ingest \(p. 333\)](#), il prefisso iniziale dell'argomento (`$aws/rules/rule-name`) non è disponibile per la funzione dell'argomento(). Ad esempio, dato l'argomento:

```
$aws/rules/BuildingManager/Buildings/Building5/Floor2/Room201/Lights  
topic() = "Buildings/Building5/Floor2/Room201/Lights"  
topic(3) = "Floor2"
```

traceid()

Restituisce l'ID traccia (UUID) del messaggio MQTT oppure `Undefined` se il messaggio non è stato inviato tramite MQTT. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:

```
traceid() = "12345678-1234-1234-1234-123456789012"
```

trunc(Decimal, Int)

Tronca il primo argomento al numero di posizioni `Decimal` specificato nel secondo argomento. Se il secondo argomento è inferiore a zero, viene impostato su zero. Se il secondo argomento è superiore a 34, viene impostato su 34. Gli zeri finali vengono eliminati dal risultato. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
trunc(2.3, 0) = 2.  
trunc(2.3123, 2) = 2.31.  
trunc(2.888, 2) = 2.88.  
trunc(2.00, 5) = 2.
```

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|---------------------------------|--------------------------|---|
| <code>Int</code> | <code>Int</code> | Valore di origine. |
| <code>Int/Decimal</code> | <code>Int/Decimal</code> | Il primo argomento viene troncato dal secondo argomento. Se il secondo argomento è di tipo <code>Int</code> , viene arrondito al valore più vicino. |
| <code>Int/Decimal/String</code> | <code>Int/Decimal</code> | Il primo argomento viene troncato dal secondo argomento. |

| Tipo argomento 1 | Tipo argomento 2 | Risultato |
|------------------|------------------|--|
| | | un tipo <code>Int</code> , viene arr più vicino. Un tipo <code>St Decimal</code> . Se la conver risultato è <code>Undefined</code> . |
| Altro valore | | <code>Undefined</code> . |

trim(String)

Rimuove tutti gli spazi vuoti iniziali e finali dal tipo `String` fornito. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempio:

```
Trim(" hi ") = "hi"
```

| Tipo di argomento | Risultato |
|------------------------|--|
| <code>Int</code> | Rappresentazione <code>String</code> del tipo <code>Int</code> con tutti gli spazi vuoti iniziali e finali rimossi. |
| <code>Decimal</code> | Rappresentazione <code>String</code> del tipo <code>Decimal</code> con tutti gli spazi vuoti iniziali e finali rimossi. |
| <code>Boolean</code> | Rappresentazione <code>String</code> del tipo <code>Boolean</code> ("true" o "false") con tutti gli spazi vuoti iniziali e finali rimossi. |
| <code>String</code> | Tipo <code>String</code> con tutti gli spazi vuoti iniziali e finali rimossi. |
| <code>Array</code> | Rappresentazione <code>String</code> del tipo <code>Array</code> usando le regole di conversione standard. |
| Oggetto | Rappresentazione <code>String</code> del tipo <code>Object</code> usando le regole di conversione standard. |
| <code>Null</code> | <code>Undefined</code> . |
| <code>Undefined</code> | <code>Undefined</code> . |

upper(String)

Restituisce la versione con caratteri maiuscoli del tipo `String` specificato. Gli argomenti non di tipo `String` vengono convertiti in `String` usando le regole di conversione standard. Supportata da SQL versione 2015-10-8 e versioni successive.

Esempi:

```
upper("hello") = "HELLO"  
upper(["hello"]) = "["HELLO\"]"
```

Clausola SELECT

La clausola SELECT AWS IoT equivale essenzialmente alla clausola SELECT ANSI SQL, con alcune piccole differenze.

È possibile usare la clausola SELECT per estrarre informazioni dai messaggi MQTT in ingresso. SELECT * permette di recuperare l'intero payload del messaggio in ingresso. Ad esempio:

```
Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL statement: SELECT * FROM 'a/b'
Outgoing payload: {"color":"red", "temperature":50}
```

Se il payload è un oggetto JSON, è possibile fare riferimento alle chiavi nell'oggetto. Il payload in uscita contiene la coppia chiave-valore. Ad esempio:

```
Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL statement: SELECT color FROM 'a/b'
Outgoing payload: {"color":"red"}
```

È possibile usare la parola chiave AS per rinominare le chiavi. Ad esempio:

```
Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL: SELECT color AS my_color FROM 'a/b'
Outgoing payload: {"my_color":"red"}
```

È possibile selezionare più elementi separandoli con una virgola. Ad esempio:

```
Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL: SELECT color as my_color, temperature as farenheit FROM 'a/b'
Outgoing payload: {"my_color":"red", "farenheit":50}
```

È possibile selezionare più elementi includendo "*" per aggiungere gli elementi al payload in ingresso. Ad esempio:

```
Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL: SELECT *, 15 as speed FROM 'a/b'
Outgoing payload: {"color":"red", "temperature":50, "speed":15}
```

È possibile usare la parola chiave "VALUE" per produrre payload in uscita che non sono oggetti JSON. È possibile selezionare un solo elemento. Ad esempio:

```
Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL: SELECT VALUE color FROM 'a/b'
Outgoing payload: "red"
```

È possibile usare la sintassi '.' per analizzare in maggiore dettaglio gli oggetti JSON nidificati nel payload in ingresso. Ad esempio:

```
Incoming payload published on topic 'a/b': {"color":{"red":255,"green":0,"blue":0},
"temperature":50}
SQL: SELECT color.red as red_value FROM 'a/b'
Outgoing payload: {"red_value":255}
```

È possibile usare le funzioni (consulta [Funzioni \(p. 289\)](#)) per trasformare il payload in ingresso. Le parentesi permettono di raggruppare più elementi. Ad esempio:

```
Incoming payload published on topic 'a/b': {"color":"red", "temperature":50}
SQL: SELECT (temperature - 32) * 5 / 9 AS celsius, upper(color) as my_color FROM 'a/b'
Outgoing payload: {"celsius":10,"my_color":"RED"}
```

Uso di payload binari

Quando il payload del messaggio deve essere gestito come dati binari non elaborati (invece che come oggetto JSON), è possibile usare l'operatore * per farvi riferimento in una clausola SELECT.

Per usare * per fare riferimento al payload del messaggio come dati binari non elaborati, segui queste regole:

1. I modelli e l'istruzione SQL non devono fare riferimento a nomi JSON diversi da *.
2. L'istruzione SELECT deve avere * come unico elemento oppure deve includere solo funzioni, ad esempio:

```
SELECT * FROM 'a/b'
```

```
SELECT encode(*, 'base64') AS data, timestamp() AS ts FROM 'a/b'
```

Esempi di payload binari

La clausola SELECT seguente può essere usata con i payload binari perché non fa riferimento a nomi JSON.

```
SELECT * FROM 'a/b'
```

La clausola SELECT seguente non può essere usata con i payload binari perché fa riferimento a device_type nella clausola WHERE.

```
SELECT * FROM 'a/b' WHERE device_type = 'thermostat'
```

La clausola SELECT seguente non può essere usata con payload binari perché viola la regola 2.

```
SELECT *, timestamp() AS timestamp FROM 'a/b'
```

La clausola SELECT seguente può essere usata con payload binari perché non viola le regole 1 e 2.

```
SELECT * FROM 'a/b' WHERE timestamp() % 12 = 0
```

La regola AWS IoT seguente non può essere usata con i payload perché viola la regola 1.

```
{
    "sql": "SELECT * FROM 'a/b'",
    "actions": [
        {
            "republish": {
                "topic": "device/${device_id}"
            }
        }
    ]
}
```

Clausola FROM

La clausola FROM esegue la sottoscrizione della regola in un argomento o un filtro di argomenti. L'argomento o il filtro dell'argomento deve essere racchiuso tra virgolette singole (''). La regola viene attivata

per ogni messaggio inviato a un argomento MQTT che corrisponde al filtro argomento specificato qui. Un filtro di argomenti permette di eseguire la sottoscrizione di un gruppo di argomenti simili.

Esempio:

Payload in ingresso pubblicato nell'argomento 'a/b': {temperature: 50}

Payload in ingresso pubblicato nell'argomento 'a/c': {temperature: 50}

SQL: "SELECT temperature AS t FROM 'a/b'".

La regola viene sottoscritta in 'a/b', quindi il payload in ingresso viene passato alla regola e il payload in uscita (passato alle operazioni della regola) è: {t: 50}. La regola non viene sottoscritta in 'a/c', quindi la regola non viene attivata per il messaggio pubblicato in 'a/c'.

Esempio di carattere jolly #:

Puoi utilizzare il carattere jolly '#' (multi-livello) per la corrispondenza con uno o più elementi del percorso particolari:

Payload in ingresso pubblicato nell'argomento 'a/b': {temperature: 50}.

Payload in ingresso pubblicato nell'argomento 'a/c': {temperature: 60}.

Payload in ingresso pubblicato nell'argomento 'a/e/f': {temperature: 70}.

Payload in ingresso pubblicato nell'argomento 'b/x': {temperature: 80}.

SQL: "SELECT temperature AS t FROM 'a/#'".

La regola viene sottoscritta per qualsiasi argomento che inizia con 'a', quindi viene eseguita tre volte, inviando i payload in uscita di {t: 50} (per a/b), {t: 60} (per a/c) e {t: 70} (per a/e/f) alle operazioni. Non viene sottoscritta in 'b/x', pertanto la regola non viene attivata per il messaggio {temperature: 80}.

Esempio di carattere jolly +:

Puoi utilizzare il carattere jolly '+' (livello singolo) per la corrispondenza con qualsiasi elemento del percorso particolare:

Payload in ingresso pubblicato nell'argomento 'a/b': {temperature: 50}.

Payload in ingresso pubblicato nell'argomento 'a/c': {temperature: 60}.

Payload in ingresso pubblicato nell'argomento 'a/e/f': {temperature: 70}.

Payload in ingresso pubblicato nell'argomento 'b/x': {temperature: 80}.

SQL: "SELECT temperature AS t FROM 'a/+'".

La regola viene sottoscritta in tutti gli argomenti con due elementi di percorso, dove il primo elemento è 'a'. La regola viene eseguita per i messaggi inviati a 'a/b' e 'a/c', ma non a 'a/e/f' o 'b/x'.

Clausola WHERE

La clausola WHERE determina se le operazioni specificate da una regola vengono eseguite. Se la clausola WHERE restituisce true, le operazioni della regola vengono eseguite. In caso contrario, le operazioni della regola non vengono eseguite.

Esempio:

Payload in ingresso pubblicato in a/b: {"color": "red", "temperature": 40}.

SQL: `SELECT color AS my_color FROM 'a/b' WHERE temperature > 50 AND color <> 'red'.`

In questo caso la regola verrebbe attivata, ma non verrebbero eseguite le operazioni specificate dalla regola. Non ci sarebbe alcun payload in uscita.

È possibile usare le funzioni e gli operatori nella clausola WHERE. Tuttavia, non è possibile fare riferimento agli alias creati con la parola chiave AS in SELECT. La clausola WHERE viene valutata per prima, per determinare se la clausola SELECT viene valutata.

Valori letterali

È possibile specificare direttamente oggetti letterali nelle clausole SELECT e WHERE della regola SQL, che possono essere utili per passare informazioni.

Note

I valori letterali sono disponibili solo quando si usa SQL 2016-03-23 o una versione successiva.

Viene usata la sintassi degli oggetti JSON (coppie chiave-valore, separate da virgolette, dove le chiavi sono stringhe e i valori sono valori JSON, racchiusi tra parentesi graffe {}). Ad esempio:

Payload in ingresso pubblicato nell'argomento a/b: {"lat_long": [47.606, -122.332]}

Istruzione SQL: `SELECT {'latitude': get(lat_long, 0), 'longitude': get(lat_long, 1)} as lat_long FROM 'a/b'`

Il payload in uscita risultante sarebbe: {"lat_long": {"latitude": 47.606, "longitude": -122.332}}.

È anche possibile specificare direttamente matrici nelle clausole SELECT e WHERE della regola SQL, per poter raggruppare le informazioni. Viene usata la sintassi JSON (elementi separati da virgola racchiusi tra parentesi quadre [] per creare una matrice letterale). Ad esempio:

Payload in ingresso pubblicato nell'argomento a/b: {"lat": 47.696, "long": -122.332}

Istruzione SQL: `SELECT [lat, long] as lat_long FROM 'a/b'`

Il payload in uscita risultante sarebbe: {"lat_long": [47.606, -122.332]}.

Istruzioni case

Le istruzioni case possono essere usate per l'esecuzione con diramazioni, come un'istruzione switch o istruzioni if/else.

Sintassi:

```
CASE v WHEN t[1] THEN r[1]
          WHEN t[2] THEN r[2] ...
          WHEN t[n] THEN r[n]
          ELSE r[e] END
```

L'espressione v viene valutata e confrontata per verificare la corrispondenza con ogni espressione t[i]. Se viene trovata una corrispondenza, l'espressione r[i] diventa il risultato dell'istruzione case. Se ci sono più corrispondenze possibili, viene selezionata la prima corrispondenza. Se non ci sono corrispondenze, viene usato come risultato l'elemento re dell'istruzione else. Se non ci sono corrispondenze e non c'è un'istruzione else, il risultato dell'istruzione case è Undefined. Ad esempio:

Payload in ingresso pubblicato nell'argomento a/b: {"color": "yellow"}

Istruzione SQL: `SELECT CASE color WHEN 'green' THEN 'go' WHEN 'yellow' THEN 'caution' WHEN 'red' THEN 'stop' ELSE 'you are not at a stop light' END as instructions FROM 'a/b'`

Il payload in uscita risultante sarebbe: {"instructions": "caution"}.

Le istruzioni case richiedono almeno una clausola WHEN. La clausola ELSE non è obbligatoria.

Note

Se v è Undefined, il risultato dell'istruzione case è Undefined.

Estensioni JSON

È possibile usare le estensioni seguenti nella sintassi SQL ANSI per semplificare l'uso degli oggetti JSON nidificati.

Operatore ". "

Questo operatore accede ai membri negli oggetti JSON incorporati e funziona in modo identico a quanto avviene in SQL ANSI e JavaScript. Ad esempio:

```
SELECT foo.bar AS bar.baz FROM 'a/b'
```

Operatore *

Funziona nello stesso modo del carattere jolly * in SQL ANSI. Viene usato solo nella clausola SELECT e crea un nuovo oggetto JSON contenente i dati del messaggio. Se il payload del messaggio non è in formato JSON, * restituisce l'intero payload del messaggio come byte non elaborati. Ad esempio:

```
SELECT * FROM 'a/b'
```

Applicazione di un funzione a un valore di attributo

Di seguito è illustrato un esempio di payload JSON che potrebbe essere pubblicato da un dispositivo:

```
{
    "deviceid" : "iot123",
    "temp" : 54.98,
    "humidity" : 32.43,
    "coords" : {
        "latitude" : 47.615694,
        "longitude" : -122.3359976
    }
}
```

L'esempio seguente applica una funzione a un valore di attributo in un payload JSON:

```
SELECT temp, md5(deviceid) AS hashed_id FROM topic/#
```

Il risultato di questa query è l'oggetto JSON seguente:

```
{
    "temp": 54.98,
```

```
        "hashed_id": "e37f81fb397e595c4aeb5645b8cbbbd1"  
    }
```

Modelli di sostituzione

È possibile usare un modello di sostituzione per aumentare i dati JSON restituiti quando una regola viene attivata e AWS IoT esegue un'operazione. La sintassi di un modello di sostituzione è `#{espressione}`, dove espressione può essere qualsiasi espressione supportata da AWS IoT nelle clausole SELECT o WHERE. Questo include funzioni, operatori e informazioni presenti nel payload del messaggio originale. Dal momento che un'espressione in un modello di sostituzione viene valutata separatamente dall'istruzione "SELECT...", non è possibile fare riferimento a un alias creato utilizzando la clausola AS. Per ulteriori informazioni sulle espressioni supportate, consulta [Documentazione di riferimento su SQL per AWS IoT \(p. 279\)](#).

I modelli di sostituzione sono inclusi nella clausola SELECT all'interno di una regola:

```
{  
    "sql": "SELECT *, topic() AS topic FROM 'my/iot/topic'",  
    "ruleDisabled": false,  
    "actions": [  
        {  
            "republish": {  
                "topic": "${topic()}/republish",  
                "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"  
            }  
        }  
    ]  
}
```

Se questa regola viene attivata dal codice JSON seguente:

```
{  
    "deviceid" : "iot123",  
    "temp" : 54.98,  
    "humidity" : 32.43,  
    "coords" : {  
        "latitude" : 47.615694,  
        "longitude" : -122.3359976  
    }  
}
```

L'output della regola è il seguente:

```
{  
    "coords":{  
        "longitude": -122.3359976,  
        "latitude": 47.615694  
    },  
    "humidity": 32.43,  
    "temp": 54.98,  
    "deviceid": "iot123",  
    "topic": "my/iot/topic"  
}
```

Versioni SQL

Il motore di regole AWS IoT usa una sintassi di tipo SQL per selezionare i dati dai messaggi MQTT. Le istruzioni SQL vengono interpretate in base a una versione di SQL specificata con la proprietà

`awsIotSqlVersion` in un documento JSON che descrive la regola. Per ulteriori informazioni sulla struttura dei documenti di regole JSON, consulta la pagina relativa alla [creazione di una regola \(p. 256\)](#). La proprietà `awsIotSqlVersion` permette di specificare la versione del motore di regole SQL AWS IoT da usare. Quando viene distribuita una nuova versione, è possibile continuare a usare una versione precedente o modificare la regola per usare la nuova versione. Le regole correnti continuano a usare la versione con cui sono state create.

L'esempio JSON seguente illustra come specificare la versione SQL usando la proprietà `awsIotSqlVersion`:

```
{  
    "sql": "expression",  
    "ruleDisabled": false,  
    "awsIotSqlVersion": "2016-03-23",  
    "actions": [  
        {  
            "republish": {  
                "topic": "my-mqtt-topic",  
                "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"  
            }  
        }  
    ]  
}
```

Le versioni attualmente supportate sono:

- 2015-10-08, versione SQL originale creata l'08/10/2015.
- 2016-03-23, versione SQL creata il 23/03/2016.
- **beta**, la più recente versione beta di SQL. L'uso di questa versione potrebbe comportare modifiche che interrompono il funzionamento delle regole.

Novità della versione del motore di regole SQL 2016-03-23

- Correzioni per la selezione di oggetti JSON nidificati.
- Correzioni per le query su matrici.
- Supporto per query all'interno di un oggetto.
- Supporto per l'output di una matrice come oggetto di primo livello.
- Aggiunta della funzione `encode (value, encodingScheme)`, che può essere applicata ai dati in formato JSON e non JSON.

Query all'interno di oggetti

Questa caratteristica permette di eseguire query per un attributo in un oggetto JSON. Ad esempio, partendo dal messaggio MQTT seguente:

```
{  
    "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 }  
    ]  
}
```

E dalla regola seguente:

```
SELECT (SELECT v FROM e WHERE n = 'temperature') as temperature FROM 'my/topic'
```

La regola genera l'output seguente:

```
{"temperature": [{"v":22.5}]}
```

Usando lo stesso messaggio MQTT con una regola leggermente più complessa, ad esempio:

```
SELECT get((SELECT v FROM e WHERE n = 'temperature'),1).v as temperature FROM 'topic'
```

La regola genera l'output seguente:

```
{"temperature":22.5}
```

Output di un oggetto Array come oggetto di primo livello

Questa caratteristica permette a una regola di restituire una matrice come oggetto di primo livello. Ad esempio, partendo dal messaggio MQTT seguente:

```
{
    "a": {"b":"c"},
    "arr":[1,2,3,4]
}
```

E dalla regola seguente:

```
SELECT VALUE arr FROM 'topic'
```

La regola genera l'output seguente:

```
[1,2,3,4]
```

Funzione encode

Codifica il payload, che potenzialmente può essere costituito da dati non JSON, nella rappresentazione di stringa in base allo schema di codifica specificato.

Basic Ingest

Basic Ingest consente di inviare in modo sicuro i dati del dispositivo ai servizi AWS supportati da [Operazioni delle regole AWS IoT \(p. 261\)](#) senza dover sostenere i [costi di messaggistica](#). Basic Ingest ottimizza il flusso di dati rimuovendo il broker di messaggi di pubblicazione/sottoscrizione dal percorso di inserimento per una maggiore efficacia in termini di costi, pur mantenendo la sicurezza e le caratteristiche di elaborazione dei dati di AWS IoT.

Per usare Basic Ingest, puoi inviare messaggi da dispositivi o applicazioni con nomi di argomento che iniziano con `$aws/rules/rule-name` come primi tre livelli, dove *rule-name* è il nome della regola AWS IoT da attivare.

Puoi continuare a utilizzare una regola esistente con Basic Ingest semplicemente aggiungendo il prefisso Basic Ingest (`$aws/rules/rule-name`) all'argomento del messaggio con cui generalmente attivi la regola. Ad esempio, se si dispone di una regola denominata "BuildingManager" che viene attivata da messaggi con argomenti di tipo "Buildings/Building5/Floor2/Room201/Lights" ("sql": "SELECT * FROM 'Buildings/#'"), è possibile attivare la stessa regola con Basic Ingest inviando un messaggio con argomento `$aws/rules/BuildingManager/Buildings/Building5/Floor2/Room201/Lights`.

È necessario tenere presente quanto segue:

- I dispositivi e le regole non possono essere iscritti ad argomenti Basic Ingest riservati. Per informazioni dettagliate, consulta [Argomenti riservati \(p. 241\)](#).
- Se hai bisogno di un broker di pubblicazione/sottoscrizione per distribuire messaggi a più sottoscrittori (per esempio, per distribuire i messaggi ad altri dispositivi nonché al Motore di regole), è necessario continuare a utilizzare il broker di messaggi AWS IoT per gestire la distribuzione dei messaggi. È sufficiente pubblicare messaggi su argomenti diversi dagli argomenti Basic Ingest.

Per utilizzare Basic Ingest

Assicurati che il tuo dispositivo o la tua applicazione utilizzi una [policy \(p. 198\)](#) con autorizzazioni di pubblicazione su `$aws/rules/*`. In alternativa, è possibile specificare autorizzazioni per regole singole con `$aws/rules/rule-name/*` nella policy. In caso contrario, i dispositivi e le applicazioni possono continuare a utilizzare le connessioni esistenti con AWS IoT Core.

Quando il messaggio raggiunge il Motore di regole, non ci sono differenze di esecuzione o gestione dell'errore tra le regole attivate da Basic Ingest e quelle attivate tramite sottoscrizioni al broker di messaggi.

Naturalmente, è possibile creare regole da utilizzare con Basic Ingest. Ricorda:

- Il prefisso iniziale di un argomento Basic Ingest (`$aws/rules/rule-name`) non è disponibile per la funzione [topic\(Decimal\) \(p. 323\)](#).
- Se si definisce una regola che viene attivata solo con Basic Ingest, la clausola `FROM` è facoltativa nel campo `sql` della definizione `rule`. Se la regola sarà attivata anche da altri messaggi, è comunque necessario che venga attivata dal broker di messaggi (ad esempio, perché gli altri messaggi devono essere distribuiti a più sottoscrittori). Consulta [Documentazione di riferimento su SQL per AWS IoT \(p. 279\)](#).
- I primi tre livelli di argomento Basic Ingest (`$aws/rules/rule-name`) non vengono conteggiati ai fini del limite di lunghezza di otto segmenti o ai fini del limite totale di 256 caratteri per un argomento. In caso contrario, si applicano le stesse restrizioni, come documentato in [Limiti per AWS IoT](#).
- Se viene ricevuto un messaggio con un argomento Basic Ingest che specifica una regola inattiva o una regola che non esiste, viene creato un log dell'errore in un log di CloudWatch per aiutarti con il debug.

(consulta [Log del motore di regole \(p. 667\)](#)). È indicato un parametro "RuleNotFound" ed è possibile creare allarmi su questo parametro. Consulta la sezione sui parametri della regola in [Parametri di AWS IoT \(p. 646\)](#).

- È ancora possibile pubblicare con QoS 1 su argomenti Basic Ingest. Riceverai un PUBACK una volta che il messaggio sarà stato inviato correttamente al Motore di regole. Ricevere un PUBACK non significa che le azioni della regola sono state completate correttamente. È possibile configurare un'operazione di errore per gestire gli errori durante l'esecuzione dell'operazione. Consulta [Gestione degli errori \(operazione in caso di errore\) \(p. 277\)](#).

Servizio Device Shadow per AWS IoT

Una copia shadow di un dispositivo è un documento JSON usato per archiviare e recuperare informazioni sullo stato corrente di un dispositivo. Il servizio Device Shadow mantiene una copia shadow per ogni dispositivo che connetti a AWS IoT. Puoi usare la copia shadow per ottenere e impostare lo stato di un dispositivo tramite MQTT o HTTP, a prescindere che il dispositivo sia connesso o meno a Internet. Ogni copia shadow del dispositivo è identificata in modo univoco dal nome dell'oggetto corrispondente.

Indice

- [Flusso di dati del servizio Device Shadow \(p. 335\)](#)
- [Documenti del servizio Device Shadow \(p. 343\)](#)
- [Uso delle copie shadow \(p. 346\)](#)
- [API RESTful del servizio Device Shadow \(p. 355\)](#)
- [Argomenti MQTT del servizio Device Shadow \(p. 357\)](#)
- [Sintassi dei documenti del servizio Device Shadow \(p. 364\)](#)
- [Messaggi di errore del servizio Shadow \(p. 367\)](#)

Flusso di dati del servizio Device Shadow

Il servizio Device Shadow funge da intermediario, permettendo ai dispositivi e alle applicazioni di recuperare e aggiornare una copia shadow del dispositivo.

In questa sezione viene illustrato il modo in cui i dispositivi e le applicazioni comunicano con il servizio Device Shadow e viene spiegato nei dettagli l'uso del client MQTT AWS IoT e dell'interfaccia a riga di comando di AWS per simulare la comunicazione tra una lampadina connessa a Internet, un'applicazione e il servizio Device Shadow.

Il servizio Device Shadow usa argomenti MQTT per semplificare la comunicazione tra applicazioni e dispositivi. Per esaminare il funzionamento, usa il client MQTT AWS IoT per sottoscrivere gli argomenti MQTT seguenti con QoS 1:

\$aws/things/myLightBulb/shadow/update/accepted

Il servizio Device Shadow invia messaggi a questo argomento quando viene effettuato correttamente un aggiornamento di una copia shadow del dispositivo.

\$aws/things/myLightBulb/shadow/update/rejected

Il servizio Device Shadow invia messaggi a questo argomento quando viene rifiutato un aggiornamento di una copia shadow del dispositivo.

\$aws/things/myLightBulb/shadow/update/delta

Il servizio Device Shadow invia messaggi a questo argomento quando viene rilevata una differenza tra le sezioni sullo stato segnalato e sullo stato desiderato di una copia shadow del dispositivo. Per ulteriori informazioni, consulta [/update/delta \(p. 360\)](#).

\$aws/things/myLightBulb/shadow/get/accepted

Il servizio Device Shadow invia messaggi a questo argomento quando viene effettuata correttamente una richiesta di una copia shadow del dispositivo.

\$aws/things/myLightBulb/shadow/get/rejected

Il servizio Device Shadow invia messaggi a questo argomento quando viene rifiutata una richiesta di una copia shadow del dispositivo.

\$aws/things/myLightBulb/shadow/delete/accepted

Il servizio Device Shadow invia messaggi a questo argomento quando viene eliminata una copia shadow del dispositivo.

\$aws/things/myLightBulb/shadow/delete/rejected

Il servizio Device Shadow invia messaggi a questo argomento quando viene eliminata una richiesta di una copia shadow del dispositivo.

\$aws/things/myLightBulb/shadow/update/documents

Il servizio Device Shadow pubblica un documento sullo stato in questo argomento ogni volta che viene eseguito correttamente un aggiornamento alla copia shadow di un dispositivo.

Per ulteriori informazioni su tutti gli argomenti MQTT usati dal servizio Device Shadow, consulta [Argomenti MQTT del servizio Device Shadow \(p. 357\)](#).

Note

È consigliabile sottoscrivere gli argomenti .../rejected per visualizzare eventuali errori inviati dal servizio Device Shadow.

Quando la lampadina è online, comunica il suo stato corrente al servizio Device Shadow inviando un messaggio MQTT all'argomento \$aws/things/myLightBulb/shadow/update.

Note

Dispositivi ombra vengono creati la prima volta che si esegue un tentativo di aggiornamento. Il servizio Device Shadow rileverà che una copia shadow non esiste e verrà creata una. Se la copia shadow esiste, verrà aggiornata.

Per simulare questa operazione, usa il client MQTT AWS IoT per pubblicare il messaggio seguente nell'argomento \$aws/things/myLightBulb/shadow/update:

```
{  
  "state": {  
    "reported": {  
      "color": "red"  
    }  
  }  
}
```

Questo messaggio imposta il colore della lampadina su "red".

Il servizio Device Shadow risponde inviando il messaggio seguente all'argomento \$aws/things/myLightBulb/shadow/update/accepted:

```
{  
  "messageNumber": 4,  
  "payload": {  
    "state": {  
      "reported": {  
        "color": "red"  
      }  
    },  
    "metadata": {  
      "reported": {  
        "color": "red"  
      }  
    }  
  }  
}
```

```
        "color": {
            "timestamp": 1469564492
        }
    },
    "version": 1,
    "timestamp": 1469564492
},
"qos": 0,
"timestamp": 1469564492848,
"topic": "$aws/things/myLightBulb/shadow/update/accepted"
}
```

Questo messaggio indica che il servizio Device Shadow ha ricevuto la richiesta UPDATE e ha aggiornato la copia shadow del dispositivo. Se la copia shadow non esiste, viene creata. In caso contrario, la copia shadow viene aggiornata con i dati contenuti nel messaggio. Se un messaggio pubblicato in \$aws/things/myLightBulb/shadow/update/accepted non viene visualizzato, controlla la sottoscrizione di \$aws/things/myLightBulb/shadow/update/rejected per visualizzare eventuali messaggi di errore.

Il servizio Device Shadow pubblica inoltre il messaggio seguente nell'argomento \$aws/things/myLightBulb/shadow/update/documents.

```
{
    "previous":null,
    "current":{
        "state":{
            "reported":{
                "color":"red"
            }
        },
        "metadata":{
            "reported":{
                "color":{

                    "timestamp":1483467764
                }
            }
        },
        "version":1
    },
    "timestamp":1483467764
}
```

Vengono pubblicati messaggi nell'argomento /update/documents ogni volta che viene eseguito correttamente un aggiornamento alla copia shadow di un dispositivo. Per ulteriori informazioni sul contenuto dei messaggi pubblicati in questo argomento, consulta [Argomenti MQTT del servizio Device Shadow \(p. 357\)](#).

Un'applicazione che interagisce con la lampadina passa online e richiede lo stato corrente della lampadina. L'applicazione invia un messaggio vuoto all'argomento \$aws/things/myLightBulb/shadow/get. Per simulare questa operazione, usa il client MQTT AWS IoT per pubblicare un messaggio vuoto ("") nell'argomento \$aws/things/myLightBulb/shadow/get.

Il servizio Device Shadow risponde pubblicando la copia shadow richiesta nell'argomento \$aws/things/myLightBulb/shadow/get/accepted:

```
{
    "messageNumber": 1,
    "payload": {
        "state": {
            "reported": {

```

```
        "color": "red"
    },
},
"metadata": {
    "reported": {
        "color": {
            "timestamp": 1469564492
        }
    }
},
"version": 1,
"timestamp": 1469564571
},
"qos": 0,
"timestamp": 1469564571533,
"topic": "$aws/things/myLightBulb/shadow/get/accepted"
}
```

Se non viene visualizzato un messaggio nell'argomento `$aws/things/myLightBulb/shadow/get/accepted`, controlla se sono presenti messaggi di errore nell'argomento `$aws/things/myLightBulb/shadow/get/rejected`.

L'applicazione visualizza queste informazioni per l'utente e l'utente richiede una modifica del colore della lampadina (da rosso a verde). A tale scopo, l'applicazione pubblica un messaggio nell'argomento `$aws/things/myLightBulb/shadow/update`:

```
{
    "state": {
        "desired": {
            "color": "green"
        }
    }
}
```

Per simulare questa operazione, usa il client MQTT AWS IoT per pubblicare il messaggio precedente nell'argomento `$aws/things/myLightBulb/shadow/update`.

Il servizio Device Shadow risponde inviando un messaggio all'argomento `$aws/things/myLightBulb/shadow/update/accepted`:

```
{
    "messageNumber": 5,
    "payload": {
        "state": {
            "desired": {
                "color": "green"
            }
        },
        "metadata": {
            "desired": {
                "color": {
                    "timestamp": 1469564658
                }
            }
        },
        "version": 2,
        "timestamp": 1469564658
    },
    "qos": 0,
    "timestamp": 1469564658286,
    "topic": "$aws/things/myLightBulb/shadow/update/accepted"
}
```

e all'argomento `$aws/things/myLightBulb/shadow/update/delta`:

```
{  
    "messageNumber": 1,  
    "payload": {  
        "version": 2,  
        "timestamp": 1469564658,  
        "state": {  
            "color": "green"  
        },  
        "metadata": {  
            "color": {  
                "timestamp": 1469564658  
            }  
        }  
    },  
    "qos": 0,  
    "timestamp": 1469564658309,  
    "topic": "$aws/things/myLightBulb/shadow/update/delta"  
}
```

Il servizio Device Shadow pubblica un messaggio in questo argomento quando accetta un aggiornamento a una copia shadow e la copia shadow risultante contiene valori diversi per lo stato desiderato e per quello segnalato.

Il servizio Device Shadow pubblica anche un messaggio nell'argomento `$aws/things/myLightBulb/shadow/update/documents`:

```
{  
    "previous": {  
        "state": {  
            "reported": {  
                "color": "red"  
            }  
        },  
        "metadata": {  
            "reported": {  
                "color": {  
                    "timestamp": 1483467764  
                }  
            }  
        }  
    },  
    "version": 1,  
    "current": {  
        "state": {  
            "desired": {  
                "color": "green"  
            },  
            "reported": {  
                "color": "red"  
            }  
        },  
        "metadata": {  
            "desired": {  
                "color": {  
                    "timestamp": 1483468612  
                }  
            }  
        },  
        "reported": {  
            "color": {  
                "timestamp": 1483467764  
            }  
        }  
    }  
}
```

```
  },
  "version":2
},
"timestamp":1483468612
}
```

La lampadina ha una sottoscrizione nell'argomento `$aws/things/myLightBulb/shadow/update/delta`, quindi riceve il messaggio, cambia il proprio colore e pubblica il nuovo stato. Per simulare questa operazione, usa il client MQTT AWS IoT per pubblicare il messaggio seguente nell'argomento `$aws/things/myLightBulb/shadow/update` per aggiornare lo stato della copia shadow dell'oggetto:

```
{
  "state":{
    "reported":{
      "color":"green"
    },
    "desired":null
  }
}
```

In risposta, il servizio Device Shadow invia un messaggio all'argomento `$aws/things/myLightBulb/shadow/update/accepted`:

```
{
  "messageNumber": 6,
  "payload": {
    "state": {
      "reported": {
        "color": "green"
      },
      "desired": null
    },
    "metadata": {
      "reported": {
        "color": {
          "timestamp": 1469564801
        }
      },
      "desired": {
        "timestamp": 1469564801
      }
    },
    "version": 3,
    "timestamp": 1469564801
  },
  "qos": 0,
  "timestamp": 1469564801673,
  "topic": "$aws/things/myLightBulb/shadow/update/accepted"
}
```

e all'argomento `$aws/things/myLightBulb/shadow/update/documents`:

```
{
  "previous": {
    "state": {
      "reported": {
        "color": "red"
      }
    },
    "metadata": {
      "reported": {
        "color": {
          "timestamp": 1469564801
        }
      }
    }
  }
}
```

```
        "timestamp":1483470355
    }
},
"version":3
},
"current":{
    "state":{
        "reported":{
            "color":"green"
        }
    },
    "metadata":{
        "reported":{
            "color":{
                "timestamp":1483470364
            }
        }
    },
    "version":4
},
"timestamp":1483470364
}
```

L'app richiede lo stato corrente al servizio Device Shadow e visualizza i dati sullo stato più recenti. Per simulare questa operazione, esegui il comando seguente:

```
aws iot-data get-thing-shadow --thing-name "myLightBulb" "output.txt" && cat "output.txt"
```

Note

In Windows ometti `&& cat "output.txt"`, che visualizza i contenuti di `output.txt` nella console. Puoi aprire il file in Blocco note o in qualsiasi editor di testo per visualizzare i contenuti della copia shadow.

Il servizio Device Shadow restituisce il documento relativo alla copia shadow:

```
{
    "state":{
        "reported":{
            "color":"green"
        }
    },
    "metadata":{
        "reported":{
            "color":{
                "timestamp":1469564801
            }
        }
    },
    "version":3,
    "timestamp":1469564864
}
```

Per eliminare la copia shadow del dispositivo, pubblica un messaggio vuoto nell'argomento `$aws/things/myLightBulb/shadow/delete`. AWS IoT risponde con la pubblicazione di un messaggio nell'argomento `$aws/things/myLightBulb/shadow/delete/accepted`:

```
{
    "version" : 1,
    "timestamp" : 1488565234
}
```

Rilevamento della connessione di un oggetto

Per determinare se un dispositivo è attualmente connesso, includi un'impostazione connected nella copia shadow e usa un messaggio LWT (Last Will and Testament) MQTT che imposta il valore di connected su false se un dispositivo è disconnesso a causa di errore.

Note

Al momento, i messaggi LWT inviati ad argomenti riservati di AWS IoT (argomenti che iniziano con \$) vengono ignorati dal servizio Device Shadow AWS IoT, ma vengono comunque elaborati dai client sottoscritti e dal motore di regole di AWS IoT. Se desideri che il servizio Device Shadow riceva i messaggi LWT, registra un messaggio LWT in un argomento non riservato e crea una regola che ripubblica il messaggio nell'argomento riservato. L'esempio seguente mostra come creare una regola di ripubblicazione che si mette in ascolto dei messaggi dall'argomento my/things/myLightBulb/update e li ripubblica in \$aws/things/myLightBulb/shadow/update.

```
{  
    "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"  
                }  
            }  
        ]  
    }  
}
```

Quando un dispositivo si connette, registra un messaggio LWT che imposta il valore di connected su false:

```
{  
    "state": {  
        "reported": {  
            "connected": "false"  
        }  
    }  
}
```

Pubblica inoltre un messaggio nell'argomento update (\$aws/things/myLightBulb/shadow/update), impostando lo stato connected su true:

```
{  
    "state": {  
        "reported": {  
            "connected": "true"  
        }  
    }  
}
```

Quando il dispositivo si disconnette correttamente, pubblica un messaggio nell'argomento update e imposta lo stato connected su false:

```
{  
    "state": {  
        "reported": {  
            "connected": "false"  
        }  
    }  
}
```

```
    }  
}
```

Se il dispositivo si disconnette a causa di un errore, il messaggio LWT viene pubblicato automaticamente nell'argomento update.

Documenti del servizio Device Shadow

Il servizio Device Shadow rispetta tutte le regole della specifica JSON. Valori, oggetti e matrici sono archiviati nel documento della copia shadow del dispositivo.

Indice

- [Proprietà del documento \(p. 343\)](#)
- [Funzione Versioni multiple per una copia shadow di un dispositivo \(p. 344\)](#)
- [Token client \(p. 344\)](#)
- [Documento di esempio \(p. 344\)](#)
- [Sezioni vuote \(p. 345\)](#)
- [Matrici \(p. 345\)](#)

Proprietà del documento

Un documento di una copia shadow di un dispositivo ha le proprietà seguenti:

state

desired

Stato desiderato dell'oggetto. Le applicazioni possono scrivere in questa parte del documento per aggiornare lo stato di un oggetto senza doversi connettere direttamente a un oggetto.

reported

Stato segnalato dell'oggetto. Gli oggetti scrivono in questa parte del documento per segnalare il proprio nuovo stato. Le applicazioni leggono questa parte del documento per determinare lo stato di un oggetto.

metadata

Informazioni sui dati archiviati nella sezione state del documento. Le informazioni includono i timestamp, in base all'epoca (Unix epoch), per ogni attributo nella sezione state, che permettono di determinare quando gli attributi sono stati aggiornati.

Note

I metadati non contribuiscono alle dimensioni del documento per le restrizioni dei servizi o i prezzi. Per ulteriori informazioni, consulta la pagina relativa alle [restrizioni dei servizi AWS IoT](#).

timestamp

Indica quando il messaggio è stato trasmesso da AWS IoT. Usando il timestamp nel messaggio e i timestamp per i singoli attributi nella sezione desired o reported, un oggetto può determinare a quando risale un elemento aggiornato, anche se non dispone di un orologio interno.

clientToken

Stringa univoca del dispositivo che permette di associare le risposte alle richieste in un ambiente MQTT.

version

Versione del documento. Ogni volta che il documento viene aggiornato, questo numero di versione viene incrementato. Questa proprietà viene usata per garantire che la versione del documento che viene aggiornata sia la più recente.

Per ulteriori informazioni, consulta [Sintassi dei documenti del servizio Device Shadow \(p. 364\)](#).

Funzione Versioni multiple per una copia shadow di un dispositivo

Il servizio Device Shadow supporta la funzione Versioni multiple per ogni messaggio di aggiornamento (sia di richiesta che di risposta), il che significa che ogni volta che una copia shadow di un dispositivo viene aggiornata, la versione del documento JSON viene incrementata. Ciò offre due possibilità:

- Un client può ricevere un errore se tenta di sovrascrivere una copia shadow usando un numero di versione precedente. Il client viene informato che è necessaria una nuova sincronizzazione prima dell'aggiornamento di una copia shadow di un dispositivo.
- Un client può decidere di non agire su un messaggio ricevuto se il messaggio ha una versione più bassa rispetto a quella archiviata dal client.

In alcuni casi, un client può bypassare la corrispondenza delle versioni evitando di inviare una versione.

Token client

È possibile usare un token client con la messaggistica basata su MQTT per verificare che lo stesso token client sia incluso in una richiesta e in una risposta a una richiesta. In questo modo la risposta e la richiesta vengono associate.

Note

Il token client non può superare i 64 byte. Un token client di dimensioni superiori a 64 byte causerà una risposta 400 (Richiesta non valida) e un messaggio di errore Token client non valido.

Documento di esempio

Di seguito è illustrato un esempio di documento di una copia shadow:

```
{  
    "state" : {  
        "desired" : {  
            "color" : "RED",  
            "sequence" : [ "RED", "GREEN", "BLUE" ]  
        },  
        "reported" : {  
            "color" : "GREEN"  
        }  
    },  
    "metadata" : {  
        "desired" : {  
            "color" : {  
                "timestamp" : 12345  
            },  
            "sequence" : {  
                "timestamp" : 12345  
            }  
        }  
    }  
}
```

```
},
"reported" : {
    "color" : {
        "timestamp" : 12345
    }
},
"version" : 10,
"clientToken" : "UniqueClientToken",
"+timestamp": 123456789
}
```

Sezioni vuote

Un documento di una copia shadow contiene una sezione `desired` solo se è presente uno stato desiderato. Nell'esempio seguente è illustrato, ad esempio, un documento sullo stato valido senza sezione `desired`:

```
{
    "reported" : { "temp": 55 }
}
```

Anche la sezione `reported` può essere vuota:

```
{
    "desired" : { "color" : "RED" }
}
```

Se a causa di un aggiornamento la sezione `desired` o `reported` diventa null, la sezione viene rimossa dal documento. Per rimuovere la sezione `desired` da un documento (in risposta, ad esempio, a un dispositivo che aggiorna il proprio stato), imposta la sezione `desired` su null:

```
{
    "state": {
        "reported": {
            "color": "red"
        },
        "desired": null
    }
}
```

È anche possibile che un documento di una copia shadow non contenga le sezioni `desired` e `reported`. In questo caso, il documento della copia shadow è vuoto. Di seguito è illustrato, ad esempio, un documento valido:

```
{
}
```

Matrici

Le copie shadow supportano le matrici, ma le trattano come normali valori, pertanto un aggiornamento di una matrice sostituisce l'intera matrice. Non è possibile aggiornare una parte di una matrice.

Stato iniziale:

```
{
    "desired" : { "colors" : [ "RED", "GREEN", "BLUE" ] }
```

```
}
```

Aggiornamento:

```
{
    "desired" : { "colors" : [ "RED" ] }
}
```

Stato finale:

```
{
    "desired" : { "colors" : [ "RED" ] }
}
```

Le matrici non possono contenere valori null. La matrice seguente, ad esempio, non è valida e verrà rifiutata.

```
{
    "desired" : {
        "colors" : [ null, "RED", "GREEN" ]
    }
}
```

Uso delle copie shadow

In AWS IoT, puoi usare una copia shadow di un dispositivo in tre modi:

UPDATE

Crea una copia shadow di un dispositivo, se non esiste, oppure aggiorna il contenuto di una copia shadow di un dispositivo con i dati forniti nella richiesta. I dati vengono archiviati con le informazioni sul timestamp, per indicare quando è avvenuto l'ultimo aggiornamento. I messaggi vengono inviati a tutti i sottoscrittori con la differenza tra stato `desired` e `reported` (delta). Gli oggetti o le app che ricevono un messaggio possono eseguire operazioni in base alla differenza tra gli stati `desired` e `reported`. Un dispositivo, ad esempio, può aggiornare il proprio stato allo stato desiderato oppure un'app può aggiornare la propria interfaccia utente per visualizzare la modifica dello stato del dispositivo.

GET

Recupera lo stato più recente archiviato nella copia shadow del dispositivo (ad esempio, durante l'avvio di un dispositivo per recuperare la configurazione e l'ultimo stato di funzionamento). Questo metodo restituisce l'intero documento JSON, inclusi i metadata.

DELETE

Elimina una copia shadow di un dispositivo, incluso tutto il relativo contenuto. In questo modo, il documento JSON viene rimosso dal datastore. Non puoi ripristinare una copia shadow di un dispositivo eliminata, ma puoi creare una nuova copia shadow con lo stesso nome.

Supporto dei protocolli

Questi metodi sono supportati tramite [MQTT](#) e un'API RESTful tramite HTTPS. Poiché MQTT è un modello di comunicazione di pubblicazione/sottoscrizione, AWS IoT implementa un set di argomenti riservati. Gli oggetti o le applicazioni sottoscrivono questi argomenti prima di pubblicare in un argomento di richiesta, al fine di implementare un comportamento di richiesta–risposta. Per ulteriori informazioni, consulta [Argomenti MQTT del servizio Device Shadow \(p. 357\)](#) e [API RESTful del servizio Device Shadow \(p. 355\)](#).

Aggiornamento di una copia shadow

Puoi aggiornare una copia shadow di un dispositivo usando l'API RESTful [UpdateThingShadow \(p. 356\)](#) o pubblicando nell'argomento [/update \(p. 358\)](#). Gli aggiornamenti interessano solo i campi specificati nella richiesta.

Stato iniziale:

```
{  
    "state": {  
        "reported" : {  
            "color" : { "r" :255, "g": 255, "b": 0 }  
        }  
    }  
}
```

Viene inviato un messaggio di aggiornamento:

```
{  
    "state": {  
        "desired" : {  
            "color" : { "r" : 10 },  
            "engine" : "ON"  
        }  
    }  
}
```

Il dispositivo riceve lo stato `desired` nell'argomento `/update/delta` attivato dal messaggio `/update` precedente e quindi esegue le modifiche desiderate. Al termine, il dispositivo deve confermare lo stato aggiornato attraverso la sezione `reported` nel documento JSON della copia shadow.

Stato finale:

```
{  
    "state": {  
        "reported" : {  
            "color" : { "r" : 10, "g" : 255, "b": 0 },  
            "engine" : "ON"  
        }  
    }  
}
```

Recupero di un documento di una copia shadow

Puoi recuperare una copia shadow di un dispositivo usando l'API RESTful [GetThingShadow \(p. 355\)](#) o sottoscrivendo l'argomento [/get \(p. 361\)](#) e pubblicando al suo interno. In questo modo, vengono recuperati l'intero documento e il relativo delta tra stati `desired` e `reported`.

Documento di esempio:

```
{  
    "state": {  
        "desired": {  
            "lights": {  
                "color": "RED"  
            },  
            "engine": "ON"  
        },  
        "reported": {  
            "lights": {  
                "color": "RED"  
            },  
            "engine": "ON"  
        }  
    }  
}
```

```
        "lights": {
            "color": "GREEN"
        },
        "engine": "ON"
    }
},
"metadata": {
    "desired": {
        "lights": {
            "color": {
                "timestamp": 123456
            },
            "engine": {
                "timestamp": 123456
            }
        }
    },
    "reported": {
        "lights": {
            "color": {
                "timestamp": 789012
            }
        },
        "engine": {
            "timestamp": 789012
        }
    },
    "version": 10,
    "timestamp": 123456789
}
}
```

Risposta:

```
{
    "state": {
        "desired": {
            "lights": {
                "color": "RED"
            },
            "engine": "ON"
        },
        "reported": {
            "lights": {
                "color": "GREEN"
            },
            "engine": "ON"
        },
        "delta": {
            "lights": {
                "color": "RED"
            }
        }
    },
    "metadata": {
        "desired": {
            "lights": {
                "color": {
                    "timestamp": 123456
                }
            },
            "engine": {
                "timestamp": 123456
            }
        }
    }
},
```

```
"reported": {
    "lights": {
        "color": {
            "timestamp": 789012
        }
    },
    "engine": {
        "timestamp": 789012
    }
},
"delta": {
    "lights": {
        "color": {
            "timestamp": 123456
        }
    }
},
"version": 10,
"timestamp": 123456789
}
```

Blocco ottimistico

Puoi usare la versione del documento sullo stato per assicurarti di aggiornare la versione più recente di un documento di una copia shadow di un dispositivo. Quando fornisci una versione con una richiesta di aggiornamento, il servizio rifiuta la richiesta con un codice di risposta di conflitto HTTP 409 se la versione corrente del documento sullo stato non corrisponde alla versione fornita.

Ad esempio:

Documento iniziale:

```
{
    "state" : {
        "desired" : { "colors" : [ "RED", "GREEN", "BLUE" ] }
    },
    "version" : 10
}
```

Aggiornamento: (la versione non corrisponde, la richiesta verrà rifiutata)

```
{
    "state": {
        "desired": {
            "colors": [
                "BLUE"
            ]
        }
    },
    "version": 9
}
```

Risultato:

```
409 Conflict
```

Aggiornamento: (la versione corrisponde, la richiesta verrà accettata)

```
{
```

```
{  
    "state": {  
        "desired": {  
            "colors": [  
                "BLUE"  
            ]  
        }  
    },  
    "version": 10  
}
```

Stato finale:

```
{  
    "state": {  
        "desired": {  
            "colors": [  
                "BLUE"  
            ]  
        }  
    },  
    "version": 11  
}
```

Eliminazione di dati

Puoi eliminare i dati da una copia shadow di un dispositivo pubblicando nell'argomento [/update \(p. 358\)](#) e impostando i campi da eliminare su null. Qualsiasi campo con un valore null viene rimosso dal documento.

Stato iniziale:

```
{  
    "state": {  
        "desired" : {  
            "lights": { "color": "RED" },  
            "engine" : "ON"  
        },  
        "reported" : {  
            "lights" : { "color": "GREEN" },  
            "engine" : "OFF"  
        }  
    }  
}
```

Viene inviato un messaggio di aggiornamento:

```
{  
    "state": {  
        "desired": null,  
        "reported": {  
            "engine": null  
        }  
    }  
}
```

Stato finale:

```
{  
    "state": {  
        "reported" : {
```

```
        "lights" : { "color" : "GREEN" }
    }
}
```

Puoi eliminare tutti i dati da una copia shadow di un dispositivo impostando il relativo stato su `null`. Inviando, ad esempio, il messaggio seguente, vengono eliminati tutti i dati sullo stato, ma la copia shadow del dispositivo viene conservata.

```
{
    "state": null
}
```

La copia shadow del dispositivo rimane disponibile anche se il suo stato è `null`. La versione della copia shadow viene incrementata quando viene eseguito l'aggiornamento successivo.

Eliminazione di una copia shadow

Puoi eliminare un documento di una copia shadow di un dispositivo usando l'API RESTful [DeleteThingShadow \(p. 357\)](#) o pubblicando nell'argomento [/delete \(p. 363\)](#).

Note

Eliminando una copia shadow di un dispositivo non si elimina l'oggetto. Eliminando una copia shadow di un oggetto non si elimina la copia shadow del dispositivo corrispondente.

Stato iniziale:

```
{
    "state": {
        "desired" : {
            "lights": { "color": "RED" },
            "engine" : "ON"
        },
        "reported" : {
            "lights" : { "color": "GREEN" },
            "engine" : "OFF"
        }
    }
}
```

Viene pubblicato un messaggio vuoto nell'argomento `/delete`.

Stato finale:

```
HTTP 404 - resource not found
```

Stato delta

Lo stato delta è un tipo di stato virtuale che contiene la differenza tra gli stati `desired` e `reported`. I campi nella sezione `desired` che non sono presenti nella sezione `reported` sono inclusi nel delta. I campi nella sezione `reported` che non sono presenti nella sezione `desired` non sono inclusi nel delta. Il delta contiene i metadata e i relativi valori corrispondono ai metadata nel campo `desired`. Ad esempio:

```
{
    "state": {
        "desired": {
            "color": "RED",
            "engine": "ON"
        }
    }
}
```

```
        "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
}
}
```

Quando gli oggetti nidificati differiscono, il delta contiene il percorso fino alla root.

```
{
    "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
}
```

Il servizio Device Shadow calcola il delta scorrendo ogni campo con stato `desired` e confrontandolo con lo stato `reported`.

Le matrici vengono trattate come valori. Se una matrice nella sezione `desired` non corrisponde alla matrice nella sezione `reported`, l'intera matrice della sezione `desired` viene copiata nel delta.

Osservazione delle modifiche dello stato

Quando una copia shadow di un dispositivo viene aggiornata, vengono pubblicati i messaggi in due argomenti MQTT:

- `$aws/things/nome-oggetto/shadow/update/accepted`
- `$aws/things/nome-oggetto/shadow/update/delta`

Il messaggio inviato all'argomento `update/delta` è destinato all'oggetto il cui stato viene aggiornato. Questo messaggio contiene solo la differenza tra le sezioni `desired` e `reported` del documento della copia shadow del dispositivo. Quando riceve questo messaggio, il dispositivo deve decidere se apportare la modifica richiesta. Se lo stato del dispositivo cambia, il nuovo stato corrente dovrebbe essere pubblicato nell'argomento `$aws/things/thing-name/shadow/update`.

I dispositivi e le applicazioni possono sottoscrivere questi argomenti per ricevere una notifica quando lo stato del documento cambia.

Di seguito è illustrato un esempio di questo flusso:

1. Un dispositivo segnala il suo stato.
2. Il sistema aggiorna il documento sullo stato nel datastore persistente.
3. Il sistema pubblica un messaggio delta, che contiene solo il delta ed è destinato ai dispositivi che hanno eseguito la sottoscrizione. I dispositivi devono sottoscrivere questo argomento per ricevere gli aggiornamenti.
4. La copia shadow del dispositivo pubblica un messaggio di accettazione, che contiene l'intero documento ricevuto, inclusi i metadata. Le applicazioni devono sottoscrivere questo argomento per ricevere gli aggiornamenti.

Ordine dei messaggi

Non vi è alcuna garanzia che i messaggi del servizio AWS IoT raggiungano il dispositivo in un ordine specifico.

Documento sullo stato iniziale:

```
{
    "state" : {
        "reported" : { "color" : "blue" }
    },
    "version" : 10,
```

```
    "timestamp": 123456777
}
```

Aggiornamento 1:

```
{
  "state": { "desired" : { "color" : "RED" } },
  "version": 10,
  "timestamp": 123456777
}
```

Aggiornamento 2:

```
{
  "state": { "desired" : { "color" : "GREEN" } },
  "version": 11,
  "timestamp": 123456778
}
```

Documento sullo stato finale:

```
{
  "state": {
    "reported": { "color" : "GREEN" }
  },
  "version": 12,
  "timestamp": 123456779
}
```

Il risultato è costituito da due messaggi delta:

```
{
  "state": {
    "color": "RED"
  },
  "version": 11,
  "timestamp": 123456778
}
```

```
{
  "state": { "color" : "GREEN" },
  "version": 12,
  "timestamp": 123456779
}
```

Il dispositivo potrebbe ricevere questi messaggi non in ordine. Poiché lo stato nei messaggi è cumulativo, un dispositivo può scartare senza problemi qualsiasi messaggio contenente un numero di versione precedente a quello monitorato. Se il dispositivo riceve il delta per la versione 12 prima della versione 11, può scartare senza problemi il messaggio con la versione 11.

Taglio dei messaggi delle copie shadow

Per ridurre le dimensioni dei messaggi delle copie shadow inviati al dispositivo, definisci una regola che seleziona solo i campi necessari per il dispositivo, quindi ripubblica il messaggio in un argomento MQTT in cui il dispositivo è in ascolto.

La regola viene specificata in formato JSON e dovrebbe essere simile a quanto segue:

```
{  
    "sql": "SELECT state, version FROM '$aws/things/+/shadow/update/delta'",  
    "ruleDisabled": false,  
    "actions": [  
        {"  
            "republish": {  
                "topic": "${topic(2)}/delta",  
                "roleArn": "arn:aws:iam::123456789012:role/my-iot-role"  
            }  
        }  
    ]  
}
```

L'istruzione SELECT determina i campi del messaggio che verranno ripubblicati nell'argomento specificato. Il carattere jolly "+" permette di trovare la corrispondenza con tutti i nomi delle copie shadow. La regola specifica che tutti i messaggi corrispondenti devono essere ripubblicati nell'argomento specificato. In questo caso, la funzione "topic()" viene usata per specificare l'argomento su cui ripetere la pubblicazione. topic(2) restituisce il nome nell'oggetto nell'argomento originale. Per ulteriori informazioni sulla creazione di regole, consulta la pagina relativa alle [regole](#).

API RESTful del servizio Device Shadow

Un copia shadow espone l'URI seguente per aggiornare le informazioni sullo stato:

```
https://endpoint/things/thingName/shadow
```

L'endpoint è specifico dell'account AWS. Per recuperare l'endpoint, usa il comando [describe-endpoint](#). Il formato dell'endpoint è il seguente:

```
identifier.iot.region.amazonaws.com
```

L'API RESTful della shadow segue le stesse associazioni tra mappe e protocolli HTTPS descritte in [Protocolli AWS IoT](#).

Operazioni dell'API

- [GetThingShadow \(p. 355\)](#)
- [UpdateThingShadow \(p. 356\)](#)
- [DeleteThingShadow \(p. 357\)](#)

Note

Quando utilizzi queste API, assicurati di utilizzare la porta 8443 come descritto in [Associazioni tra protocolli e porte \(p. 239\)](#).

GetThingShadow

Ottiene la copia shadow per l'oggetto specificato.

Il documento sullo stato della risposta include il delta tra gli stati `desired` e `reported`.

Richiesta

La richiesta include le intestazioni HTTP standard più l'URI seguente:

```
HTTP GET https://endpoint/things/thingName/shadow
```

Risposta

In caso di esito positivo, la risposta include le intestazioni HTTP standard più il codice e il corpo seguenti:

```
HTTP 200
BODY: response state document
```

Per ulteriori informazioni, consulta il [documento di esempio sullo stato della risposta \(p. 365\)](#).

Autorizzazione

Per recuperare una copia shadow, è necessaria una policy che permetta all'intermediario di eseguire l'operazione `iot:GetThingShadow`. Il servizio Device Shadow accetta due forme di autenticazione: Signature Version 4 con credenziali IAM o autenticazione reciproca TLS con certificato client.

Di seguito è riportato un esempio di policy che permette a un intermediario di recuperare una copia shadow di un dispositivo:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:GetThingShadow",
      "Resource": ["arn:aws:iot:region:account:thing/thing"]
    }
}
```

UpdateThingShadow

Aggiorna la copia shadow per l'oggetto specificato.

Gli aggiornamenti interessano solo i campi specificati nel documento sullo stato della richiesta. Qualsiasi campo con un valore `null` viene rimosso dalla copia shadow del dispositivo.

Richiesta

La richiesta include le intestazioni HTTP standard più l'URI e il corpo seguenti:

```
HTTP POST https://endpoint/things/thingName/shadow
BODY: request state document
```

Per ulteriori informazioni, consulta il [documento di esempio sullo stato della richiesta \(p. 365\)](#).

Risposta

In caso di esito positivo, la risposta include le intestazioni HTTP standard più il codice e il corpo seguenti:

```
HTTP 200
BODY: response state document
```

Per ulteriori informazioni, consulta il [documento di esempio sullo stato della risposta \(p. 365\)](#).

Autorizzazione

Per aggiornare una copia shadow, è necessaria una policy che permetta all'intermediario di eseguire l'operazione `iot:UpdateThingShadow`. Il servizio Device Shadow accetta due forme di autenticazione: Signature Version 4 con credenziali IAM o autenticazione reciproca TLS con certificato client.

Di seguito è riportato un esempio di policy che permette a un intermediario di aggiornare una copia shadow di un dispositivo:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "iot:UpdateThingShadow",  
            "Resource": ["arn:aws:iot:region:account:thing/thing"]  
        }  
    ]  
}
```

DeleteThingShadow

Elimina la copia shadow per l'oggetto specificato.

Richiesta

La richiesta include le intestazioni HTTP standard più l'URI seguente:

```
HTTP DELETE https://endpoint/things/thingName/shadow
```

Risposta

In caso di esito positivo, la risposta include le intestazioni HTTP standard più il codice e il corpo seguenti:

```
HTTP 200  
BODY: Empty response state document
```

Autorizzazione

Per eliminare una copia shadow di un dispositivo è necessaria una policy che permetta all'intermediario di eseguire l'operazione `iot:DeleteThingShadow`. Il servizio Device Shadow accetta due forme di autenticazione: Signature Version 4 con credenziali IAM o autenticazione reciproca TLS con certificato client.

Di seguito è riportato un esempio di policy che permette a un intermediario di eliminare una copia shadow di un dispositivo:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "iot:DeleteThingShadow",  
            "Resource": ["arn:aws:iot:region:account:thing/thing"]  
        }  
    ]  
}
```

Argomenti MQTT del servizio Device Shadow

Il servizio Device Shadow usa argomenti MQTT riservati per permettere alle applicazioni e ai dispositivi di ottenere, aggiornare o eliminare le informazioni sullo stato per un dispositivo (copia shadow). I nomi di questi argomenti iniziano con `$aws/things/nomeOggetto/shadow`. Per la pubblicazione e la sottoscrizione negli argomenti delle copie shadow è richiesta l'autorizzazione basata su argomento. AWS IoT si riserva il diritto di aggiungere nuovi argomenti alla struttura di argomenti esistente. Per questo motivo, è consigliabile evitare le sottoscrizioni con caratteri jolly degli argomenti delle copie shadow. Evita, ad esempio, di

sottoscrivere filtri di argomenti come `$aws/things/thingName/shadow/#`, perché il numero di argomenti che corrispondono a questo filtro potrebbe aumentare man mano che AWS IoT introduce nuovi argomenti della copia shadow. Per esempi di messaggi pubblicati in questi argomenti, consulta [Flusso di dati del servizio Device Shadow \(p. 335\)](#).

Di seguito sono elencati gli argomenti MQTT usati per l'interazione con le copie shadow.

Argomenti

- [/update \(p. 358\)](#)
- [/update/accepted \(p. 359\)](#)
- [/update/documents \(p. 359\)](#)
- [/update/rejected \(p. 360\)](#)
- [/update/delta \(p. 360\)](#)
- [/get \(p. 361\)](#)
- [/get/accepted \(p. 362\)](#)
- [/get/rejected \(p. 362\)](#)
- [/delete \(p. 363\)](#)
- [/delete/accepted \(p. 363\)](#)
- [/delete/rejected \(p. 364\)](#)

/update

Pubblica un documento sullo stato della richiesta in questo argomento per aggiornare la copia shadow del dispositivo:

```
$aws/things/thingName/shadow/update
```

Un client che tenta di aggiornare lo stato di un oggetto invia un documento sullo stato della richiesta JSON analogo al seguente:

```
{  
    "state" : {  
        "desired" : {  
            "color" : "red",  
            "power" : "on"  
        }  
    }  
}
```

Un dispositivo che aggiorna la propria copia shadow invia un documento sullo stato della richiesta JSON analogo al seguente:

```
{  
    "state" : {  
        "reported" : {  
            "color" : "red",  
            "power" : "on"  
        }  
    }  
}
```

AWS IoT risponde tramite la pubblicazione in [/update/accepted \(p. 359\)](#) o [/update/rejected \(p. 360\)](#).

Per ulteriori informazioni, consulta [Documenti sullo stato della richiesta \(p. 365\)](#).

Policy di esempio

Di seguito è illustrato un esempio della policy necessaria:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": ["iot:Publish"],  
            "Resource": ["arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/  
update"]  
        }]  
}
```

/update/accepted

AWS IoT pubblica un documento sullo stato della risposta in questo argomento quando accetta una modifica per la copia shadow del dispositivo:

```
$aws/things/thingName/shadow/update/accepted
```

Per ulteriori informazioni, consulta [Documenti sullo stato della risposta \(p. 365\)](#).

Policy di esempio

Di seguito è illustrato un esempio della policy necessaria:

```
{  
    "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 pubblica un documento sullo stato in questo argomento ogni volta che un aggiornamento nella copia shadow va a buon fine:

```
$aws/things/thingName/shadow/update/documents
```

Il documento JSON conterrà due nodi principali: `previous` e `current`. Il nodo `previous` include i contenuti del documento della copia shadow completo prima dell'esecuzione dell'aggiornamento, mentre `current` include il documento della copia shadow completo dopo la corretta applicazione dell'aggiornamento. Quando la copia shadow viene aggiornata (creata) per la prima volta, il nodo `previous` contiene `null`.

Policy di esempio

Di seguito è illustrato un esempio della policy necessaria:

```
{  
    "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/accepted"]  
        }  
    ]  
}
```

/update/rejected

AWS IoT pubblica un documento di risposta di errore in questo argomento quando rifiuta una modifica apportata alla copia shadow del dispositivo:

```
$aws/things/thingName/shadow/update/rejected
```

Per ulteriori informazioni, consulta [Documenti di risposta di errore \(p. 366\)](#).

Policy di esempio

Di seguito è illustrato un esempio della policy necessaria:

```
{  
    "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"]  
        }  
    ]  
}
```

/update/delta

AWS IoT pubblica un documento sullo stato della risposta in questo argomento quando accetta una modifica della copia shadow del dispositivo e il documento sullo stato della richiesta contiene valori diversi per gli stati `desired` e `reported`:

```
$aws/things/thingName/shadow/update/delta
```

Per ulteriori informazioni, consulta [Documenti sullo stato della risposta \(p. 365\)](#).

Dettagli relativi alla pubblicazione

- Un messaggio pubblicato in `update/delta` include solo gli attributi desiderati diversi tra le sezioni `desired` e `reported`. Contiene tutti questi attributi, indipendentemente dal fatto che siano inclusi nel messaggio di aggiornamento corrente o siano già archiviati in AWS IoT. Gli attributi che non presentano differenze tra le sezioni `desired` e `reported` non sono inclusi.
- Se un attributo è nella sezione `reported`, ma non ha un equivalente nella sezione `desired`, non viene incluso.
- Se un attributo è nella sezione `desired`, ma non ha un equivalente nella sezione `reported`, viene incluso.
- Se un attributo viene eliminato dalla sezione `reported`, ma è ancora presente nella sezione `desired`, viene incluso.

Policy di esempio

Di seguito è illustrato un esempio della policy necessaria:

```
{  
    "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"]  
        }  
    ]  
}
```

/get

Pubblica un messaggio vuoto in questo argomento per ottenere la copia shadow del dispositivo:

```
$aws/things/thingName/shadow/get
```

AWS IoT risponde tramite la pubblicazione in [/get/accepted \(p. 362\)](#) o [/get/rejected \(p. 362\)](#).

Policy di esempio

Di seguito è illustrato un esempio della policy necessaria:

```
{  
    "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 pubblica un documento sullo stato della risposta in questo argomento quando restituisce la copia shadow del dispositivo:

```
$aws/things/thingName/shadow/get/accepted
```

Per ulteriori informazioni, consulta [Documenti sullo stato della risposta \(p. 365\)](#).

Policy di esempio

Di seguito è illustrato un esempio della policy necessaria:

```
{  
    "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" ]  
        }  
    ]  
}
```

/get/rejected

AWS IoT pubblica un documento di risposta di errore in questo argomento quando non può restituire la copia shadow del dispositivo:

```
$aws/things/thingName/shadow/get/rejected
```

Per ulteriori informazioni, consulta [Documenti di risposta di errore \(p. 366\)](#).

Policy di esempio

Di seguito è illustrato un esempio della policy necessaria:

```
{  
    "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: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"]
    }
}
```

/delete

Per eliminare una copia shadow di un dispositivo, pubblica un messaggio vuoto nell'argomento delete:

```
$aws/things/thingName/shadow/delete
```

Il contenuto del messaggio viene ignorato.

AWS IoT risponde tramite la pubblicazione in [/delete/accepted \(p. 363\)](#) o [/delete/rejected \(p. 364\)](#).

Policy di esempio

Di seguito è illustrato un esempio della policy necessaria:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["iot:Subscribe"],
            "Resource": ["arn:aws:iot:region:account:topicfilter/$aws/things/thingName/shadow/delete"]
        },
        {
            "Effect": "Allow",
            "Action": ["iot:Receive"],
            "Resource": ["arn:aws:iot:region:account:topic/$aws/things/thingName/shadow/delete"]
        }
    ]
}
```

/delete/accepted

AWS IoT pubblica un messaggio in questo argomento quando una copia shadow di un dispositivo viene eliminata:

```
$aws/things/thingName/shadow/delete/accepted
```

Policy di esempio

Di seguito è illustrato un esempio della policy necessaria:

```
{
    "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 pubblica un documento di risposta di errore in questo argomento quando non può eliminare la copia shadow del dispositivo:

```
$aws/things/thingName/shadow/delete/rejected
```

Per ulteriori informazioni, consulta [Documenti di risposta di errore \(p. 366\)](#).

Policy di esempio

Di seguito è illustrato un esempio della policy necessaria:

```
{
  "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"]
    }
  ]
}
```

Sintassi dei documenti del servizio Device Shadow

Il servizio Device Shadow usa i documenti seguenti nelle operazioni UPDATE, GET e DELETE con l'[API RESTful \(p. 355\)](#) o i [messaggi di pubblicazione/sottoscrizione MQTT \(p. 357\)](#). Per ulteriori informazioni, consulta [Documenti del servizio Device Shadow \(p. 343\)](#).

Esempi

- [Documenti sullo stato della richiesta \(p. 365\)](#)
- [Documenti sullo stato della risposta \(p. 365\)](#)

- Documenti di risposta di errore (p. 366)

Documenti sullo stato della richiesta

I documenti sullo stato della richiesta hanno il formato seguente:

```
{  
    "state": {  
        "desired": {  
            "attribute1": integer2,  
            "attribute2": "string2",  
            ...  
            "attributeN": boolean2  
        },  
        "reported": {  
            "attribute1": integer1,  
            "attribute2": "string1",  
            ...  
            "attributeN": boolean1  
        }  
    },  
    "clientToken": "token",  
    "version": version  
}
```

- **state** — Gli aggiornamenti interessano solo i campi specificati.
- **clientToken** — Se usato, permette di verificare che la richiesta e la risposta contengano lo stesso token client.
- **version** — Se usato, il servizio Device Shadow elabora l'aggiornamento solo se la versione specificata corrisponde alla versione più recente.

Documenti sullo stato della risposta

I documenti sullo stato della risposta hanno il formato seguente:

```
{  
    "state": {  
        "desired": {  
            "attribute1": integer2,  
            "attribute2": "string2",  
            ...  
            "attributeN": boolean2  
        },  
        "reported": {  
            "attribute1": integer1,  
            "attribute2": "string1",  
            ...  
            "attributeN": boolean1  
        },  
        "delta": {  
            "attribute3": integerX,  
            "attribute5": "stringY"  
        }  
    },  
    "metadata": {  
        "desired": {  
            "attribute1": {  
                "timestamp": timestamp  
            }  
        }  
    }  
}
```

```
        },
        "attribute2": {
            "timestamp": timestamp
        },
        ...
        "attributeN": {
            "timestamp": timestamp
        }
    },
    "reported": {
        "attribute1": {
            "timestamp": timestamp
        },
        "attribute2": {
            "timestamp": timestamp
        },
        ...
        "attributeN": {
            "timestamp": timestamp
        }
    }
},
"timestamp": timestamp,
"clientToken": "token",
"version": version
}
```

- **state**
 - **reported** — Presente solo se un oggetto ha segnalato dati nella sezione `reported` e contiene solo campi che erano presenti nel documento sullo stato della richiesta.
 - **desired** — Presente solo se un oggetto ha segnalato dati nella sezione `desired` e contiene solo campi che erano presenti nel documento sullo stato della richiesta.
- **metadata** — Contiene i timestamp per ogni attributo nelle sezioni `desired` e `reported`, per consentire di determinare quando lo stato è stato aggiornato.
- **timestamp** — Data e ora rispetto all'epoca (Unix epoch) in cui la risposta è stata generata da AWS IoT.
- **clientToken** — Presente solo se è stato usato un token client durante la pubblicazione di un contenuto JSON valido nell'argomento `/update`.
- **version** — Versione corrente del documento della copia shadow del dispositivo condivisa in AWS IoT. Il valore viene aumentato di uno rispetto alla versione precedente del documento.

Documenti di risposta di errore

I documenti di risposta di errore hanno il formato seguente:

```
{
    "code": error-code,
    "message": "error-message",
    "timestamp": timestamp,
    "clientToken": "token"
}
```

- **code** — Codice di risposta HTTP che indica il tipo di errore.
- **message** — Messaggio di testo che fornisce ulteriori informazioni.
- **timestamp** — Data e ora in cui la risposta è stata generata da AWS IoT.
- **clientToken** — Presente solo se è stato usato un token client durante la pubblicazione di un contenuto JSON valido nell'argomento `/update`.

Per ulteriori informazioni, consulta [Messaggi di errore del servizio Shadow \(p. 367\)](#).

Messaggi di errore del servizio Shadow

Il servizio Device Shadow pubblica un messaggio di errore nell'argomento di errore (tramite MQTT) quando un tentativo di modificare il documento sullo stato ha esito negativo. Questo messaggio viene inviato solo in risposta a una richiesta di pubblicazione in uno degli argomenti \$aws riservati. Se il client aggiorna il documento usando l'API REST, riceve il codice di errore HTTP come parte della risposta e non viene inviato alcun messaggio di errore MQTT.

| Codice di errore HTTP | Descrizione dell'errore |
|---------------------------------------|--|
| 400 (Richiesta non valida) | <ul style="list-style-type: none">• JSON non valido• Nodo richiesto mancante: stato• Il nodo di stato deve essere un oggetto• Il nodo desiderato deve essere un oggetto• Il nodo segnalato deve essere un oggetto• Versione non valida• Token client non valido <p>Note</p> <p>Un token client di dimensioni superiori a 64 byte genererà questo tipo di risposta.</p> <ul style="list-style-type: none">• JSON contiene troppi livelli di nidificazione; il numero massimo è 6• Lo stato contiene un nodo non valido |
| 401 (Non autorizzato) | <ul style="list-style-type: none">• Non autorizzato |
| 403 (Accesso negato) | <ul style="list-style-type: none">• Accesso negato |
| 404 (Non trovato) | <ul style="list-style-type: none">• Oggetto non trovato |
| 409 (Conflitto) | <ul style="list-style-type: none">• Conflitto di versioni |
| 413 (Payload troppo grande) | <ul style="list-style-type: none">• Il payload supera le dimensioni massime permesse |
| 415 (Tipo di supporto non supportato) | <ul style="list-style-type: none">• Codifica non supportata; la codifica supportata è UTF-8 |
| 429 (Troppe richieste) | <ul style="list-style-type: none">• Il servizio Device Shadow genera questo messaggio di errore quando ci sono più di 10 richieste in transito. |
| 500 (Errore interno del server) | <ul style="list-style-type: none">• Errore interno del servizio |

Processi

AWS IoT Jobs può essere utilizzato per definire un set di operazioni remote inviate a ed eseguite in uno o più dispositivi connessi a AWS IoT.

Concetti chiave di Jobs

job

Un processo è un'operazione remota che viene inviata a uno o più dispositivi connessi a AWS IoT ed eseguita su di essi. Puoi ad esempio definire un processo che indichi a un set di dispositivi di scaricare e installare aggiornamenti per le applicazioni o il firmware, eseguire il riavvio, ruotare i certificati o eseguire operazioni di risoluzione dei problemi in remoto.

documento del processo

Per creare un processo, devi prima creare un documento del processo che sia una descrizione delle operazioni remote che i dispositivi dovranno eseguire.

I documenti dei processi sono documenti JSON con codifica UTF-8 e devono contenere qualsiasi informazione necessaria ai dispositivi per eseguire un processo. Un documento di un processo contiene probabilmente uno o più URL da cui il dispositivo può scaricare un aggiornamento o altri dati. Il documento del processo può essere archiviato in un bucket Amazon S3 oppure essere incluso inline con il comando che crea il processo.

target

Quando crei un processo, devi specificare un elenco di target che sono i dispositivi che devono eseguire le operazioni. I target possono essere oggetti, [gruppi di oggetti \(p. 163\)](#) o entrambi. AWS IoT Jobs invia un messaggio a ogni target per informarlo che è disponibile un processo.

esecuzione del processo

L'esecuzione di un processo è un'istanza di un processo su un dispositivo target. Il target avvia l'esecuzione di un processo scaricando il documento del processo. Quindi esegue le operazioni specificate dal documento e ne segnala lo stato di avanzamento a AWS IoT. Un numero di esecuzione è un identificatore univoco dell'esecuzione di un processo specifico su un determinato target. Il servizio Jobs fornisce i comandi per monitorare lo stato di avanzamento dell'esecuzione di un processo in un target specifico e l'avanzamento generale in tutti i target del processo.

processo snapshot

Per impostazione predefinita, un processo viene inviato a tutti i target specificati al momento della creazione del processo. Dopo che i target completano il processo (o segnalano l'impossibilità di farlo), il processo è completato.

processo continuo

Un processo continuo viene inviato a tutti i target specificati al momento della creazione del processo, ma rimane in esecuzione e viene inviato a tutti i dispositivi (cose) che vengono aggiunti al gruppo target. Ad esempio, un processo continuo può essere usato per l'onboarding o l'aggiornamento dei dispositivi quando vengono aggiunti a un gruppo. Puoi rendere un processo continuo impostando un parametro opzionale quando crei il processo.

rollout

Puoi specificare con che velocità vengono inviate ai target le notifiche relative all'esecuzione di un processo in sospeso. In questo modo, è possibile creare un'implementazione per fasi, per gestire meglio aggiornamenti, riavvii e altre operazioni.

Il campo seguente può essere aggiunto alla richiesta `CreateJob` per specificare il numero massimo di target che riceveranno informazioni sul processo ogni minuto. Questo esempio imposta una velocità di rollout statica.

```
"jobExecutionRolloutConfig": {  
    "maximumPerMinute": "integer"  
}
```

Puoi anche impostare una velocità di rollout variabile con il campo `exponentialRate`. L'esempio seguente crea un rollout che ha una velocità esponenziale.

```
"jobExecutionsRolloutConfig": {  
    "exponentialRate": {  
        "baseRatePerMinute": integer,  
        "incrementFactor": integer,  
        "rateIncreaseCriteria": {  
            "numberOfNotifiedThings": integer, // Set one or the other  
            "numberOfSucceededThings": integer // of these two values.  
        },  
        "maximumPerMinute": integer  
    }  
}
```

Per ulteriori informazioni sulla configurazione dei rollout di processo, consulta la sezione relativa a [configurazione dei rollout e delle interruzioni di processo](#).

abort

È possibile creare una serie di condizioni per interrompere i rollout una volta soddisfatti determinati criteri specificati dall'utente. Per ulteriori informazioni sulla configurazione delle condizioni per l'interruzione dei rollout di processo, consulta la sezione relativa a [configurazione dei rollout e delle interruzioni di processo](#).

URL prefirmati

Per permettere a un dispositivo l'accesso sicuro e limitato nel tempo ai dati al di là di quelli inclusi nel documento del processo, puoi usare URL Amazon S3 prefirmati. Puoi inserire i dati in un bucket Amazon S3 e aggiungere un collegamento segnaposto ai dati nel documento del processo. Quando il servizio Jobs riceve una richiesta per il documento del processo, analizza il documento cercando i collegamenti segnaposto e li sostituisce con URL Amazon S3 prefirmati.

Il collegamento segnaposto ha il formato seguente:

```
`${aws:iot:s3-presigned-url:https://s3.amazonaws.com/bucket/key`}
```

dove `bucket` è il nome del bucket e `key` è l'oggetto nel bucket a cui rimanda il collegamento.

timeout

Note

La caratteristica di timeout del processo non è attualmente disponibile nella regione PDT (us-gov-west-1).

I timeout del processo ti consentono di ricevere notifiche ogni volta che l'esecuzione di un processo si blocca nello stato `IN_PROGRESS` per un periodo di tempo inaspettatamente lungo. Sono disponibili due tipi di timer: in corso e della fase.

Quando crei un processo, puoi impostare un valore per la proprietà `inProgressTimeoutInMinutes` dell'oggetto `TimeoutConfig` opzionale. Il timer in corso non può essere aggiornato e verrà applicato a tutte le esecuzioni del processo. Se l'esecuzione del processo resta nello stato `IN_PROGRESS` per un periodo di tempo superiore a quello consentito dall'intervallo, l'esecuzione del processo non andrà a buon fine e verrà impostato lo stato `TIMED_OUT` terminale. Inoltre, AWS IoT pubblicherà una notifica MQTT.

Puoi anche impostare un timer della fase per l'esecuzione di un processo specifico impostando un valore per `stepTimeoutInMinutes` quando richiami `UpdateJobExecution`. Il timer della fase si applica solo all'esecuzione del processo in fase di aggiornamento e puoi impostare un nuovo valore per questo timer ogni volta che aggiorni l'esecuzione di un processo. Puoi anche creare un timer della fase quando richiami `StartNextPendingJobExecution`. Se l'esecuzione del processo resta nello stato `IN_PROGRESS` per un periodo di tempo superiore a quello consentito dall'intervallo del timer della fase, l'esecuzione del processo non andrà a buon fine e verrà impostato lo stato `TIMED_OUT` terminale. Il timer della fase non ha alcun effetto su quello in corso impostato al momento della creazione di un processo.

Il seguente schema con le descrizioni mostra le varie interazioni fra i timeout in corso e quelli della fase.

Creazione del processo: `CreateJob` imposta un timer in corso che scade venti minuti dopo. Questo timer si applica a tutte le esecuzioni dei processi e non può essere aggiornato.

12.00: l'esecuzione del processo ha inizio e passa allo stato `IN_PROGRESS`. Il timer in corso inizia il conto alla rovescia.

12.05: `UpdateJobExecution` crea un timer della fase con un valore di 7 minuti. Se non viene creato un nuovo timer della fase, il timeout dell'esecuzione del processo avverrà alle 12.12.

12.10: `UpdateJobExecution` crea un nuovo timer della fase con un valore di 5 minuti. Il timer della fase precedente viene eliminato. Se non viene creato un nuovo timer della fase, il timeout dell'esecuzione del processo avverrà alle 12.15.

12.13: `UpdateJobExecution` crea un nuovo timer della fase con un valore di 9 minuti. Il timeout dell'esecuzione del processo si verifica alle 12.20 perché il timer in corso scade alle 12.20. Il timer della fase non può superare il limite assoluto creato dal timer in corso.

`UpdateJobExecution` può anche eliminare un timer della fase già esistente creandone uno nuovo con un valore di -1.

Gestione dei processi

È possibile utilizzare la [console AWS IoT](#), l'API HTTPS dei processi, l'AWS Command Line Interface oppure gli SDK AWS per creare e gestire i processi. Per ulteriori informazioni, consulta [API di gestione e controllo dei processi \(p. 394\)](#), [Riferimento ai comandi AWS CLI: iot](#) o [SDK e strumenti AWS](#).

Lo scopo principale dei processi è quello di inviare notifica ai dispositivi riguardo un aggiornamento del software o del firmware. Durante l'invio di codice ai dispositivi, la best practice è accedere al file del codice. Ciò consente ai dispositivi di stabilire se il codice è stato modificato durante il transito. Le istruzioni nella sezione seguente vengono scritte supponendo che si desidera firmare con codice l'aggiornamento del software che si sta inviando ai dispositivi.

Per ulteriori informazioni sulla firma del codice, consulta la sezione che spiega [cos'è la firma del codice per AWS IoT](#).

Prima di creare un processo, è necessario creare un documento del processo. Se si utilizza la firma del codice per AWS IoT, è necessario caricare il documento del processo su una versione di un bucket

Amazon S3. Per ulteriori informazioni su come creare un bucket Amazon S3 e su come caricare i file in esso, consulta [Nozioni di base su Amazon Simple Storage Service](#) nella Guida alle operazioni di base di Amazon S3.

Il documento di processo può contenere un URL Amazon S3 prefirmato che punta al file di codice (o ad altri file). Gli URL Amazon S3 prefirmati sono validi per un periodo di tempo limitato e quindi non sono generati fino a quando un dispositivo non richiede un documento di processo. Poiché l'URL preformato non è stato creato durante la creazione del documento di processo, è necessario inserire un URL segnaposto nel documento di processo. Un URL segnaposto ha un formato simile al seguente: \${aws:iot:s3-presigned-url:https://s3.region.amazonaws.com/<bucket>/<code file>} dove **bucket** è il bucket Amazon S3 che contiene il file del codice e il **file del codice** è la chiave Amazon S3 del file del codice.

Quando un dispositivo richiede il documento di processo, AWS IoT genera l'URL prefirmato e sostituisce l'URL del placeholder con l'URL prefirmato. Il documento di processo viene quindi inviato al dispositivo.

Quando crei un processo che utilizza gli URL Amazon S3 prefirmati, devi fornire un ruolo IAM che conceda l'autorizzazione per il download di file dal bucket Amazon S3 in cui sono archiviati i dati o gli aggiornamenti. Il ruolo deve anche concedere ad AWS IoT l'autorizzazione per assumere il ruolo.

È possibile specificare un timeout opzionale per l'URL prefirmato. Per ulteriori informazioni, consulta [CreateJob \(p. 409\)](#).

Per concedere ai processi l'autorizzazione ad assumere il ruolo

1. Accedi alla Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, selezionare Roles (Ruoli).
3. Cercare il ruolo e selezionarlo.
4. Selezionare la scheda Trust Relationships (Relazioni di trust) e quindi scegliere Edit Trust Relationship (Modifica relazione di trust).
5. Nella pagina Edit Trust Relationship (Modifica relazione di trust) sostituire il documento della policy con il codice JSON seguente:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": [  
                    "iot.amazonaws.com"  
                ]  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

6. Scegliere Update Trust Policy (Aggiorna policy di trust).
7. Se il processo utilizza un documento del processo che è un oggetto Amazon S3, scegliere Permissions (Autorizzazioni) e, con il JSON seguente, aggiungere una policy per la concessione dell'autorizzazione a scaricare file dal bucket Amazon S3:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": "s3:GetObject",  
            "Resource": "arn:aws:s3:::<bucket>/*",  
            "Principal": "iot.amazonaws.com"  
        }  
    ]  
}
```

```
{  
    "Effect": "Allow",  
    "Action": "s3:GetObject",  
    "Resource": "arn:aws:s3:::your_S3_bucket/*"  
}  
]  
}
```

Creazione e gestione di processi (Console)

Se si sta usando la firma di codice per AWS IoT, è necessario aggiungere due URL segnaposto nel documento di processo:

Un segnaposto per il file del codice avrà il formato simile al seguente: \${aws:iot:s3-presigned-url:https://s3.amazonaws.com/<my-s3-bucket>/<my-code-file>}.

Note

Al momento, non sono supportate le versioni per i segnaposto URL prefirmati per i processi. Se si aggiorna il file del codice e si copia nella stessa posizione Amazon S3, è necessario creare una nuova firma e quindi fare riferimento alla nuova versione di firma nel documento di processo.

Un segnaposto per la firma avrà il formato simile al seguente: \${aws:iot:code-signature:s3://<region>.<my-s3-bucket>/<my-code-file>@<code-file-version-id>}.

Per creare un processo

1. Passare alla [console AWS IoT](#).
2. Nel riquadro di navigazione, scegliere Manage (Gestisci), quindi Jobs (Processi).
3. Scegli Create a job (Crea un processo).
4. Scegliere Create a custom job (Crea un processo personalizzato).
5. Immettere un ID alfanumerico per il processo e una descrizione facoltativa.

Note

Non è consigliabile utilizzare informazioni di identificazione personale negli ID processo o descrizioni.

6. Selezionare il dispositivo o i gruppi di dispositivi che si desidera aggiornare.
7. In Add a job file (Aggiungi un file di processo), scegliere Select (Seleziona), quindi selezionare il documento di processo.
8. Selezionare Sign image for me (Firma immagine per me). Se non si aggiorna la firma del codice, è possibile ignorare questo passaggio.
9. Creare o selezionare un profilo per la firma del codice. Se non si aggiorna la firma del codice, è possibile ignorare questo passaggio.
10. In Pre-sign resource URLs (URL risorsa prefirmati), scegliere I want to pre-sign my URLs and have configured my job file (Desidero prefirmare gli URL e configurare il file di processo). Se non si aggiorna la firma del codice, è possibile ignorare questo passaggio.
11. Selezionare un ruolo e un'ora di scadenza per l'URL prefirmato.
12. In Job type (Tipo processo), scegliere l'opzione appropriata per l'aggiornamento, quindi scegliere Next (Avanti).
13. Specificare i valori per tutte le configurazioni avanzate e quindi scegliere Create (Crea).

Dopo aver creato il processo, la console genera una firma JSON e la inserisce nel documento di processo.

Puoi utilizzare la [console AWS IoT](#) per visualizzare lo stato di un processo, annullare o eliminare il processo.

1. Passare alla [console AWS IoT](#).
2. Nel riquadro di navigazione, scegliere Manage (Gestisci), quindi Jobs (Processi).

Creazione e gestione di processi (CLI)

Questa sezione illustra come creare e gestire i processi.

Creazione di processi

Utilizza il comando `CreateJob` per creare un processo AWS IoT. Il processo viene accodato per l'esecuzione nei target (oggetti o gruppi di oggetti) specificati. Per creare un processo AWS IoT, devi disporre di un documento di processo che può essere incluso nel corpo della richiesta oppure inserito come collegamento a un documento Amazon S3. Se il processo include il download di file utilizzando gli URL Amazon S3 prefissati, è necessario un ARN del ruolo IAM che disponga dell'autorizzazione per il download del file e conceda a AWS IoT l'autorizzazione ad assumere il ruolo.

Firma del codice con i processi

In caso di utilizzo della firma del codice per AWS IoT, è necessario avviare un processo di firma del codice e includere l'output nel documento di processo. Utilizzare il comando `start-signing-job` per creare un processo di firma del codice. `start-signing-job` restituisce un ID processo. Utilizzare il comando `describe-signing-job` per ottenere la posizione di Amazon S3 in cui è archiviata la firma. È possibile eseguire il download della firma da Amazon S3. Per ulteriori informazioni sui processi di firma del codice, consulta [Firma del codice per AWS IoT](#).

Il documento di processo deve contenere un segnaposto URL prefissato per il file del codice e l'output di firma JSON in un bucket Amazon S3 utilizzando il comando `start-signing-job`, racchiuso in un elemento `codesign`:

```
{  
    "presign": "${aws:iot:s3-presigned-url:https://s3.region.amazonaws.com/bucket/image}",  
    "codesign": {  
        "rawPayloadSize": <image-file-size>,  
        "signature": <signature>,  
        "signatureAlgorithm": <signature-algorithm>,  
        "payloadLocation": {  
            "s3": {  
                "bucketName": <my-s3-bucket>,  
                "key": <my-code-file>,  
                "version": <code-file-version-id>  
            }  
        }  
    }  
}
```

Creazione di un processo con un documento di processo

Il comando seguente mostra come creare un processo utilizzando un documento di processo (`job-document.json`) archiviato in un bucket Amazon S3 (`jobBucket`) e un ruolo con l'autorizzazione al download dei file da Amazon S3 (`S3DownloadRole`).

```
aws iot create-job \  
  --job-id 010 \  
  --targets arn:aws:iot:us-east-1:123456789012:thing/thingOne \  
  --document-source https://s3.amazonaws.com/my-s3-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}"
```

Il processo viene eseguito su [thingOne](#).

Il parametro `timeout-config` opzionale specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione del processo. Il timer viene avviato quando imposti lo stato di esecuzione del processo su `IN_PROGRESS`. Se lo stato di esecuzione del processo non è impostato su un altro stato terminale prima della scadenza del tempo a disposizione, verrà automaticamente impostato su `TIMED_OUT`.

Note

La caratteristica di timeout del processo non è attualmente disponibile nella regione PDT (us-gov-west-1).

Il timer in corso non può essere aggiornato e viene applicato a tutte le esecuzioni del processo. Se l'esecuzione del processo resta nello stato `IN_PROGRESS` per un periodo di tempo superiore a quello consentito dall'intervallo, l'esecuzione del processo non va a buon fine e viene impostato lo stato `TIMED_OUT` terminale. Inoltre, AWS IoT pubblica una notifica MQTT.

Per ulteriori informazioni sulla creazione delle configurazioni dei rollout e delle interruzioni di processo, consulta la sezione relativa a [configurazione dei rollout e delle interruzioni di processo](#).

Note

I documenti dei processi specificati come file Amazon S3 vengono recuperati al momento della creazione del processo. Se modifichi i contenuti del file Amazon S3 usato come origine del documento del processo dopo la creazione del processo, ciò che viene inviato ai target del processo non cambia.

Aggiornamento di un processo

Utilizza il comando `UpdateJob` per aggiornare un processo. È possibile aggiornare i campi `description`, `presignedUrlConfig`, `jobExecutionsRolloutConfig`, `abortConfig` e `timeoutConfig` di un processo.

```
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}"
```

Per ulteriori informazioni sulla configurazione dei rollout e delle interruzioni di processo, consulta la sezione relativa a [configurazione dei rollout e delle interruzioni di processo](#).

Annullamento di un processo

Utilizza il comando `CancelJob` per annullare un processo. L'annullamento di un processo interrompe il rollout delle nuove esecuzioni di processo da parte di AWS IoT. Inoltre, annulla le esecuzioni dei processi con uno stato `QUEUED`. AWS IoT lascia qualsiasi esecuzione di processo in uno stato terminale invariato perché il dispositivo ha già completato il processo. Se lo stato di esecuzione di un processo è `IN_PROGRESS`, non verrà modificato, a meno che non si utilizzi il parametro opzionale `--force`.

Il comando seguente mostra come annullare un processo con ID 010.

```
aws iot cancel-job --job-id 010
```

Il comando visualizza il seguente output:

```
{  
    "jobArn": "string",  
    "jobId": "string",  
    "description": "string"  
}
```

Quando si annulla un processo, le esecuzioni con stato `QUEUED` vengono annullate. Le esecuzioni del processo con stato `IN_PROGRESS` saranno annullate se si specifica il parametro opzionale `--force`. Le esecuzioni del processo con stato terminale non vengono annullate.

Warning

L'annullamento di un processo con stato `IN_PROGRESS` (impostando il parametro `--force`) annulla tutte le esecuzioni dei processi in corso e impedisce al dispositivo che esegue il processo di aggiornarne lo stato di esecuzione. Prestare attenzione e verificare che tutti i dispositivi in cui è in esecuzione un processo annullato siano in grado di effettuare il ripristino a uno stato valido.

Lo stato di un processo annullato o di una delle sue esecuzioni è di tipo consistente finale. AWS IoT interrompe la pianificazione di nuove esecuzioni del processo e delle esecuzioni del processo con stato `QUEUED` il prima possibile. La modifica dello stato dell'esecuzione di un processo in `CANCELED` potrebbe tuttavia richiedere un po' di tempo, a seconda del numero di dispositivi e di altri fattori.

Se un processo viene annullato perché soddisfa i criteri definiti da un oggetto `AbortConfig`, il servizio aggiunge valori popolati automaticamente per i campi `reasonCode` e `comment`. I clienti possono creare i propri valori per `reasonCode` quando l'annullamento del processo è basato sull'utente.

Annullamento dell'esecuzione di un processo

Puoi usare il comando `CancelJobExecution` per annullare l'esecuzione di un processo su un dispositivo. Questo comando annulla un processo che si trova in uno stato `QUEUED`. Per annullare l'esecuzione di un processo in corso, è necessario utilizzare il parametro `--force`.

Il comando seguente mostra come annullare l'esecuzione del processo 010 su `myThing`.

```
aws iot cancel-job-execution --job-id 010 --thing-name myThing
```

Il comando non visualizza alcun output.

Annulla l'esecuzione di un processo che si trova in uno stato `QUEUED`. L'esecuzione di un processo con stato `IN_PROGRESS` viene annullata se si specifica il parametro opzionale `--force`. Le esecuzioni del processo con stato terminale non possono essere annullate.

Warning

Quando si annulla l'esecuzione di un processo con uno stato `IN_PROGRESS`, il dispositivo non è in grado di aggiornarne lo stato di esecuzione del processo. Prestare attenzione e verificare che il dispositivo sia in grado di effettuare il ripristino a uno stato valido.

Se l'esecuzione del processo è in uno stato terminale oppure se è nello stato `IN_PROGRESS` e il parametro `--force` non è impostato su `true`, questo comando genera un'eccezione `InvalidStateTransitionException`.

Lo stato dell'esecuzione di un processo annullato è consistente finale. La modifica dello stato dell'esecuzione di un processo in `CANCELED` potrebbe tuttavia richiedere un po' di tempo, a seconda di vari fattori.

Eliminare un processo

Puoi usare il comando `DeleteJob` per eliminare un processo e le relative esecuzioni. Per impostazione predefinita, è possibile eliminare solo un processo in stato terminale (`SUCCEEDED` o `CANCELED`). In caso contrario, viene generata un'eccezione. È possibile eliminare un processo nello stato `IN_PROGRESS` se il parametro `force` è impostato su `true`.

Per eliminare un processo, eseguire il seguente comando:

```
aws iot delete-job --job-id 010 --force|--no-force
```

Il comando non visualizza alcun output.

Warning

Quando si elimina un processo con uno stato `IN_PROGRESS`, il dispositivo che sta eseguendo il processo non è in grado di accedere alle informazioni sul processo o di aggiornare lo stato di esecuzione del processo. Prestare attenzione e verificare che tutti i dispositivi in cui è in esecuzione un processo annullato siano in grado di effettuare il ripristino a uno stato valido.

L'eliminazione di un processo potrebbe richiedere del tempo, a seconda del numero di esecuzioni create per il processo e di altri fattori. Mentre il processo viene eliminato, il suo stato viene indicato come `DELETION_IN_PROGRESS`. Il tentativo di eliminare o annullare un processo il cui stato è già `DELETION_IN_PROGRESS` restituisce un errore.

Solo 10 processi possono essere nello stato `DELETION_IN_PROGRESS` nello stesso momento. In caso contrario, si verifica un'eccezione `LimitExceededException`.

Recupero di un documento del processo

Utilizza il comando `GetJobDocument` per recuperare un documento per un processo. Un documento del processo è una descrizione delle operazioni remote che i dispositivi dovranno eseguire.

Esegui il comando seguente per ottenere un documento di processo:

```
aws iot get-job-document --job-id 010
```

Il comando restituisce il documento per il processo specificato:

```
{
    "document": "{\n\t\"operation\":\"install\", \n\t"url\":\"http://amazon.com/\nfirmWareUpdate-01\", \n\t"data\":\"\${aws:iot:s3-presigned-url:https://s3.amazonaws.com/job-\ntest-bucket/datafile}\n\""
}
```

Note

Quando utilizzi questo comando per recuperare un documento di processo, gli URL segnaposto non vengono sostituiti dagli URL Amazon S3 prefirmati. Quando un dispositivo chiama l'API MQTT [GetPendingJobExecutions \(p. 457\)](#), gli URL segnaposto vengono sostituiti da URL Amazon S3 prefirmati nel documento di processo.

Visualizzazione di un elenco dei processi

Usa il comando `ListJobs` per ottenere un elenco di tutti i processi nell'account AWS. I dati del processo e della relativa esecuzione vengono eliminati dopo 90 giorni. Per elencare tutti i processi dell'account AWS, esegui il comando seguente.

```
aws iot list-jobs
```

Il comando restituisce tutti i processi nell'account ordinati in base allo stato:

```
{
  "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"
    }
  ]
}
```

Descrizione di un processo

Esegui il comando `DescribeJob` per ottenere lo stato di un processo specifico. Il comando seguente mostra come descrivere un processo:

```
$ aws iot describe-job --job-id 010
```

Il comando restituisce lo stato del processo specificato. Ad esempio:

```
{
  "documentSource": "https://s3.amazonaws.com/job-test-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
    }
}
}

```

Visualizzazione di un elenco delle esecuzioni per un processo

Un processo in esecuzione in un determinato dispositivo è rappresentato da un oggetto esecuzione del processo. Esegui il comando `ListJobExecutionsForJob` per elencare tutte le esecuzioni per un processo. Segue una descrizione di come visualizzare l'elenco delle esecuzioni per un processo:

```
aws iot list-job-executions-for-job --job-id 010
```

Il comando restituisce un elenco delle esecuzioni del processo:

```
{  
    "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  
            }  
        }  
    ]  
}
```

Visualizzazione di un elenco delle esecuzioni di un processo per un oggetto

Esegui il comando `ListJobExecutionsForThing` per elencare tutte le esecuzioni di processo in corso su un oggetto. Segue una descrizione di come visualizzare l'elenco delle esecuzioni di processo per un oggetto:

```
aws iot list-job-executions-for-thing --thing-name thingOne
```

Il comando restituisce un elenco delle esecuzioni del processo in corso o che sono avvenute nell'oggetto specificato:

```
{  
    "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",  
                "lastUpdatedAt": 1486685870.729  
            },  
            "jobId": "011"  
        }  
    ]  
}
```

```
        "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"
}
]
```

Descrizione dell'esecuzione di un processo

Esegui il comando `DescribeJobExecution` per ottenere lo stato dell'esecuzione di un processo. Per identificare l'esecuzione del processo, devi specificare un ID processo, un nome di oggetto e, facoltativamente, un numero di esecuzione. La sezione seguente mostra come descrivere l'esecuzione di un processo:

```
aws iot describe-job-execution --job-id 017 --thing-name thingOne
```

Il comando restituisce [JobExecution](#) (p. 398). Ad esempio:

```
{
    "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"
            }
        }
    }
}
```

Eliminazione dell'esecuzione di un processo.

Esegui il comando `DeleteJobExecution` per eliminare l'esecuzione di un processo. Per identificare l'esecuzione del processo, devi specificare un ID processo, un nome di oggetto e, facoltativamente, un numero di esecuzione. La sezione seguente mostra come eliminare l'esecuzione di un processo:

```
aws iot delete-job-execution --job-id 017 --thing-name thingOne --execution-number
1234567890 --force|--no-force
```

Il comando non visualizza alcun output.

Per impostazione predefinita, lo stato di esecuzione del processo deve essere `QUEUED` o terminale (`SUCCEEDED`, `FAILED`, `REJECTED`, `TIMED_OUT`, `REMOVED` o `CANCELED`). In caso contrario, si verifica un errore. Per eliminare l'esecuzione di un processo con uno stato `IN_PROGRESS`, è possibile impostare il parametro `force` su `true`.

Warning

Quando si elimina l'esecuzione di un processo con stato `IN_PROGRESS`, il dispositivo che sta eseguendo il processo non è in grado di accedere alle informazioni sul processo o di aggiornare lo stato di esecuzione del processo. Prestare attenzione e verificare che il dispositivo sia in grado di effettuare il ripristino a uno stato valido.

Dispositivi e servizio Jobs

device communication with Jobs

I dispositivi possono comunicare con il servizio AWS IoT Jobs tramite uno dei metodi seguenti:

- MQTT
- HTTP Signature Version 4
- HTTP TLS

using the MQTT protocol

La comunicazione tra il servizio AWS IoT Jobs e i dispositivi può avvenire tramite il protocollo MQTT. I dispositivi sottoscrivono gli argomenti MQTT per ricevere una notifica dei nuovi processi e le risposte dal servizio AWS IoT Jobs. I dispositivi pubblicano negli argomenti MQTT per eseguire query o aggiornare lo stato dell'esecuzione di un processo. Ogni dispositivo ha il proprio argomento MQTT generale. Per ulteriori informazioni sulla pubblicazione e sulla sottoscrizione di argomenti MQTT, consulta [Broker di messaggi per AWS IoT \(p. 239\)](#).

Note

È necessario utilizzare l'endpoint corretto quando si comunica con il servizio AWS IoT Jobs tramite MQTT. Utilizza il comando `DescribeEndpoint` per trovarlo. Ad esempio, se si esegue questo comando:

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

si ottiene un risultato simile al seguente:

```
{  
    "endpointAddress": "a1b2c3d4e5f6g7.iot.us-west-2.amazonaws.com"  
}
```

Con questo metodo, il dispositivo usa il proprio certificato specifico e la chiave privata per eseguire l'autenticazione con il servizio AWS IoT Jobs.

I dispositivi possono:

- Ricevere una notifica ogni volta che l'esecuzione di un processo viene aggiunta o rimossa dall'elenco di esecuzioni in sospeso mediante sottoscrizione all'argomento `$aws/`

`things/<thing-name>/jobs/notify`, dove `thing-name` è il nome dell'oggetto associato al dispositivo.

- Ricevere una notifica quando l'esecuzione del processo in sospeso successiva cambia, sottoscrivendo l'argomento MQTT `$aws/things/<thing-name>/jobs/notify-next`, dove `thing-name` è il nome dell'oggetto associato al dispositivo.
- Aggiornare lo stato dell'esecuzione di un processo chiamando l'API [UpdateJobExecution \(p. 471\)](#).
- Eseguire una query sullo stato dell'esecuzione di un processo chiamando l'API [DescribeJobExecution \(p. 466\)](#).
- Recuperare un elenco delle esecuzioni del processo in sospeso chiamando l'API [GetPendingJobExecutions \(p. 457\)](#).
- Recuperare l'esecuzione del processo in sospeso successiva chiamando l'API [DescribeJobExecution \(p. 466\)](#) con `jobId $next`.
- Ottenere e avviare l'esecuzione del processo in sospeso successiva chiamando l'API [StartNextPendingJobExecution \(p. 460\)](#).

Il servizio AWS IoT Jobs pubblica messaggi di successo e di errore su un argomento MQTT. L'argomento viene formato accodando `accepted` o `rejected` all'argomento utilizzato per effettuare la richiesta. Se, ad esempio, viene pubblicato un messaggio di richiesta sull'argomento `$aws/things/myThing/jobs/get`, il servizio AWS IoT Jobs pubblica i messaggi di esito positivo sull'argomento `$aws/things/myThing/jobs/get/accepted` e i messaggi di esito negativo sull'argomento `$aws/things/myThing/jobs/get/rejected`.

using HTTP Signature Version 4

La comunicazione tra il servizio AWS IoT Jobs e i dispositivi può avvenire tramite il protocollo HTTP Signature Version 4 sulla porta 443. Questo è il metodo usato dagli SDK e dall'interfaccia a riga di comando di AWS. Per ulteriori informazioni su questi strumenti, consulta [Riferimento ai comandi AWS CLI: iot-jobs-data](#) o [SDK e strumenti AWS](#) e fai riferimento alla sezione `iotJobsDataPlane` per la tua lingua preferita.

Note

È necessario utilizzare l'endpoint corretto quando si comunica con il servizio AWS IoT Jobs tramite HTTP Signature Version 4 o impiegando un SDK AWS oppure il comando `iotJobsDataPlane` dell'interfaccia a riga di comando. Utilizza il comando `DescribeEndpoint` per trovarlo. Ad esempio, se si esegue questo comando:

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

si ottiene un risultato simile al seguente:

```
{  
    "endpointAddress": "a1b2c3d4e5f6g7.jobs.iot.us-west-2.amazonaws.com"  
}
```

Con questo metodo di comunicazione, il dispositivo utilizza le credenziali IAM per eseguire l'autenticazione con il servizio AWS IoT Jobs.

Se si usa questo metodo sono disponibili i seguenti comandi:

- `DescribeJobExecution`
- ```
aws iot-jobs-data describe-job-execution ...
```
- `GetPendingJobExecutions`

```
aws iot-jobs-data get-pending-job-executions ...
• StartNextPendingJobExecution

aws iot-jobs-data start-next-pending-job-execution ...
• UpdateJobExecution

aws iot-jobs-data update-job-execution ...
```

using HTTP TLS

La comunicazione tra il servizio AWS IoT Jobs e i tuoi dispositivi può verificarsi tramite il protocollo HTTP TLS sulla porta 8443 usando un client software di terze parti che supporti questo protocollo.

#### Note

È necessario utilizzare l'endpoint corretto quando si comunica con il servizio AWS IoT Jobs tramite HTTP TLS. Utilizza il comando `DescribeEndpoint` per trovarlo. Ad esempio, se si esegue questo comando:

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

si ottiene un risultato simile al seguente:

```
{
 "endpointAddress": "a1b2c3d4e5f6g7.jobs.iot.us-west-2.amazonaws.com"
}
```

Con questo metodo, il dispositivo usa l'autenticazione basata su certificato X.509 (ad esempio, usando il proprio certificato specifico del dispositivo e la chiave privata).

Se si usa questo metodo sono disponibili i seguenti comandi:

- `DescribeJobExecution`
- `GetPendingJobExecutions`
- `StartNextPendingJobExecution`
- `UpdateJobExecution`

## Programmazione dei dispositivi per l'uso di Jobs

Gli esempi di questa sezione usano MQTT per illustrare come funziona un dispositivo che utilizza il servizio AWS IoT Jobs. In alternativa, puoi usare l'API corrispondente o i comandi dell'interfaccia a riga di comando. Per questi esempi, supponiamo che un dispositivo chiamato `MyThing` effettuerà la sottoscrizione ai seguenti argomenti MQTT:

- `$aws/things/MyThing/jobs/notify` (oppure `$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`

In caso di utilizzo di firma del codice per AWS IoT, il codice del tuo dispositivo deve verificare la firma del file di codice. La firma sarà nel documento del processo all'interno della proprietà `codesign`. Per ulteriori

informazioni sulla verifica della firma del file di codice, consulta la sezione relativa all'esempio di agente del dispositivo.

## Flusso di lavoro dei dispositivi

Un dispositivo può gestire i processi da eseguire in due modi.

### Option A: Get the next job

1. Quando un dispositivo passa online per la prima volta, deve sottoscrivere l'argomento `notify-next` del dispositivo.
2. Viene chiamata l'API MQTT [DescribeJobExecution \(p. 466\)](#) con `jobId $next` per ottenere il processo successivo, il relativo documento e altri dettagli, inclusi gli stati salvati in `statusDetails`. Se il documento del processo ha una firma del file del codice, è necessario verificare la firma prima di continuare con l'elaborazione della richiesta di processo.
3. Viene chiamata l'API MQTT [UpdateJobExecution \(p. 471\)](#) per aggiornare lo stato del processo. In alternativa, combinando questa fase con la precedente, il dispositivo può chiamare [StartNextPendingJobExecution \(p. 460\)](#).
4. Se lo desideri, puoi aggiungere un timer della fase impostando un valore per `stepTimeoutInMinutes` quando richiami [UpdateJobExecution \(p. 471\)](#) o [StartNextPendingJobExecution \(p. 460\)](#).
5. Vengono eseguite le operazioni specificate dal documento del processo usando l'API MQTT [UpdateJobExecution \(p. 471\)](#) per segnalare lo stato del processo.
6. Continua a monitorare l'esecuzione del processo chiamando l'[DescribeJobExecution \(p. 466\)](#) API MQTT con questo ID processo. Se l'esecuzione del processo viene annullata o eliminata mentre il dispositivo sta eseguendo il processo, il dispositivo dovrebbe essere in grado di effettuare il ripristino a uno stato valido.
7. Chiama l'[UpdateJobExecution \(p. 471\)](#) API MQTT al termine del processo per aggiornare lo stato del processo e segnalare l'esito positivo o negativo.
8. Poiché lo stato dell'esecuzione di questo processo è stato modificato in stato terminale, il processo successivo disponibile per l'esecuzione (se presente) cambia. Al dispositivo viene inviata una notifica che segnala che l'esecuzione del processo in sospeso successiva è cambiata. A questo punto, il dispositivo deve continuare come descritto nella fase 2.

Se il dispositivo rimane online, continua a ricevere le notifiche delle esecuzioni del processo in sospeso successive, inclusi i dati di esecuzione del processo, quando un processo viene completato o quando viene aggiunta una nuova esecuzione del processo in sospeso. Quando ciò si verifica, il dispositivo continua come descritto nella fase 2.

### Option B: Pick from available jobs

1. Quando un dispositivo passa online per la prima volta, deve sottoscrivere l'argomento `notify` dell'oggetto.
2. Viene chiamata l'API MQTT [GetPendingJobExecutions \(p. 457\)](#) per ottenere un elenco delle esecuzioni del processo in sospeso.
3. Se l'elenco contiene una o più esecuzioni, ne viene selezionata una.
4. Viene chiamata l'API MQTT [DescribeJobExecution \(p. 466\)](#) per ottenere il documento del processo e altri dettagli, inclusi gli stati salvati in `statusDetails`.
5. Viene chiamata l'API MQTT [UpdateJobExecution \(p. 471\)](#) per aggiornare lo stato del processo. Se il campo `includeJobDocument` è impostato su `true` in questo comando, il dispositivo può ignorare la fase precedente e recuperare il documento del processo da questo punto.
6. Se lo desideri, puoi aggiungere un timer della fase impostando un valore per `stepTimeoutInMinutes` quando richiami [UpdateJobExecution \(p. 471\)](#).

7. Vengono eseguite le operazioni specificate dal documento del processo usando l'API MQTT [UpdateJobExecution \(p. 471\)](#) per segnalare lo stato del processo.
8. Continua a monitorare l'esecuzione del processo chiamando l'[DescribeJobExecution \(p. 466\)](#) API MQTT con questo ID processo. Se l'esecuzione del processo viene annullata o eliminata mentre il dispositivo sta eseguendo il processo, il dispositivo dovrebbe essere in grado di effettuare il ripristino a uno stato valido.
9. Chiama l'[UpdateJobExecution \(p. 471\)](#) API MQTT al termine del processo per aggiornare lo stato del processo e per segnalare l'esito positivo o negativo.

Se il dispositivo rimane online, riceve una notifica di tutte le esecuzioni del processo in sospeso quando una nuova esecuzione in sospeso diventa disponibile. Quando ciò si verifica, il dispositivo può continuare come descritto nella fase 2.

Se il dispositivo non è in grado di eseguire il processo, deve chiamare l'API MQTT [UpdateJobExecution \(p. 471\)](#) per aggiornare lo stato del processo a REJECTED.

## Avvio di un nuovo processo

new job notification

Quando viene creato un nuovo processo, il servizio AWS IoT Jobs pubblica un messaggio sull'argomento `$aws/things/thing-name/jobs/notify` per ogni dispositivo target.

more info (1)

Il messaggio contiene le informazioni seguenti:

```
{
 "timestamp":1476214217017,
 "jobs":{
 "QUEUED": [{
 "jobId":"0001",
 "queuedAt":1476214216981,
 "lastUpdatedAt":1476214216981,
 "versionNumber" : 1
 }]
 }
}
```

Il dispositivo riceve questo messaggio sull'argomento '`$aws/things/thingName/jobs/notify`' quando l'esecuzione del processo viene aggiunta alla coda.

get job information

Per ottenere ulteriori informazioni sull'esecuzione di un processo, il dispositivo chiama l'API MQTT [DescribeJobExecution \(p. 466\)](#) con il campo `includeJobDocument` impostato su `true` (impostazione di default).

more info (2)

Se la richiesta ha esito positivo, il servizio AWS IoT Jobs pubblica un messaggio sull'argomento `$aws/things/MyThing/jobs/0023/get/accepted`:

```
{
 "clientToken" : "client-001",
 "timestamp" : 1489097434407,
 "execution" : {
 "approximateSecondsBeforeTimedOut": number,
 }
}
```

```
 "jobId" : "023",
 "status" : "QUEUED",
 "queuedAt" : 1489097374841,
 "lastUpdatedAt" : 1489097374841,
 "versionNumber" : 1,
 "jobDocument" : {
 < contents of job document >
 }
 }
}
```

#### Note

Se la richiesta ha esito negativo, il servizio AWS IoT Jobs pubblica un messaggio sull'argomento `$aws/things/MyThing/jobs/0023/get/rejected`.

Il dispositivo a questo punto dispone del documento del processo che può utilizzare per eseguire le operazioni remote per il processo. Se il documento del processo contiene un URL Amazon S3 prefirmato, il dispositivo può usare l'URL per scaricare i file necessari per il processo.

## Segnalazione dello stato dell'esecuzione del processo

update execution status

Quando un dispositivo esegue il processo, può chiamare l'API MQTT [UpdateJobExecution \(p. 471\)](#) per aggiornare lo stato dell'esecuzione del processo.

more info (3)

Ad esempio, un dispositivo può aggiornare lo stato dell'esecuzione di un processo impostandolo su IN\_PROGRESS pubblicando il messaggio seguente nell'argomento `$aws/things/MyThing/jobs/0023/update`:

```
{
 "status": "IN_PROGRESS",
 "statusDetails": {
 "progress": "50%"
 },
 "expectedVersion": "1",
 "clientToken": "client001"
}
```

Jobs risponde pubblicando un messaggio nell'argomento `$aws/things/MyThing/jobs/0023/update/accepted` o `$aws/things/MyThing/jobs/0023/update/rejected`:

```
{
 "clientToken": "client001",
 "timestamp": 1476289222841
}
```

Il dispositivo può combinare le due richieste precedenti chiamando [StartNextPendingJobExecution \(p. 460\)](#). In questo modo si ottiene e si avvia la successiva esecuzione di processo in sospeso e si consente al dispositivo di aggiornare lo stato di esecuzione del processo. Questa richiesta, inoltre, restituisce il documento del processo quando c'è un'esecuzione del processo in sospeso.

Se il processo contiene un [TimeoutConfig](#), il timer in corso si avvia. Puoi anche impostare un timer della fase per l'esecuzione di un processo impostando un valore per `stepTimeoutInMinutes` quando richiami [UpdateJobExecution](#). Il timer della fase si applica solo all'esecuzione del processo

che stai aggiornando. È possibile impostare un nuovo valore per questo timer ogni volta che si aggiorna l'esecuzione di un processo. Puoi anche creare un timer della fase quando richiami [StartNextPendingJobExecution](#). Se l'esecuzione del processo resta nello stato `IN_PROGRESS` per un periodo di tempo superiore a quello consentito dall'intervallo del timer della fase, l'esecuzione del processo non va a buon fine e viene impostato lo stato `TIMED_OUT` terminale. Il timer della fase non ha alcun effetto su quello in corso impostato al momento della creazione di un processo.

#### Note

La caratteristica di timeout del processo non è attualmente disponibile nella regione PDT (us-gov-west-1).

Il campo `status` può essere impostato su `IN_PROGRESS`, `SUCCEEDED` o `FAILED`. Non è possibile aggiornare lo stato dell'esecuzione di un processo già in stato terminale.

#### report execution completed

Quando il dispositivo completa l'esecuzione del processo, chiama l'API MQTT [UpdateJobExecution \(p. 471\)](#). Se il processo ha avuto esito positivo, impostare `status` su `SUCCEEDED` e, nel payload del messaggio, in `statusDetails`, aggiungere altre informazioni sul processo come coppie nome-valore. Il timer in corso e quello della fase si interrompono al completamento dell'esecuzione del processo.

[more info \(4\)](#)

Ad esempio:

```
{
 "status": "SUCCEEDED",
 "statusDetails": {
 "progress": "100%"
 },
 "expectedVersion": "2",
 "clientToken": "client-001"
}
```

Se il processo ha avuto esito negativo, il valore di `status` viene impostato su `FAILED` e in `statusDetails` vengono aggiunte informazioni sull'errore che si è verificato:

```
{
 "status": "FAILED",
 "statusDetails": {
 "errorCode": "101",
 "errorMsg": "Unable to install update"
 },
 "expectedVersion": "2",
 "clientToken": "client-001"
}
```

#### Note

L'attributo `statusDetails` può contenere un numero qualsiasi di coppie nome-valore.

Quando il servizio AWS IoT Jobs riceve questo aggiornamento, pubblica un messaggio sull'argomento `$aws/things/MyThing/jobs/notify` per indicare che l'esecuzione del processo è completa:

```
{
 "timestamp": 1476290692776,
 "jobs": {}
}
```

}

## Processi aggiuntivi

additional jobs

Se ci sono altre esecuzioni dei processi in sospeso per il dispositivo, vengono incluse nel messaggio pubblicato in `$aws/things/MyThing/jobs/notify`.

more info (5)

Ad esempio:

```
{
 "timestamp":1476290692776,
 "jobs":{
 "QUEUED": [{
 "jobId": "0002",
 "queuedAt": 1476290646230,
 "lastUpdatedAt": 1476290646230
 }],
 "IN_PROGRESS": [{
 "jobId": "0003",
 "queuedAt": 1476290646230,
 "lastUpdatedAt": 1476290646230
 }]
 }
}
```

## Notifiche dei job

Il servizio AWS IoT Jobs pubblica messaggi MQTT in argomenti riservati in caso di processi in sospeso o se viene modificata la prima esecuzione di un processo nell'elenco. I dispositivi possono tenere traccia dei processi in sospeso iscrivendosi a questi argomenti.

Le notifiche dei processi vengono pubblicate in MQTT come payload JSON. Sono disponibili due tipi di notifiche:

- `ListNotification` contiene un elenco di un massimo di 10 esecuzioni di processo in sospeso. Le esecuzioni dei processi in questo elenco hanno valori di stato di `IN_PROGRESS` o `QUEUED`. Sono ordinate in base allo stato (le esecuzioni dei processi `IN_PROGRESS` hanno la precedenza rispetto alle esecuzioni dei processi `QUEUED`), quindi in base al momento in cui sono state messi in coda.

Una notifica `ListNotification` viene pubblicata ogni volta che viene soddisfatto uno dei seguenti criteri.

- Una nuova esecuzione di un processo è in coda o passa a uno stato non terminale (`IN_PROGRESS` o `QUEUED`).
- Un'esecuzione precedente di un processo passa a uno stato terminale (`FAILED`, `SUCCEEDED`, `CANCELED`, `TIMED_OUT`, `REJECTED` o `REMOVED`).
- `NextNotification` contiene informazioni di riepilogo sull'esecuzione di processo successiva nella coda.

Una notifica `NextNotification` viene pubblicata ogni volta che la prima esecuzione di un processo nell'elenco cambia.

- Una nuova esecuzione di un processo viene aggiunta all'elenco come `QUEUED` ed è la prima nell'elenco.

- Lo stato dell'esecuzione di un processo che non era la prima nell'elenco passa da `QUEUED` a `IN_PROGRESS` e l'esecuzione diventa la prima nell'elenco. Ciò si verifica quando non sono presenti altre esecuzioni di processi `IN_PROGRESS` nell'elenco o quando l'esecuzione del processo il cui stato passa da `QUEUED` a `IN_PROGRESS` era stata messa in coda prima di ogni altra esecuzione di un processo `IN_PROGRESS` nell'elenco.
- L'esecuzione del processo prima nell'elenco passa a uno stato terminale e viene rimossa dall'elenco.

Per ulteriori informazioni sulla pubblicazione e sulla sottoscrizione di argomenti MQTT, consulta [Broker di messaggi per AWS IoT \(p. 239\)](#).

#### Note

Quando si utilizza HTTP Signature Version 4 o HTTP TLS per comunicare con i processi, le notifiche non sono disponibili.

job pending

Il servizio AWS IoT Jobs pubblica un messaggio in un argomento MQTT quando un processo viene aggiunto o rimosso dall'elenco di esecuzioni in sospeso per un oggetto oppure se viene modificata la prima esecuzione di un processo nell'elenco:

- `$aws/things/thingName/jobs/notify`
- `$aws/things/thingName/jobs/notify-next`

more info (6)

I messaggi contengono i payload di esempio seguenti:

`$aws/things/thingName/jobs/notify:`

```
{
 "timestamp" : 10011,
 "jobs" : {
 "IN_PROGRESS" : [{
 "jobId" : "other-job",
 "queuedAt" : 10003,
 "lastUpdatedAt" : 10009,
 "executionNumber" : 1,
 "versionNumber" : 1
 }],
 "QUEUED" : [{
 "jobId" : "this-job",
 "queuedAt" : 10011,
 "lastUpdatedAt" : 10011,
 "executionNumber" : 1,
 "versionNumber" : 0
 }]
 }
}
```

`$aws/things/thingName/jobs/notify-next:`

```
{
 "timestamp" : 10011,
 "execution" : {
 "jobId" : "other-job",
 "status" : "IN_PROGRESS",
 "queuedAt" : 10009,
 "lastUpdatedAt" : 10009,
 "executionNumber" : 1,
 "versionNumber" : 1
 }
}
```

```
 "lastUpdatedAt" : 10009,
 "versionNumber" : 1,
 "executionNumber" : 1,
 "jobDocument" : {"c":"d"}
 }
}
```

Possibili valori di stato dell'esecuzione del processo sono QUEUED, IN\_PROGRESS, FAILED, SUCCEEDED, CANCELED, TIMED\_OUT, REJECTED e REMOVED.

La serie di esempi riportata di seguito mostra le notifiche che vengono pubblicate in ciascun argomento quando le esecuzioni dei processi vengono create e passano da uno stato all'altro.

Per prima cosa, viene creato un processo chiamato job1. Questa notifica viene pubblicata nell'argomento jobs/notify:

```
{
 "timestamp": 1517016948,
 "jobs": {
 "QUEUED": [
 {
 "jobId": "job1",
 "queuedAt": 1517016947,
 "lastUpdatedAt": 1517016947,
 "executionNumber": 1,
 "versionNumber": 1
 }
]
 }
}
```

Questa notifica viene pubblicata nell'argomento jobs/notify-next:

```
{
 "timestamp": 1517016948,
 "execution": {
 "jobId": "job1",
 "status": "QUEUED",
 "queuedAt": 1517016947,
 "lastUpdatedAt": 1517016947,
 "versionNumber": 1,
 "executionNumber": 1,
 "jobDocument": {
 "operation": "test"
 }
 }
}
```

Quando viene creato un altro processo (job2), questa notifica viene pubblicata nell'argomento jobs/notify:

```
{
 "timestamp": 1517017192,
 "jobs": {
 "QUEUED": [
 {
 "jobId": "job1",
 "queuedAt": 1517016947,
 "lastUpdatedAt": 1517016947,
 "executionNumber": 1,
 "versionNumber": 1
 }
]
 }
}
```

```
 },
 [
 {
 "jobId": "job2",
 "queuedAt": 1517017191,
 "lastUpdatedAt": 1517017191,
 "executionNumber": 1,
 "versionNumber": 1
 }
]
 }
}
```

Una notifica non viene pubblicata nell'argomento `jobs/notify-next` poiché il processo successivo nella coda (`job1`) non è cambiato. Quando inizia l'esecuzione di `job1`, passa allo stato `IN_PROGRESS`. Non vengono pubblicate notifiche perché l'elenco dei processi e il processo successivo in coda non sono cambiati.

Quando viene aggiunto un terzo processo (`job3`), questa notifica viene pubblicata nell'argomento `jobs/notify`:

```
{
 "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
 }
]
 }
}
```

Una notifica non viene pubblicata nell'argomento `jobs/notify-next` poiché il processo successivo nella coda è ancora `job1`.

Quando `job1` viene completato, passa allo stato `SUCCEEDED` e questa notifica viene pubblicata nell'argomento `jobs/notify`:

```
{
 "timestamp": 1517186269,
 "jobs": {
 "QUEUED": [

```

```
{
 "jobId": "job2",
 "queuedAt": 1517017191,
 "lastUpdatedAt": 1517017191,
 "executionNumber": 1,
 "versionNumber": 1
},
{
 "jobId": "job3",
 "queuedAt": 1517017905,
 "lastUpdatedAt": 1517017905,
 "executionNumber": 1,
 "versionNumber": 1
}
]
}
```

A questo punto, job1 è stato rimosso dalla coda e il processo successivo da eseguire è job2. Questa notifica viene pubblicata nell'argomento `jobs/notify-next`:

```
{
 "timestamp": 1517186269,
 "execution": {
 "jobId": "job2",
 "status": "QUEUED",
 "queuedAt": 1517017191,
 "lastUpdatedAt": 1517017191,
 "versionNumber": 1,
 "executionNumber": 1,
 "jobDocument": {
 "operation": "test"
 }
 }
}
```

Se job3 deve essere eseguito prima di job2 (operazione non consigliata), è possibile modificare lo stato di job3 in IN\_PROGRESS. In questo caso, job2 non è più il successivo processo in coda e questa notifica viene pubblicata sull'argomento `jobs/notify-next`:

```
{
 "timestamp": 1517186779,
 "execution": {
 "jobId": "job3",
 "status": "IN_PROGRESS",
 "queuedAt": 1517017905,
 "startedAt": 1517186779,
 "lastUpdatedAt": 1517186779,
 "versionNumber": 2,
 "executionNumber": 1,
 "jobDocument": {
 "operation": "test"
 }
 }
}
```

Non vengono pubblicate notifiche nell'argomento `jobs/notify` perché non sono stati aggiunti o rimossi processi.

Se il dispositivo respinge job2 e aggiorna lo stato in REJECTED, questa notifica viene pubblicata sull'argomento `jobs/notify`:

```
{
 "timestamp": 1517189392,
 "jobs": [
 "IN_PROGRESS": [
 {
 "jobId": "job3",
 "queuedAt": 1517017905,
 "lastUpdatedAt": 1517186779,
 "startedAt": 1517186779,
 "executionNumber": 1,
 "versionNumber": 2
 }
]
 }
}
```

Se job3 (che è ancora in corso) viene eliminato in modo forzato, questa notifica viene pubblicata sull'argomento `jobs/notify`:

```
{
 "timestamp": 1517189551,
 "jobs": {}
}
```

A questo punto, la coda è vuota. Questa notifica viene pubblicata nell'argomento `jobs/notify-next`:

```
{
 "timestamp": 1517189551
}
```

## Uso delle API di AWS IoT Jobs

Sono due le categorie di API usate nel servizio AWS IoT Jobs:

- La API usate per la gestione e il controllo dei processi.
- Le API usate dai dispositivi che eseguono i processi.

In generale, per la gestione e il controllo dei processi viene usata un'API del protocollo HTTPS. I dispositivi possono usare un'API del protocollo MQTT o HTTPS. L'API HTTPS è progettata per un basso volume di chiamate, come avviene in genere quando si creano e si monitorano i processi. In genere apre una connessione per una singola richiesta e quindi chiude la connessione dopo la ricezione della risposta. L'API MQTT permette il polling lungo. È progettata per grandi quantità di traffico, che può arrivare a milioni di dispositivi.

### Note

Ogni API HTTPS di AWS IoT Jobs dispone di un comando corrispondente che permette di chiamare l'API dall'AWS CLI. I comandi sono in caratteri minuscoli, con trattini tra le parole che compongono il nome dell'API. È ad esempio possibile richiamare l'API `CreateJob` nell'interfaccia a riga di comando digitando:

```
aws iot create-job ...
```

# API di gestione e controllo dei processi

## Tipi di dati di gestione e controllo dei processi

I tipi di dati seguenti vengono usati dalle applicazioni di gestione e controllo per comunicare con il servizio AWS IoT Jobs.

### Processo

#### Job data type

L'oggetto `Job` contiene i dettagli di un processo.

syntax (1)

```
{
 "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
 }
]
 },
}
```

```
 "timeoutConfig": {
 "inProgressTimeoutInMinutes": long
 }
}
```

**description (1)**

**jobArn**

ARN che identifica il processo nel formato "arn:aws:iot:**region:account**:job/**jobId**".

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

**status**

Stato del processo, tra IN\_PROGRESS, CANCELED e SUCCEEDED.

**targetSelection**

Specifica se l'esecuzione del processo continua (CONTINUOUS) o se il processo viene completato dopo che tutti gli oggetti specificati come target hanno completato il processo (SNAPSHOT). Se il valore è CONTINUOUS, il processo può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un processo viene eseguito in un oggetto quando l'oggetto viene aggiunto a un gruppo target, anche dopo che il processo è stato completato da tutti gli oggetti originariamente nel gruppo.

**comment**

Se il processo è stato aggiornato, descrive il motivo dell'aggiornamento.

**targets**

Elenco di oggetti e gruppi di oggetti AWS IoT cui deve essere inviato il processo.

**description**

Breve descrizione di testo del processo.

**createdAt**

Periodo di tempo, in secondi, dall'epoca (Unix epoch) alla creazione del processo.

**lastUpdatedAt**

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento del processo.

**completedAt**

Periodo di tempo, in secondi, dall'epoca al completamento del processo.

**jobProcessDetails**

Dettagli sull'elaborazione del processo:

**processingTargets**

Elenco di oggetti e gruppi di oggetti AWS IoT che stanno attualmente eseguendo il processo.

**numberOfCanceledThings**

Numero di oggetti AWS IoT che hanno annullato il processo.

**numberOfSucceededThings**

Numero di oggetti AWS IoT che hanno completato con successo il processo.

**numberOfFailedThings**

Numero di oggetti AWS IoT che non hanno completato il processo.

**numberOfRejectedThings**

Numero di oggetti AWS IoT che hanno rifiutato il processo.

**numberOfQueuedThings**

Numero di oggetti AWS IoT che sono in attesa dell'esecuzione del processo.

**numberOfInProgressThings**

Numero di oggetti AWS IoT che stanno attualmente eseguendo il processo.

**numberOfRemovedThings**

Numero di oggetti AWS IoT per cui non è più pianificata l'esecuzione del processo, perché sono stati eliminati o rimossi dal gruppo che costituiva un target del processo.

**numberOfTimedOutThings**

Il numero di oggetti il cui stato di esecuzione del processo è `TIMED_OUT`.

**presignedUrlConfig**

Informazioni di configurazione per URL Amazon S3 prefirmati.

**expiresInSec**

Periodo di validità (in secondi) degli URL prefirmati. I valori validi sono compresi tra 60 e 3600. Il valore predefinito è 3600 secondi. Gli URL prefirmati vengono generati quando il servizio AWS IoT Jobs riceve una richiesta MQTT per il documento del processo.

**roleArn**

ARN di un ruolo IAM che concede l'autorizzazione per il download di file da un bucket Amazon S3. Il ruolo deve anche concedere l'autorizzazione affinché AWS IoT esegua il download dei file. Per ulteriori informazioni su come creare e configurare il ruolo, consulta [Creazione di processi \(p. 373\)](#).

**jobExecutionRolloutConfig**

Opzionale. Permette di creare un'implementazione per fasi di un processo.

**maximumPerMinute**

Numero massimo di oggetti (dispositivi) a cui il processo viene inviato per l'esecuzione, per minuto.

**exponentialRate**

Consente di creare una velocità esponenziale di rollout per un processo.

**baseRatePerMinute**

Il numero minimo di oggetti che ricevono una notifica di un processo in sospeso, ogni minuto, all'inizio del rollout di processo. Questo parametro consente di definire la velocità iniziale di un rollout.

**incrementFactor**

Il fattore esponenziale per aumentare la velocità di rollout per un processo.

**rateIncreaseCriteria**

I criteri per avviare l'aumento della velocità di rollout per un processo. Puoi specificare `numberOfNotifiedThings` o `numberOfSucceededThing`, ma non entrambi.

**numberOfNotifiedThings**

La soglia per il numero di oggetti notificati che avvia l'aumento della velocità di rollout.

**numberOfSucceededThings**

La soglia per il numero di oggetti completati che avvia l'aumento della velocità di rollout.

**abortConfig**

Opzionale. Dettagli dei criteri di interruzione per interrompere il processo.

**criteriaList**

L'elenco dei criteri di eliminazione per definire regole per interrompere il processo.

**action**

Il tipo di operazione di eliminazione per avviare l'interruzione di un processo.

**failureType**

Il tipo di errore di esecuzione di processo per definire una regola di avvio dell'interruzione di un processo.

**minNumberOfExecutedThings**

Il numero minimo di oggetti eseguiti prima della valutazione della regola di interruzione.

**thresholdPercentage**

La soglia come percentuale del numero totale di oggetti eseguiti che iniziano l'interruzione di un processo.

**timeoutConfig**

Opzionale. Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione del processo. Il timer viene avviato quando imposti lo stato di esecuzione del processo su **IN\_PROGRESS**. Se lo stato di esecuzione del processo non è impostato su un altro stato terminale prima della scadenza del tempo a disposizione, viene automaticamente impostato su **TIMED\_OUT**.

**Note**

La caratteristica di timeout del processo non è attualmente disponibile nella regione PDT (`us-gov-west-1`).

**inProgressTimeoutInMinutes**

Specifica l'intervallo di tempo, in minuti, a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Un timer viene avviato o riavviato ogni volta che lo stato di questa esecuzione del processo viene specificato come **IN\_PROGRESS**, con il campo compilato. Se lo stato di esecuzione del processo non viene impostato su uno stato terminale prima del timeout o prima che un altro aggiornamento dello stato di esecuzione del processo venga inviato con il campo compilato, lo stato viene impostato su **TIMED\_OUT**.

## JobSummary

### JobSummary data type

L'oggetto **JobSummary** contiene il riepilogo di un processo.

#### syntax (2)

```
{
 "jobArn": "string",
 "jobId": "string",
 "status": "IN_PROGRESS|CANCELED|SUCCEEDED",
 "targetSelection": "CONTINUOUS|SNAPSHOT",
}
```

```
 "thingGroupId": "string",
 "createdAt": timestamp,
 "lastUpdatedAt": timestamp,
 "completedAt": timestamp
}
```

description (2)

jobArn

ARN che identifica il processo.

jobId

Identificatore univoco assegnato al processo al momento della creazione.

status

Stato del processo. Può essere IN\_PROGRESS, CANCELED o SUCCEEDED.

targetSelection

Specifica se l'esecuzione del processo continua (CONTINUOUS) o se il processo viene completato dopo che tutti gli oggetti specificati come target hanno completato il processo (SNAPSHOT). Se il valore è CONTINUOUS, il processo può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un processo viene eseguito in un oggetto quando l'oggetto viene aggiunto a un gruppo target, anche dopo che il processo è stato completato da tutti gli oggetti originariamente nel gruppo.

thingGroupId

ID del gruppo di oggetti.

createdAt

Timestamp UNIX relativo al momento della creazione del processo.

lastUpdatedAt

Timestamp UNIX relativo al momento dell'ultimo aggiornamento del processo.

completedAt

Timestamp UNIX relativo al momento del completamento del processo.

## JobExecution

JobExecution data type

L'oggetto JobExecution rappresenta l'esecuzione di un processo in un dispositivo.

syntax (3)

```
{
 "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
}
```

#### description (3)

##### approximateSecondsBeforeTimedOut

Il numero stimato di secondi che rimangono prima che lo stato di esecuzione del processo venga modificato in `TIMED_OUT`. L'intervallo di timeout può essere compreso fra 1 minuto e 7 giorni (da 1 a 10080 minuti). L'effettivo timeout dell'esecuzione del processo può verificarsi 60 secondi dopo la durata stimata.

##### jobId

Identificatore univoco assegnato al processo al momento della creazione.

##### executionNumber

Numero che identifica l'esecuzione del processo nel dispositivo. Può essere usato successivamente in comandi che restituiscono o aggiornano le informazioni sull'esecuzione del processo.

##### thingArn

ARN dell'oggetto AWS IoT.

##### queuedAt

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.

##### lastUpdatedAt

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.

##### startedAt

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.

##### status

Stato dell'esecuzione del processo. Può essere `QUEUED`, `IN_PROGRESS`, `FAILED`, `SUCCEEDED`, `CANCELED`, `TIMED_OUT`, `REJECTED` o `REMOVED`.

##### statusDetails

Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo.

## JobExecutionSummary

### JobExecutionSummary data type

L'oggetto `JobExecutionSummary` contiene informazioni di riepilogo sull'esecuzione del processo:

#### syntax (4)

```
{
 "executionNumber": 1234567890,
 "queuedAt": timestamp,
 "lastUpdatedAt": timestamp,
```

```
 "startedAt": timestamp,
 "status": "QUEUED|IN_PROGRESS|FAILED|SUCCEEDED|CANCELED|TIMED_OUT|REJECTED|REMOVED"
 }
```

description (4)

**executionNumber**

Numero che identifica un'esecuzione di un processo in un dispositivo. Può essere usato successivamente in comandi che restituiscono o aggiornano le informazioni sull'esecuzione del processo.

**queuedAt**

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.

**lastUpdatedAt**

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.

**startAt**

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.

**status**

Lo stato dell'esecuzione del processo: QUEUED, IN\_PROGRESS, FAILED, SUCCEEDED, CANCELED, TIMED\_OUT, REJECTED o REMOVED.

## JobExecutionSummaryForJob

JobExecutionSummaryForJob data type

L'oggetto JobExecutionSummaryForJob contiene un riepilogo delle informazioni sulle esecuzioni di un determinato processo.

syntax (5)

```
{
 "executionSummaries": [
 {
 "thingArn": "arn:aws:iot:us-west-2:123456789012:thing/MyThing",
 "jobExecutionSummary": {
 "status": "IN_PROGRESS",
 "lastUpdatedAt": 1549395301.389,
 "queuedAt": 1541526002.609,
 "executionNumber": 1
 }
 },
 ...
]
}
```

description (5)

**thingArn**

ARN dell'oggetto AWS IoT.

**jobExecutionSummary**

Oggetto [JobExecutionSummary](#) (p. 399).

## JobExecutionSummaryForThing

JobExecutionSummaryForThing data type

L'oggetto `JobExecutionSummaryForThing` contiene un riepilogo delle informazioni sull'esecuzione di un processo in un oggetto specifico.

syntax (6)

```
{
 "executionSummaries": [
 {
 "jobExecutionSummary": {
 "status": "IN_PROGRESS",
 "lastUpdatedAt": 1549395301.389,
 "queuedAt": 1541526002.609,
 "executionNumber": 1
 },
 "jobId": "MyThingJob"
 },
 ...
]
}
```

description (6)

`jobId`

Identificatore univoco assegnato al processo al momento della creazione.

`jobExecutionSummary`

Oggetto [JobExecutionSummary](#) (p. 399).

## Comandi HTTPS di gestione e controllo dei processi

Per la gestione e il controllo delle applicazioni tramite il protocollo HTTPS sono disponibili i comandi seguenti.

### AssociateTargetsWithJob

AssociateTargetsWithJob command

Associa un gruppo a un processo continuo. Per ulteriori informazioni, consulta [CreateJob](#) (p. 409). Devono essere soddisfatti i criteri seguenti:

- Il processo deve essere stato creato con il campo `targetSelection` impostato su `CONTINUOUS`.
- Lo stato del processo deve essere `IN_PROGRESS`.
- Il numero totale di target associati a un processo non deve essere superiore a 100.

HTTPS (1)

Richiesta:

```
POST /jobs/jobId/targets

{
 "targets": ["string"],
 "comment": "string"
}
```

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

**targets**

Elenco di ARN dei gruppi di oggetti che definiscono i target del processo.

**comment**

Opzionale. Stringa di commento che descrive il motivo per cui il processo è stato associato ai target.

Risposta:

```
{
 "jobArn": "string",
 "jobId": "string",
 "description": "string"
}
```

**jobArn**

ARN che identifica il processo.

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

**description**

Breve descrizione di testo del processo.

CLI (1)

Riepilogo:

```
aws iot associate-targets-with-job \
 --targets <value> \
 --job-id <value> \
 [--comment <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "targets": [
 "string"
],
 "jobId": "string",
 "comment": "string"
}
```

Campi di **cli-input-json**:

| Nome    | Tipo                        | Descrizione                                                                |
|---------|-----------------------------|----------------------------------------------------------------------------|
| targets | elenco<br>Membro: TargetArn | Elenco di ARN dei gruppi di oggetti che definiscono i target del processo. |

| Nome      | Tipo                                                                       | Descrizione                                                                                 |
|-----------|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| TargetArn | Stringa                                                                    |                                                                                             |
| jobId     | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+ | Identificatore univoco assegnato al processo al momento della creazione.                    |
| comment   | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+               | Stringa facoltativa che descrive il motivo per cui il processo è stato associato ai target. |

Output:

```
{
 "jobArn": "string",
 "jobId": "string",
 "description": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome        | Tipo                                                                       | Descrizione                                                              |
|-------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------|
| jobArn      | Stringa                                                                    | ARN che identifica il processo.                                          |
| jobId       | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+ | Identificatore univoco assegnato al processo al momento della creazione. |
| description | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+               | Breve descrizione di testo del processo.                                 |

## MQTT (1)

Non disponibile.

## CancelJob

CancelJob command

Annulla un processo.

## HTTPS (2)

Richiesta:

```
PUT /jobs/jobId/cancel
```

```
{
 "force": boolean,
 "comment": "string",
 "reasonCode": "string"
}
```

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

**force**

[Opzionale] Se true, le esecuzioni di processo con stato IN\_PROGRESS e QUEUED sono annullate. Altrimenti, sono annullate solo le esecuzioni di processo con stato QUEUED. Il valore di default è false.

**Warning**

L'annullamento di un processo con stato IN\_PROGRESS impedirà al dispositivo che esegue il processo di aggiornarne lo stato di esecuzione del processo. Prestare attenzione e verificare che tutti i dispositivi in cui sono in esecuzione processi annullati siano in grado di effettuare il ripristino a uno stato valido.

**comment**

[Opzionale] Stringa di commento che descrive il motivo per cui il processo è stato annullato.

**reasonCode**

[Opzionale] Una stringa di codice motivo che spiega perché il processo è stato annullato. Se un processo viene annullato perché soddisfa le condizioni definite da un abortConfig, questo campo viene compilato automaticamente.

Risposta:

```
{
 "jobArn": "string",
 "jobId": "string",
 "description": "string"
}
```

**jobArn**

ARN del processo.

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

**description**

Breve descrizione di testo del processo.

CLI (2)

Riepilogo:

```
aws iot cancel-job \
 --job-id <value> \

```

```
[--force <value>] \
[--comment <value>] \
[--reasonCode <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "jobId": "string",
 "force": boolean,
 "comment": "string"
}
```

Campi di **cli-input-json**:

| Nome       | Tipo                                                                     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId      | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-zA-Z0-9_-]+ | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                                                                                                                                                                                                                                                                                                          |
| force      | booleano                                                                 | Se true, i processi con stato QUEUED e IN_PROGRESS sono annullati. Altrimenti, sono annullati solo i processi con stato QUEUED.<br><br>Warning<br><br>L'annullamento di un processo con stato IN_PROGRESS impedirà al dispositivo che esegue il processo di aggiornarne lo stato di esecuzione del processo. Prestare attenzione e verificare che tutti i dispositivi in cui sono in esecuzione processi annullati siano in grado di effettuare il ripristino a uno stato valido. |
| comment    | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+             | Una stringa di commento opzionale che descrive il motivo per cui il processo è stato annullato.                                                                                                                                                                                                                                                                                                                                                                                   |
| reasonCode | Stringa<br><br>Lunghezza max: 128<br><br>Modello: [\p{Upper}\p{Digit}_]+ | Una stringa facoltativa che spiega il motivo per cui il processo è stato annullato. Se un processo viene annullato perché soddisfa i criteri definiti da un <code>abortConfig</code> ,                                                                                                                                                                                                                                                                                            |

| Nome | Tipo | Descrizione                                   |
|------|------|-----------------------------------------------|
|      |      | questo campo viene compilato automaticamente. |

Output:

```
{
 "jobArn": "string",
 "jobId": "string",
 "description": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome        | Tipo    | Descrizione                                           |
|-------------|---------|-------------------------------------------------------|
| jobArn      | Stringa | ARN del processo.                                     |
| jobId       | Stringa | Lunghezza max: 64, min.: 1<br>Modello: [a-zA-Z0-9_-]+ |
| description | Stringa | Breve descrizione di testo del processo.              |

## MQTT (2)

Non disponibile.

## CancelJobExecution

CancelJobExecution command

Annulla l'esecuzione di un processo su un dispositivo.

## HTTPS (3)

Richiesta:

```
PUT /things/thingName/jobs/jobId/cancel
{
 "force": boolean,
 "expectedVersion": "string",
 "statusDetails": {
 "string": "string"
 ...
 }
}
```

**thingName**

Il nome dell'oggetto di cui verrà annullata l'esecuzione del processo.

**jobId**

Identificatore univoco assegnato al processo quando è stato creato.

**force**

Opzionale. Se `true`, l'esecuzione di un processo con stato `IN_PROGRESS` o `QUEUED` può essere annullata. Altrimenti, può essere annullata solo l'esecuzione di un processo con stato `QUEUED`. Se si tenta di annullare l'esecuzione di un processo con stato `IN_PROGRESS` e non si imposta `force` su `true`, viene generata un'eccezione `InvalidStateTransitionException`. Il valore di default è `false`.

**Warning**

L'annullamento di un processo con stato `IN_PROGRESS` impedirà al dispositivo che esegue il processo di aggiornarne lo stato di esecuzione del processo. Prestare attenzione e verificare che tutti i dispositivi in cui sono in esecuzione processi annullati siano in grado di effettuare il ripristino a uno stato valido.

**expectedVersion**

Opzionale. Versione corrente prevista dell'esecuzione del processo. Ogni volta che aggiorni l'esecuzione del processo, la versione viene incrementata. Se la versione dell'esecuzione del processo archiviata nel servizio AWS IoT non corrisponde, l'aggiornamento viene rifiutato con errore `VersionConflictException` e viene restituita una risposta `ErrorResponse` che contiene i dati sullo stato di esecuzione del processo corrente. Questo comportamento rende inutile una richiesta `DescribeJobExecution` separata per ottenere i dati sullo stato dell'esecuzione del processo.

**statusDetails**

Opzionale. Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo.

Risposta:

```
{
}
```

CLI (3)

Riepilogo:

```
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]
```

Formato di `cli-input-json`:

```
{
 "jobId": "string",
 "thingName": "string",
 "force": boolean,
 "expectedVersion": long,
 "statusDetails": {
 "string": "string"
 }
}
```

}

#### Campi di `cli-input-json`:

| Nome            | Tipo                                                                  | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId           | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+   | Il processo da annullare.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| thingName       | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Il nome dell'oggetto di cui verrà annullata l'esecuzione del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| force           | booleano                                                              | <p>Opzionale. Se <code>true</code>, l'esecuzione del processo viene annullata se ha uno stato di <code>IN_PROGRESS</code> o <code>QUEUED</code>. Altrimenti, l'esecuzione del processo viene annullata solo se ha uno stato <code>QUEUED</code>. Tuttavia, se si tenta di annullare l'esecuzione di un processo con stato <code>IN_PROGRESS</code> e non si imposta <code>--force</code> su <code>true</code>, viene generata un'eccezione <code>InvalidStateException</code>. Il valore di default è <code>false</code>.</p> <p><b>Warning</b></p> <p>L'annullamento di un processo con stato <code>IN_PROGRESS</code> impedirà al dispositivo che esegue il processo di aggiornarne lo stato di esecuzione del processo. Prestare attenzione e verificare che tutti i dispositivi in cui sono in esecuzione processi annullati siano in grado di effettuare il ripristino a uno stato valido.</p> |
| expectedVersion | Long<br>Classe Java: <code>java.lang.Long</code>                      | Opzionale. Versione corrente prevista dell'esecuzione del processo. Ogni volta che aggiorni l'esecuzione del processo, la versione viene incrementata. Se la versione dell'esecuzione del processo archiviata nel servizio AWS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Nome                       | Tipo                                                                                  | Descrizione                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            |                                                                                       | IoT Jobs non corrisponde, l'aggiornamento viene rifiutato con errore <code>VersionMismatch</code> e viene restituita una risposta <code>ErrorResponse</code> che contiene i dati sullo stato di esecuzione del processo corrente. Questo comportamento rende inutile una richiesta <code>DescribeJobExecution</code> separata per ottenere i dati sullo stato dell'esecuzione del processo. |
| <code>statusDetails</code> | mappa<br><br>Chiave: <code>DetailsKey</code><br><br>Valore: <code>DetailsValue</code> | Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo. Se non è specificato, <code>statusDetails</code> resta invariato.                                                                                                                                                                                                                                      |
| <code>DetailsKey</code>    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_]+          |                                                                                                                                                                                                                                                                                                                                                                                             |
| <code>DetailsValue</code>  | Stringa<br><br>Lunghezza max: 1024, min.: 1<br><br>Modello: [^\p{C}]*+                |                                                                                                                                                                                                                                                                                                                                                                                             |

Output:

Nessuna  
MQTT (3)

Non disponibile.

## CreateJob

CreateJob command

Crea un processo. È possibile fornire il documento del processo come collegamento a un file in un bucket Amazon S3 (parametro `documentSource`) oppure nel corpo della richiesta (parametro `document`).

Un processo può essere reso continuo impostando il parametro `targetSelection` opzionale su `CONTINUOUS`. (Il valore di default è `SNAPSHOT`.) Un processo continuo può essere usato per l'onboarding o l'aggiornamento dei dispositivi quando vengono aggiunti a un gruppo perché rimane in esecuzione e viene eseguito quando vengono aggiunti nuovi oggetti, anche dopo che gli oggetti presenti nel gruppo al momento della creazione del processo hanno completato il processo.

Un processo può avere un `TimeoutConfig` opzionale, che imposta il valore del timer in corso. Il timer in corso non può essere aggiornato e viene applicato a tutte le esecuzioni del processo.

## Note

La caratteristica di timeout del processo non è attualmente disponibile nella regione PDT (us-gov-west-1).

Negli argomenti per l'API `CreateJob` vengono eseguite le convalide seguenti:

- L'argomento `targets` deve essere un elenco di ARN di oggetti o gruppi di oggetti validi. Tutti gli oggetti e i gruppi di oggetti devono trovarsi nell'account AWS.
- L'argomento `documentSource` deve essere un URL Amazon S3 valido per un documento del processo. Gli URL Amazon S3 presentano il formato: `https://s3.amazonaws.com/bucketName/objectName`.
- Il documento archiviato nell'URL specificato dall'argomento `documentSource` deve essere un documento JSON con codifica UTF-8.
- La dimensione di un documento del processo non può essere superiore a 32 KB, a causa dei limiti relativi alle dimensioni dei messaggi MQTT (128 KB) e della crittografia.
- `jobId` deve essere univoco nell'account AWS.

## HTTPS (4)

Richiesta:

```
PUT /jobs/jobId

{
 "targets": ["string"],
 "document": "string",
 "documentSource": "string",
 "description": "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
 }
]
 },
 "timeoutConfig": {
 "inProgressTimeoutInMinutes": long
 }
}
```

**jobId**

Identificatore del processo, che deve essere univoco per l'account AWS. È consigliabile usare un UUID. Qui è possibile usare caratteri alfanumerici "-" e "\_".

**targets**

Elenco di ARN di oggetti o gruppi di oggetti che definiscono i target del processo.

**document**

Opzionale. Documento del processo.

**documentSource**

Opzionale. Collegamento Amazon S3 al documento del processo.

**description**

Opzionale. Breve descrizione di testo del processo.

**presignedUrlConfigData**

Opzionale. Informazioni di configurazione per URL Amazon S3 prefirmati.

**roleArn**

ARN del ruolo IAM che contiene le autorizzazioni di accesso al bucket Amazon S3. Si tratta del bucket che contiene i dati che i dispositivi scaricano con gli URL Amazon S3 prefirmati. Questo ruolo deve anche concedere ad AWS IoT l'autorizzazione per assumere il ruolo. Per ulteriori informazioni, consulta [Creazione di processi \(p. 373\)](#).

**expiresInSec**

Periodo di validità (in secondi) degli URL prefirmati. I valori validi sono compresi tra 60 e 3600. Il valore predefinito è 3600 secondi. Gli URL prefirmati vengono generati quando il servizio AWS IoT Jobs riceve una richiesta MQTT per il documento del processo.

**targetSelection**

Opzionale. Specifica se l'esecuzione del processo continua (CONTINUOUS) o se il processo viene completato dopo che tutti gli oggetti specificati come target hanno completato il processo (SNAPSHOT). Se il valore è CONTINUOUS, il processo può anche essere pianificato per essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un processo è pianificato per essere eseguito in un oggetto quando l'oggetto viene aggiunto a un gruppo target, anche dopo che il processo è stato completato da tutti gli oggetti originariamente nel gruppo.

**jobExecutionRolloutConfig**

Opzionale. Permette di creare un'implementazione per fasi di un processo.

**maximumPerMinute**

Numero massimo di oggetti in cui il processo viene inviato per l'esecuzione, per ogni minuto. I valori validi sono compresi tra 1 e 1000. Se il valore non viene specificato, viene usato il valore predefinito 1000. Il numero effettivo di oggetti che ricevono il processo può essere inferiore in un determinato intervallo di un minuto (a causa della latenza di sistema), ma non è mai superiore al valore specificato.

**exponentialRate**

Consente di creare una velocità esponenziale di rollout per un processo.

**baseRatePerMinute**

Il numero minimo di oggetti che ricevono una notifica di un processo in sospeso, ogni minuto, all'inizio del rollout di processo. Questo parametro consente di definire la velocità iniziale di un rollout.

**incrementFactor**

Il fattore esponenziale per aumentare la velocità di rollout per un processo.

**rateIncreaseCriteria**

I criteri per avviare l'aumento della velocità di rollout per un processo. Imposta i valori per `numberOfNotifiedThings` oppure `numberOfSucceededThings`, ma non entrambi.  
`numberOfNotifiedThings`

La soglia per il numero di oggetti notificati che avvia l'aumento della velocità di rollout.

`numberOfSucceededThings`

La soglia per il numero di oggetti completati che avvia l'aumento della velocità di rollout.

**abortConfig**

Opzionale. Dettagli dei criteri di interruzione per interrompere il processo.

**criteriaList**

L'elenco dei criteri di eliminazione per definire regole per interrompere il processo.

**action**

Il tipo di operazione di eliminazione per avviare l'interruzione di un processo.

**failureType**

Il tipo di errore di esecuzione di processo per definire una regola di avvio dell'interruzione di un processo.

**minNumberOfExecutedThings**

Il numero minimo di oggetti eseguiti prima della valutazione della regola di interruzione.

**thresholdPercentage**

La soglia come percentuale del numero totale di oggetti eseguiti che iniziano l'interruzione di un processo.

**timeoutConfig**

Opzionale. Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione del processo. Il timer viene avviato quando imposti lo stato di esecuzione del processo su `IN_PROGRESS`. Se lo stato di esecuzione del processo non è impostato su un altro stato terminale prima della scadenza del tempo a disposizione, viene automaticamente impostato su `TIMED_OUT`.

**Note**

La caratteristica di timeout del processo non è attualmente disponibile nella regione PDT (us-gov-west-1).

**inProgressTimeoutInMinutes**

Specifica l'intervallo di tempo, in minuti, a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Un timer viene avviato o riavviato ogni volta che lo stato di questa esecuzione del processo viene specificato come `IN_PROGRESS`, con il campo compilato. Se lo stato di esecuzione del processo non viene impostato su uno stato terminale prima del timeout o prima che un altro aggiornamento dello stato di esecuzione del processo venga inviato con il campo compilato, lo stato viene impostato su `TIMED_OUT`.

Risposta:

```
{
 "jobArn": "string",
 "jobId": "string",
 "description": "string"
}
```

**jobArn**

ARN del processo.

**jobId**

Identificatore univoco assegnato al processo.

**description**

Breve descrizione di testo facoltativa del processo.

#### CLI (4)

Riepilogo:

```
aws iot create-job \
 --job-id <value> \
 --targets <value> \
 [--document-source <value>] \
 [--document <value>] \
 [--description <value>] \
 [--presigned-url-config <value>] \
 [--target-selection <value>] \
 [--job-executions-rollout-config <value>] \
 [--abort-config <value>] \
 [--timeout-config <value>] \
 [--document-parameters <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "jobId": "string",
 "targets": [
 "string"
],
 "documentSource": "string",
 "document": "string",
 "description": "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"
 }
 }
 }
}

```

**Campi di `cli-input-json`:**

| Nome               | Tipo                                                                     | Descrizione                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId              | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-zA-Z0-9_-]+ | Identificatore del processo, che deve essere univoco per l'account AWS. È consigliabile usare un UUID. I caratteri alfanumerici, "-" e "_" sono i caratteri validi da usare qui.                                                                           |
| targets            | elenco<br><br>Membro: TargetArn                                          | Elenco di oggetti e gruppi di oggetti cui deve essere inviato il processo.                                                                                                                                                                                 |
| TargetArn          | Stringa                                                                  |                                                                                                                                                                                                                                                            |
| documentSource     | Stringa<br><br>Lunghezza max: 1350, min.: 1                              | Collegamento S3 al documento del processo.                                                                                                                                                                                                                 |
| document           | Stringa<br><br>Lunghezza max: 32768                                      | Documento del processo.                                                                                                                                                                                                                                    |
| description        | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+             | Breve descrizione di testo del processo.                                                                                                                                                                                                                   |
| presignedUrlConfig | PresignedUrlConfig                                                       | Informazioni di configurazione per URL S3 prefissati.                                                                                                                                                                                                      |
| roleArn            | Stringa<br><br>Lunghezza max: 2048, min.: 20                             | L'ARN di un ruolo IAM che concede l'autorizzazione per scaricare file dal bucket Amazon S3 in cui vengono archiviati i dati o gli aggiornamenti del processo. Il ruolo deve anche concedere l'autorizzazione affinché AWS IoT esegua il download dei file. |

| Nome                       | Tipo                                                                                | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| expiresInSec               | Long<br><br>Classe Java: java.lang.Long<br><br>Intervallo – Max: 3600, min.: 60     | Periodo di validità (in secondi) degli URL prefirmati. I valori validi sono compresi tra 60 e 3600. Il valore predefinito è 3600 secondi. Gli URL prefirmati vengono generati quando il servizio AWS IoT Jobs riceve una richiesta MQTT per il documento del processo.                                                                                                                                                                                                                                                 |
| targetSelection            | Stringa<br><br>Enumerazione: CONTINUOUS   SNAPSHOT                                  | Specifica se l'esecuzione del processo continua (CONTINUOUS) o se il processo viene completato dopo che tutti gli oggetti specificati come target hanno completato il processo (SNAPSHOT). Se è continuo, il processo può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un processo viene eseguito in un oggetto quando l'oggetto viene aggiunto a un gruppo target, anche dopo che il processo è stato completato da tutti gli oggetti originariamente nel gruppo. |
| jobExecutionsRolloutConfig | JobExecutionsRolloutConfig                                                          | Permette di creare un'implementazione per fasi del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| maximumPerMinute           | intero<br><br>Classe Java: java.lang.Integer<br><br>Intervallo – Max: 1000, min.: 1 | Numero massimo di oggetti che riceveranno una notifica di un processo in sospeso, ogni minuto. Questo parametro permette di creare un'implementazione per fasi.                                                                                                                                                                                                                                                                                                                                                        |
| exponentialRate            | ExponentialRolloutRate                                                              | La velocità di aumento di un rollout di processo. Questo parametro consente di definire una velocità esponenziale per un rollout di processo.                                                                                                                                                                                                                                                                                                                                                                          |
| baseRatePerMinute          | Classe Java: java.lang.Integer                                                      | Il numero minimo di oggetti che riceveranno una notifica di un processo in sospeso, ogni minuto all'inizio del rollout di processo. Questo parametro consente di definire la velocità iniziale di un rollout.                                                                                                                                                                                                                                                                                                          |

| Nome                      | Tipo                                                               | Descrizione                                                                                                                                                                                                                |
|---------------------------|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| incrementFactor           | java class: java.lang.Double                                       | Il fattore esponenziale per aumentare la velocità di rollout per un processo.                                                                                                                                              |
| rateIncreaseCriteria      | RateIncreaseCriteria                                               | Consente di definire un criterio per avviare l'aumento della velocità di rollout per un processo. Imposta un valore per <code>numberOfNotifiedThings</code> oppure <code>numberOfSucceededThings</code> , ma non entrambi. |
| numberOfNotifiedThings    | java class: java.lang.Double                                       | La soglia per il numero di oggetti notificati che avvierà l'aumento della velocità di rollout.                                                                                                                             |
| numberOfSucceededThings   | java class: java.lang.Double                                       | La soglia per il numero di oggetti completati che avvierà l'aumento della velocità di rollout.                                                                                                                             |
| abortConfig               | AbortConfig                                                        | Consente di creare criteri per interrompere un processo.                                                                                                                                                                   |
| criteriaList              | AbortCriteria                                                      | L'elenco dei criteri di eliminazione per definire regole per interrompere il processo.                                                                                                                                     |
| action                    | java class: java.lang.String (CANCEL)                              | Il tipo di operazione di eliminazione per avviare l'interruzione di un processo.                                                                                                                                           |
| failureType               | java class: java.lang.String (FAILED   REJECTED   TIMED_OUT   ALL) | Il tipo di errore di esecuzione di processo per definire una regola di avvio dell'interruzione di un processo.                                                                                                             |
| minNumberOfExecutedThings | java class: java.lang.Integer                                      | Il numero minimo di oggetti eseguiti prima della valutazione della regola di interruzione.                                                                                                                                 |
| thresholdPercentage       | java class: java.lang.Double                                       | La soglia come percentuale del numero totale di oggetti eseguiti che iniziano l'interruzione di un processo.<br><br>AWS IoT supporta fino a due cifre dopo il decimale (ad esempio, 10,9 e 10,99, ma non 10,999).          |

| Nome                       | Tipo                                                                       | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| timeoutConfig              | TimeoutConfig                                                              | <p>Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione del processo. Il timer viene avviato quando imposti lo stato di esecuzione del processo su <b>IN_PROGRESS</b>. Se lo stato di esecuzione del processo non è impostato su un altro stato terminale prima della scadenza del tempo a disposizione, viene automaticamente impostato su <b>TIMED_OUT</b>.</p> <p><b>Note</b></p> <p>La caratteristica di timeout del processo non è attualmente disponibile nella regione PDT (us-gov-west-1).</p>                   |
| inProgressTimeoutInMinutes | Long                                                                       | Specifica l'intervallo di tempo, in minuti, a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Un timer viene avviato o riavviato ogni volta che lo stato di questa esecuzione del processo viene specificato come <b>IN_PROGRESS</b> , con il campo compilato. Se lo stato di esecuzione del processo non viene impostato su uno stato terminale prima del timeout o prima che un altro aggiornamento dello stato di esecuzione del processo venga inviato con il campo compilato, lo stato viene impostato su <b>TIMED_OUT</b> . |
| documentParameters         | mappa<br><br>Chiave: ParameterKey<br><br>Valore: ParameterValue            | Parametri per il documento del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ParameterKey               | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z0-9:_-]+ |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Nome           | Tipo                                                                  | Descrizione |
|----------------|-----------------------------------------------------------------------|-------------|
| ParameterValue | Stringa<br><br>Lunghezza max: 1024, min.: 1<br><br>Modello: [^\p{C}]+ |             |

Output:

```
{
 "jobArn": "string",
 "jobId": "string",
 "description": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome        | Tipo                                                                     | Descrizione                                   |
|-------------|--------------------------------------------------------------------------|-----------------------------------------------|
| jobArn      | Stringa                                                                  | ARN del processo.                             |
| jobId       | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-zA-Z0-9_-]+ | Identificatore univoco assegnato al processo. |
| description | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+             | Descrizione del processo.                     |

## MQTT (4)

Non disponibile.

## DeleteJob

### DeleteJob command

Elimina un processo e le relative esecuzioni.

L'eliminazione di un processo potrebbe richiedere del tempo, a seconda del numero di esecuzioni create per il processo e di altri fattori. Mentre il processo viene eliminato, lo stato del processo viene indicato come "DELETION\_IN\_PROGRESS". Il tentativo di eliminare o annullare un processo il cui stato è già "DELETION\_IN\_PROGRESS" restituirà un errore.

## HTTPS (5)

Sintassi della richiesta:

```
DELETE /jobs/jobID?force=force
```

Parametri della richiesta URI:

| Nome  | Tipo      | Obbligatorio? | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------|-----------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId | JobId     | sì            | L'ID del processo da eliminare.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| force | ForceFlag | no            | <p>(Opzionale)<br/>         Quando true, è possibile eliminare l'esecuzione di un processo con stato "IN_PROGRESS". Altrimenti, è possibile eliminare solo un processo che è in uno stato terminale ("SUCCEEDED" o "CANCELED") o si verifica un'eccezione. Il valore predefinito è false.</p> <p><b>Note</b></p> <p>L'eliminazione di un processo con stato "IN_PROGRESS" impedirà al dispositivo in cui è in esecuzione il processo di accedere alle informazioni sul processo o di aggiornarne lo stato di esecuzione. Prestare attenzione e verificare che tutti i dispositivi in cui sono in esecuzione processi eliminati siano in grado di effettuare il ripristino a uno stato valido.</p> |

Errori:

#### InvalidRequestException

I contenuti della richiesta non sono validi. Ad esempio, questo codice viene restituito quando una richiesta UpdateJobExecution contiene dettagli sullo stato non validi. Il messaggio contiene dettagli sull'errore.

Codice di risposta HTTP: 400

#### InvalidStateException

Un aggiornamento ha tentato di modificare il processo o l'esecuzione del processo impostando uno stato non valido in base al suo stato corrente (ad esempio, un tentativo di modificare una richiesta con stato SUCCEEDED impostando lo stato IN\_PROGRESS). In questo caso, il corpo del messaggio di errore contiene anche il campo executionState.

Codice di risposta HTTP: 409

#### ResourceNotFoundException

La risorsa specificata non esiste.

Codice di risposta HTTP: 404

#### ThrottlingException

La velocità supera il limite.

Codice di risposta HTTP: 429

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

Codice di risposta HTTP: 503

### CLI (5)

Riepilogo:

```
aws iot delete-job \
 --job-id <value> \
 [--force | --no-force] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "jobId": "string",
 "force": boolean
}
```

Campi di **cli-input-json**:

| Nome  | Tipo     | Descrizione                                                                              |
|-------|----------|------------------------------------------------------------------------------------------|
| jobId | Stringa  | L'ID del processo da eliminare.<br>Lunghezza max: 64, min.: 1<br>Modello: [a-zA-Z0-9_-]+ |
| force | booleano | (Opzionale) Quando true, è possibile eliminare l'esecuzione                              |

| Nome | Tipo | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |      | <p>di un processo con stato IN_PROGRESS. Altrimenti, è possibile eliminare solo un processo che è in uno stato terminale (SUCCEEDED o CANCELED) o si verifica un'eccezione. Il valore predefinito è false.</p> <p><b>Note</b></p> <p>L'eliminazione di un processo con stato IN_PROGRESS impedirà al dispositivo in cui è in esecuzione il processo di accedere alle informazioni sul processo o di aggiornarne lo stato di esecuzione. Prestare attenzione e verificare che tutti i dispositivi in cui sono in esecuzione processi eliminati siano in grado di effettuare il ripristino a uno stato valido.</p> |

Output:

Nessuna  
MQTT (5)  
Non disponibile.

## DeleteJobExecution

DeleteJobExecution command

Elimina l'esecuzione di un processo.

HTTPS (6)

Sintassi della richiesta:

```
DELETE /things/thingName/jobs/jobId/executionNumber/executionNumber?force=force
```

Parametri della richiesta URI:

| Nome  | Tipo  | Obbligatorio? | Descrizione                                            |
|-------|-------|---------------|--------------------------------------------------------|
| jobId | JobId | sì            | L'ID del processo di cui verrà eliminata l'esecuzione. |

| Nome            | Tipo            | Obbligatorio? | Descrizione                                                                                                                                                                                                                                                                                                               |
|-----------------|-----------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingName       | ThingName       | sì            | Il nome dell'oggetto di cui verrà eliminata l'esecuzione del processo.                                                                                                                                                                                                                                                    |
| executionNumber | ExecutionNumber | sì            | L'ID dell'esecuzione del processo da eliminare.                                                                                                                                                                                                                                                                           |
| force           | ForceFlag       | no            | (Opzionale) Quando true, è possibile eliminare l'esecuzione di un processo con stato IN_PROGRESS. Altrimenti, è possibile eliminare solo l'esecuzione di un processo che è in uno stato terminale (SUCCEEDED, FAILED, TIMED_OUT, REJECTED, REMOVED o CANCELED) o si verifica un'eccezione. Il valore predefinito è false. |

Errori:

#### InvalidRequestException

I contenuti della richiesta non sono validi. Ad esempio, questo codice viene restituito quando una richiesta UpdateJobExecution contiene dettagli sullo stato non validi. Il messaggio contiene dettagli sull'errore.

Codice di risposta HTTP: 400

#### InvalidStateException

Un aggiornamento ha tentato di modificare l'esecuzione del processo impostando uno stato non valido in base allo stato corrente dell'esecuzione del processo (ad esempio, un tentativo di modificare una richiesta con stato SUCCEEDED impostando lo stato IN\_PROGRESS). In questo caso, il corpo del messaggio di errore contiene anche il campo executionState.

Codice di risposta HTTP: 409

#### ResourceNotFoundException

La risorsa specificata non esiste.

Codice di risposta HTTP: 404

#### ThrottlingException

La velocità supera il limite.

Codice di risposta HTTP: 429

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

Codice di risposta HTTP: 503

### CLI (6)

Riepilogo:

```
aws iot delete-job-execution \
--job-id <value> \
--thing-name <value> \
--execution-number <value> \
[--force | --no-force] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di cli-input-json:

```
{
 "jobId": "string",
 "thingName": "string",
 "executionNumber": long,
 "force": boolean
}
```

Campi di **cli-input-json**:

| Nome  | Tipo    | Descrizione                                                                          |
|-------|---------|--------------------------------------------------------------------------------------|
| jobId | Stringa | L'ID del processo di cui verrà eliminata l'esecuzione.<br>Lunghezza max: 64, min.: 1 |

| Nome            | Tipo                                                                          | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | Modello: [a–z A–Z 0–9 _]+                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| thingName       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Il nome dell'oggetto di cui verrà eliminata l'esecuzione del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| executionNumber | Long<br><br>Classe Java: java.lang.Long                                       | L'ID dell'esecuzione del processo da eliminare.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| force           | booleano                                                                      | <p>(Opzionale) Quando true, è possibile eliminare l'esecuzione di un processo con stato IN_PROGRESS. Altrimenti, è possibile eliminare solo l'esecuzione di un processo che è in uno stato terminale (SUCCEEDED, FAILED, TIMED_OUT, REJECTED, REMOVED o CANCELED) o si verifica un'eccezione. Il valore predefinito è false.</p> <p><b>Note</b></p> <p>L'eliminazione dell'esecuzione di un processo con stato IN_PROGRESS impedisce al dispositivo di accedere alle informazioni sul processo o di aggiornarne lo stato di esecuzione. Prestare attenzione e verificare che il dispositivo sia in grado di effettuare il ripristino a uno stato valido.</p> |

Output:

Nessuna

MQTT (6)

Non disponibile.

## DescribeJob

DescribeJob command

Ottiene i dettagli del processo specificato.

## HTTPS (7)

Richiesta:

```
GET /jobs/jobId
```

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

Risposta:

```
{
 "documentSource": "string",
 "job": Job
}
```

**documentSource**

Collegamento Amazon S3 al documento del processo.

**job**

Oggetto [Processo \(p. 394\)](#).

## CLI (7)

Riepilogo:

```
aws iot describe-job \
 --job-id <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "jobId": "string"
}
```

Campi di **cli-input-json**:

| Nome  | Tipo                                                                     | Descrizione                                                              |
|-------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|
| jobId | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-zA-Z0-9_-]+ | Identificatore univoco assegnato al processo al momento della creazione. |

Output:

```
{
 "documentSource": "string",
 "job": {
 "jobArn": "string",
 "jobId": "string",
 "targetSelection": "string",
 },
}
```

```
"status": "string",
"forceCanceled": boolean,
"comment": "string",
"targets": [
 "string"
],
"description": "string",
"presignedUrlConfig": {
 "roleArn": "string",
 "expiresInSec": long
},
"jobExecutionsRolloutConfig": {
 "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
 }
]
},
"createdAt": "timestamp",
"lastUpdatedAt": "timestamp",
"completedAt": "timestamp",
"jobProcessDetails": {
 "processingTargets": [
 "string"
],
 "numberOfCanceledThings": "integer",
 "numberOfSucceededThings": "integer",
 "numberOfFailedThings": "integer",
 "numberOfRejectedThings": "integer",
 "numberOfQueuedThings": "integer",
 "numberOfInProgressThings": "integer",
 "numberOfRemovedThings": "integer",
 "numberOfTimedOutThings": "integer"
},
"documentParameters": {
 "string": "string"
},
"timeoutConfig": {
 "inProgressTimeoutInMinutes": number
}
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome           | Tipo                                    | Descrizione                                       |
|----------------|-----------------------------------------|---------------------------------------------------|
| documentSource | Stringa<br>Lunghezza max: 1350, min.: 1 | Collegamento Amazon S3 al documento del processo. |

| Nome            | Tipo                                                                       | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| job             | Processo                                                                   | Informazioni sul processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| jobArn          | Stringa                                                                    | ARN che identifica il processo in formato "arn:aws:iot:regione:account:processo/jobId".                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| jobId           | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+ | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| targetSelection | Stringa<br><br>Enumerazione: CONTINUOUS   SNAPSHOT                         | Specifica se l'esecuzione del processo continua (CONTINUOUS) o se il processo viene completato dopo che tutti gli oggetti specificati come target hanno completato il processo (SNAPSHOT). Se è continuo, il processo può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un processo viene eseguito in un dispositivo quando l'oggetto che rappresenta il dispositivo viene aggiunto a un gruppo target, anche dopo che il processo è stato completato da tutti gli oggetti originariamente nel gruppo. |
| stato           | Stringa<br><br>enumerazione: IN_PROGRESS   CANCELED   SUCCEEDED            | Stato del processo, tra IN_PROGRESS, CANCELED e SUCCEEDED.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| forceCanceled   | booleano<br><br>Classe Java: java.lang.Boolean                             | È true se il processo è stato annullato con il parametro opzionale force impostato su true.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| comment         | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+               | Se il processo è stato aggiornato, descrive il motivo dell'aggiornamento.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| targets         | elenco<br><br>Membro: TargetArn                                            | Elenco di oggetti e gruppi di oggetti AWS IoT cui deve essere inviato il processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| TargetArn       | Stringa                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Nome                       | Tipo                                                                                | Descrizione                                                                                                                                                                                                                                                                 |
|----------------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| description                | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+                        | Breve descrizione di testo del processo.                                                                                                                                                                                                                                    |
| presignedUrlConfig         | PresignedUrlConfig                                                                  | Configurazione per gli URL Amazon S3 prefirmati.                                                                                                                                                                                                                            |
| roleArn                    | Stringa<br><br>Lunghezza max: 2048, min.: 20                                        | L'ARN di un ruolo IAM che concede l'autorizzazione per scaricare file dal bucket Amazon S3 in cui vengono archiviati i dati o gli aggiornamenti del processo. Il ruolo deve anche concedere l'autorizzazione affinché il servizio AWS IoT Jobs esegua il download dei file. |
| expiresInSec               | Long<br><br>Classe Java: java.lang.Long<br><br>Intervallo – Max: 3600, min.: 60     | Periodo di validità (in secondi) degli URL prefirmati. I valori validi sono compresi tra 60 e 3600. Il valore predefinito è 3600 secondi. Gli URL prefirmati vengono generati quando il servizio AWS IoT Jobs riceve una richiesta MQTT per il documento del processo.      |
| jobExecutionsRolloutConfig | JobExecutionsRolloutConfig                                                          | Permette di creare un'implementazione per fasi del processo.                                                                                                                                                                                                                |
| maximumPerMinute           | intero<br><br>Classe Java: java.lang.Integer<br><br>Intervallo – Max: 1000, min.: 1 | Numero massimo di oggetti che riceveranno una notifica di un processo in sospeso, ogni minuto. Questo parametro permette di creare un'implementazione per fasi.                                                                                                             |
| exponentialRate            | ExponentialRolloutRate                                                              | La velocità di aumento di un rollout di processo. Questo parametro consente di definire una velocità esponenziale per un rollout di processo.                                                                                                                               |
| baseRatePerMinute          | Classe Java: java.lang.Integer                                                      | Il numero minimo di oggetti che ricevono una notifica di un processo in sospeso, ogni minuto, all'inizio del rollout di processo. Questo parametro consente di definire la velocità iniziale di un rollout.                                                                 |

| Nome                      | Tipo                                                               | Descrizione                                                                                                                                                                                                                |
|---------------------------|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| incrementFactor           | java class: java.lang.Double                                       | Il fattore esponenziale per aumentare la velocità di rollout per un processo.                                                                                                                                              |
| rateIncreaseCriteria      | RateIncreaseCriteria                                               | Consente di definire un criterio per avviare l'aumento della velocità di rollout per un processo. Imposta un valore per <code>numberOfNotifiedThings</code> oppure <code>numberOfSucceededThings</code> , ma non entrambi. |
| numberOfNotifiedThings    | java class: java.lang.Double                                       | La soglia per il numero di oggetti notificati che avvia l'aumento della velocità di rollout.                                                                                                                               |
| numberOfSucceededThings   | java class: java.lang.Double                                       | La soglia per il numero di oggetti completati che avvia l'aumento della velocità di rollout.                                                                                                                               |
| abortConfig               | AbortConfig                                                        | Consente di creare criteri per interrompere un processo.                                                                                                                                                                   |
| criteriaList              | AbortCriteria                                                      | L'elenco dei criteri di eliminazione per definire regole per interrompere il processo.                                                                                                                                     |
| action                    | java class: java.lang.String (CANCEL)                              | Il tipo di operazione di eliminazione per avviare l'interruzione di un processo.                                                                                                                                           |
| failureType               | java class: java.lang.String (FAILED   REJECTED   TIMED_OUT   ALL) | Il tipo di errore di esecuzione di processo per definire una regola di avvio dell'interruzione di un processo.                                                                                                             |
| minNumberOfExecutedThings | java class: java.lang.Integer                                      | Il numero minimo di oggetti eseguiti prima della valutazione della regola di interruzione.                                                                                                                                 |
| thresholdPercentage       | java class: java.lang.Double                                       | La soglia come percentuale del numero totale di oggetti eseguiti che iniziano l'interruzione di un processo.<br><br>AWS IoT supporta fino a due cifre dopo il decimale (ad esempio, 10,9 e 10,99, ma non 10,999).          |
| createdAt                 | Timestamp                                                          | Periodo di tempo, in secondi, dall'epoca (Unix epoch) alla creazione del processo.                                                                                                                                         |

| Nome                     | Tipo                                                                             | Descrizione                                                                                                                                                        |
|--------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lastUpdatedAt            | timestamp                                                                        | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento del processo.                                                                       |
| completedAt              | timestamp                                                                        | Periodo di tempo, in secondi, dall'epoca al completamento del processo.                                                                                            |
| jobProcessDetails        | JobProcessDetails                                                                | Dettagli sull'elaborazione del processo.                                                                                                                           |
| processingTargets        | elenco<br><br>Membro:<br>ProcessingTargetName<br><br>Classe Java: java.util.List | Dispositivi in cui il processo è in esecuzione.                                                                                                                    |
| ProcessingTargetName     | Stringa                                                                          |                                                                                                                                                                    |
| numberOfCanceledThings   | intero<br><br>Classe Java: java.lang.Integer                                     | Numero di oggetti che hanno annullato il processo.                                                                                                                 |
| numberOfSucceededThings  | intero<br><br>Classe Java: java.lang.Integer                                     | Numero di oggetti che hanno completato con successo il processo.                                                                                                   |
| numberOfFailedThings     | intero<br><br>Classe Java: java.lang.Integer                                     | Numero di oggetti che non hanno eseguito il processo.                                                                                                              |
| numberOfRejectedThings   | intero<br><br>Classe Java: java.lang.Integer                                     | Numero di oggetti che hanno rifiutato il processo.                                                                                                                 |
| numberOfQueuedThings     | intero<br><br>Classe Java: java.lang.Integer                                     | Numero di oggetti che sono in attesa dell'esecuzione del processo.                                                                                                 |
| numberOfInProgressThings | intero<br><br>Classe Java: java.lang.Integer                                     | Numero di oggetti che stanno attualmente eseguendo il processo.                                                                                                    |
| numberOfRemovedThings    | intero<br><br>Classe Java: java.lang.Integer                                     | Numero di oggetti per cui non è più pianificata l'esecuzione del processo, perché sono stati eliminati o rimossi dal gruppo che costituiva un target del processo. |
| numberOfTimedOutThings   | intero<br><br>Classe Java: java.lang.Integer                                     | Il numero di oggetti il cui stato di esecuzione del processo è <b>TIMED_OUT</b> .                                                                                  |

| Nome               | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| documentParameters | mappa<br><br>Chiave: ParameterKey<br><br>Valore: ParameterValue              | Parametri specificati per il documento del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ParameterKey       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z 0-9 :_-]+ |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ParameterValue     | Stringa<br><br>Lunghezza max: 1024, min.: 1<br><br>Modello: [^\p{C}]+        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| timeoutConfig      | TimeoutConfig                                                                | <p>Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione del processo. Viene avviato un timer quando imposta lo stato di esecuzione del processo su <b>IN_PROGRESS</b>. Se lo stato di esecuzione del processo non è impostato su un altro stato terminale prima della scadenza del timer, viene automaticamente impostato su <b>TIMED_OUT</b>.</p> <p><b>Note</b></p> <p>La caratteristica di timeout del processo non è attualmente disponibile nella regione PDT (us-gov-west-1).</p> |

| Nome                       | Tipo | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| inProgressTimeoutInMinutes | Long | Specifica l'intervallo di tempo, in minuti, a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. L'intervallo di timeout può essere compreso fra 1 minuto e 7 giorni (da 1 a 10080 minuti). Il timer in corso non può essere aggiornato e viene applicato a tutte le esecuzioni del processo. Se l'esecuzione del processo resta nello stato <code>IN_PROGRESS</code> per un periodo di tempo superiore a quello consentito dall'intervallo, l'esecuzione del processo non va a buon fine e viene impostato lo stato <code>TIMED_OUT</code> terminale. |

## MQTT (7)

Non disponibile.

## DescribeJobExecution

### DescribeJobExecution command

Ottiene i dettagli di un'esecuzione del processo. Lo stato dell'esecuzione del processo deve essere `SUCCEEDED` o `FAILED`.

### HTTPS (8)

Richiesta:

```
GET /things/thingName/jobs/jobId?executionNumber=executionNumber
```

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

**thingName**

Nome dell'oggetto associato al dispositivo in cui è in corso l'esecuzione del processo.

**executionNumber**

Opzionale. Numero utilizzato per specificare l'esecuzione di un processo in un dispositivo. (Consulta [JobExecution \(p. 398\)](#).) Se non è specificato, viene restituita l'ultima esecuzione del processo.

Risposta:

```
{
 "execution": { JobExecution }
```

}

#### execution

Oggetto [JobExecution \(p. 398\)](#).

#### CLI (8)

Riepilogo:

```
aws iot describe-job-execution \
--job-id <value> \
--thing-name <value> \
[--execution-number <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`:

```
{
 "jobId": "string",
 "thingName": "string",
 "executionNumber": long
}
```

Campi di `cli-input-json`:

| Nome            | Tipo                                                                      | Descrizione                                                                                                                                        |
|-----------------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId           | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-zA-Z0-9_-]+  | Identificatore univoco assegnato al processo al momento della creazione.                                                                           |
| thingName       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z0-9_-]+ | Nome dell'oggetto in cui è in corso l'esecuzione del processo.                                                                                     |
| executionNumber | Long<br><br>Classe Java: java.lang.Long                                   | Stringa (costituita dalle cifre comprese tra "0" e "9") usata per specificare l'esecuzione di un determinato processo in un dispositivo specifico. |

Output:

```
{
 "execution": {
 "approximateSecondsBeforeTimedOut": "number"
 "jobId": "string",
 "status": "string",
 "forceCanceled": boolean,
 "statusDetails": {
 "detailsMap": {
 "string": "string"
 }
 }
 }
}
```

```

 },
 "thingArn": "string",
 "queuedAt": "timestamp",
 "startedAt": "timestamp",
 "lastUpdatedAt": "timestamp",
 "executionNumber": long,
 "versionNumber": long
}
}

```

Campi di output dell'interfaccia a riga di comando:

| Nome                             | Tipo                                                                                                               | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| execution                        | JobExecution                                                                                                       | Informazioni sull'esecuzione del processo.                                                                                                                                                                                                                                                                                                                                                                       |
| approximateSecondsBeforeTimedOut | long                                                                                                               | Il numero stimato di secondi che rimangono prima che lo stato di esecuzione del processo venga modificato in TIMED_OUT. L'intervallo di timeout può essere compreso fra 1 minuto e 7 giorni (da 1 a 10080 minuti). L'effettivo timeout dell'esecuzione del processo può verificarsi 60 secondi dopo la durata stimata. Questo valore non è incluso se l'esecuzione del processo ha raggiunto lo stato terminale. |
| jobId                            | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-zA-Z0-9_-]+                                           | Identificatore univoco assegnato al processo quando è stato creato.                                                                                                                                                                                                                                                                                                                                              |
| stato                            | Stringa<br><br>enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED | Stato dell'esecuzione del processo (IN_PROGRESS, QUEUED, FAILED, SUCCEEDED, TIMED_OUT, CANCELED o REJECTED).                                                                                                                                                                                                                                                                                                     |
| forceCanceled                    | booleano<br><br>Classe Java: java.lang.Boolean                                                                     | È true se l'esecuzione del processo è stata annullata con il parametro opzionale force impostato su true.                                                                                                                                                                                                                                                                                                        |
| statusDetails                    | JobExecutionStatusDetails                                                                                          | Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo.                                                                                                                                                                                                                                                                                                                             |
| detailsMap                       | mappa<br><br>Chiave: DetailsKey<br><br>Valore: DetailsValue                                                        | Stato di esecuzione del processo.                                                                                                                                                                                                                                                                                                                                                                                |

| Nome            | Tipo                                                                         | Descrizione                                                                                                                                                                                                                          |
|-----------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DetailsKey      | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_]+ |                                                                                                                                                                                                                                      |
| DetailsValue    | Stringa<br><br>Lunghezza max: 1024, min.: 1<br><br>Modello: [^\p{C}]*+       |                                                                                                                                                                                                                                      |
| thingArn        | Stringa                                                                      | ARN dell'oggetto in cui è in corso l'esecuzione del processo.                                                                                                                                                                        |
| queuedAt        | timestamp                                                                    | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                                                                           |
| startedAt       | timestamp                                                                    | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                                                                                        |
| lastUpdatedAt   | timestamp                                                                    | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                                                                                         |
| executionNumber | Long<br><br>Classe Java: java.lang.Long                                      | Stringa (costituita dalle cifre comprese tra "0" e "9") che identifica l'esecuzione di questo processo in questo dispositivo. Può essere usata in comandi che restituiscono o aggiornano le informazioni di esecuzione del processo. |
| versionNumber   | Long                                                                         | Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che vengono aggiornate da un dispositivo.                                                                           |

## MQTT (8)

Non disponibile.

## GetJobDocument

GetJobDocument command

Ottiene il documento per un processo.

### Note

Gli URL segnaposto non vengono sostituiti con URL Amazon S3 prefirmati nel documento restituito. Gli URL prefirmati vengono generati solo quando il servizio AWS IoT Jobs riceve una richiesta tramite MQTT.

## HTTPS (9)

Richiesta:

```
GET /jobs/jobId/job-document
```

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

Risposta:

```
{
 "document": "string"
}
```

**document**

Contenuto del documento del processo.

## CLI (9)

Riepilogo:

```
aws iot get-job-document \
 --job-id <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "jobId": "string"
}
```

Campi di **cli-input-json**:

| Nome         | Tipo                                                             | Descrizione                                                                    |
|--------------|------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <b>jobId</b> | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a-zA-Z0-9_-]+ | Identificatore univoco<br>assegnato al processo al<br>momento della creazione. |

Output:

```
{
 "document": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome     | Tipo                            | Descrizione                           |
|----------|---------------------------------|---------------------------------------|
| document | Stringa<br>Lunghezza max: 32768 | Contenuto del documento del processo. |

## MQTT (9)

Non disponibile.

## ListJobExecutionsForJob

ListExecutionsForJob command

Ottiene un elenco delle esecuzioni per un processo.

## HTTPS (10)

Richiesta:

```
GET /jobs/jobId/things?status=status&maxResults=maxResults&nextToken=nextToken
```

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

**status**

Opzionale. Filtro che permette di cercare i processi con lo stato specificato: QUEUED, IN\_PROGRESS, SUCCEEDED, FAILED, TIMED\_OUT, REJECTED, REMOVED o CANCELED.

**maxResults**

Opzionale. Numero massimo di risultati da restituire per ogni richiesta.

**nextToken**

Opzionale. Token usato per recuperare il successivo set di risultati.

Risposta:

```
{
 "executionSummaries": [JobExecutionSummary ...]
}
```

**executionSummaries**

Elenco di oggetti [JobExecutionSummary](#) (p. 399) associati a un job ID specificato.

## CLI (10)

Riepilogo:

```
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]
```

Formato di **cli-input-json**:

```
{
 "jobId": "string",
 "status": "string",
 "maxResults": "integer",
 "nextToken": "string"
}
```

Campi di **cli-input-json**:

| Nome       | Tipo                                                                                                               | Descrizione                                                              |
|------------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| jobId      | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+                                         | Identificatore univoco assegnato al processo al momento della creazione. |
| stato      | Stringa<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED | Stato del processo.                                                      |
| maxResults | intero<br><br>Classe Java: java.lang.Integer<br><br>Intervallo – Max: 250, min.: 1                                 | Numero massimo di risultati da restituire per ogni richiesta.            |
| nextToken  | Stringa                                                                                                            | Token usato per recuperare il successivo set di risultati.               |

Output:

```
{
 "executionSummaries": [
 {
 "thingArn": "string",
 "jobExecutionSummary": {
 "status": "string",
 "queuedAt": "timestamp",
 "startedAt": "timestamp",
 "lastUpdatedAt": "timestamp",
 "executionNumber": long
 }
 }
],
 "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome                      | Tipo                                                                                                               | Descrizione                                                                                                                                                                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| executionSummaries        | elenco<br><br>Membro:<br>JobExecutionSummaryForJob<br><br>Classe Java: java.util.List                              | Elenco dei riepiloghi di esecuzione del processo.                                                                                                                                                                                                      |
| JobExecutionSummaryForJob | JobExecutionSummaryForJob                                                                                          |                                                                                                                                                                                                                                                        |
| thingArn                  | Stringa                                                                                                            | ARN dell'oggetto in cui è in corso l'esecuzione del processo.                                                                                                                                                                                          |
| jobExecutionSummary       | JobExecutionSummary                                                                                                | Contiene un sottoinsieme delle informazioni sull'esecuzione di un processo.                                                                                                                                                                            |
| stato                     | Stringa<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED | Stato dell'esecuzione del processo.                                                                                                                                                                                                                    |
| queuedAt                  | timestamp                                                                                                          | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione della coda.                                                                                                                                                         |
| startedAt                 | timestamp                                                                                                          | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                                                                                                          |
| lastUpdatedAt             | timestamp                                                                                                          | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                                                                                                           |
| executionNumber           | Long<br><br>Classe Java: java.lang.Long                                                                            | Stringa (costituita dalle cifre comprese tra "0" e "9") che identifica l'esecuzione di questo processo in questo dispositivo. Può essere usato successivamente in comandi che restituiscono o aggiornano le informazioni sull'esecuzione del processo. |
| nextToken                 | Stringa                                                                                                            | Token per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi.                                                                                                                                                              |

## MQTT (10)

Non disponibile.

## ListJobExecutionsForThing

### ListJobExecutionsForThing command

Ottiene un elenco delle esecuzioni di un processo per un oggetto.

#### HTTPS (11)

Richiesta:

```
GET /things/thingName/jobs?status=status&maxResults=maxResults&nextToken=nextToken
```

**thingName**

Nome dell'oggetto per cui verrà creato l'elenco JobExecutions.

**status**

Filtro opzionale che permette di cercare i processi con lo stato specificato: QUEUED, IN\_PROGRESS, SUCCEEDED, FAILED, TIMED\_OUT, REJECTED, REMOVED o CANCELED.

**maxResults**

Numero massimo di risultati da restituire per ogni richiesta.

**nextToken**

Token per il successivo set di risultati oppure `null` se non ci sono risultati aggiuntivi.

Risposta:

```
{
 "executionSummaries": [JobExecutionSummary ...]
}
```

**executionSummaries**

Elenco degli oggetti [JobExecutionSummary \(p. 399\)](#) delle esecuzioni del processo associate all'oggetto specificato.

#### CLI (11)

Riepilogo:

```
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]
```

Formato di `cli-input-json`:

```
{
 "thingName": "string",
 "status": "string",
 "maxResults": "integer",
 "nextToken": "string"
}
```

Campi di **cli-input-json**:

| Nome       | Tipo                                                                                                               | Descrizione                                                                       |
|------------|--------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| thingName  | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+                                      | Nome dell'oggetto.                                                                |
| stato      | Stringa<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED | Filtro opzionale che permette di cercare processi che hanno lo stato specificato. |
| maxResults | intero<br><br>Classe Java: java.lang.Integer<br><br>Intervallo – Max: 250, min.: 1                                 | Numero massimo di risultati da restituire per ogni richiesta.                     |
| nextToken  | Stringa                                                                                                            | Token usato per recuperare il successivo set di risultati.                        |

Output:

```
{
 "executionSummaries": [
 {
 "jobId": "string",
 "jobExecutionSummary": {
 "status": "string",
 "queuedAt": "timestamp",
 "startedAt": "timestamp",
 "lastUpdatedAt": "timestamp",
 "executionNumber": long
 }
 }
],
 "nextToken": "string"
}
```

Campi di output CLI:

| Nome               | Tipo                                                 | Descrizione                                       |
|--------------------|------------------------------------------------------|---------------------------------------------------|
| executionSummaries | elenco<br><br>Membro:<br>JobExecutionSummaryForThing | Elenco dei riepiloghi di esecuzione del processo. |

| Nome                        | Tipo                                                                                                           | Descrizione                                                                                                                                                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | Classe Java: java.util.List                                                                                    |                                                                                                                                                                                                                                                        |
| JobExecutionSummaryForThing | JobExecutionSummaryForThing                                                                                    |                                                                                                                                                                                                                                                        |
| jobId                       | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a–z A–Z 0–9 _]+                                             | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                                                                               |
| jobExecutionSummary         | JobExecutionSummary                                                                                            | Contiene un sottoinsieme delle informazioni sull'esecuzione di un processo.                                                                                                                                                                            |
| stato                       | Stringa<br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED | Stato dell'esecuzione del processo.                                                                                                                                                                                                                    |
| queuedAt                    | timestamp                                                                                                      | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                                                                                             |
| startedAt                   | timestamp                                                                                                      | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                                                                                                          |
| lastUpdatedAt               | timestamp                                                                                                      | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                                                                                                           |
| executionNumber             | Long<br>Classe Java: java.lang.Long                                                                            | Stringa (costituita dalle cifre comprese tra "0" e "9") che identifica l'esecuzione di questo processo in questo dispositivo. Può essere usato successivamente in comandi che restituiscono o aggiornano le informazioni sull'esecuzione del processo. |
| nextToken                   | Stringa                                                                                                        | Token per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi.                                                                                                                                                              |

## MQTT (11)

Non disponibile.

## ListJobs

ListJobs command

Ottiene un elenco dei processi nell'account AWS.

HTTPS (12)

Richiesta:

```
GET /jobs?
status=status&targetSelection=targetSelection&thingGroupName=thingGroupName&thingGroupId=thingGroupId
```

**status**

Opzionale. Filtro che permette di cercare i processi con lo stato specificato: IN\_PROGRESS, CANCELED o SUCCEEDED.

**targetSelection**

Opzionale. Filtro che permette di cercare i processi con il valore targetSelection specificato: CONTINUOUS o SNAPSHOT.

**thingGroupName**

Opzionale. Filtro che permette di cercare i processi con il nome del gruppo di oggetti specificato come target.

**thingGroupId**

Opzionale. Filtro che permette di cercare i processi con l'ID del gruppo di oggetti specificato come target.

**maxResults**

Opzionale. Numero massimo di risultati da restituire per ogni richiesta.

**nextToken**

Opzionale. Token usato per recuperare il successivo set di risultati.

Risposta:

```
{
 "jobs": [JobSummary ...],
}
```

**jobs**

Elenco di oggetti [JobSummary \(p. 397\)](#), uno per ogni processo nell'account AWS che corrisponde ai criteri di filtro specificati.

CLI (12)

Riepilogo:

```
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]
```

Formato di **cli-input-json**:

```
{
 "status": "string",
 "targetSelection": "string",
 "maxResults": "integer",
 "nextToken": "string",
 "thingGroupName": "string",
 "thingGroupId": "string"
}
```

Campi di **cli-input-json**:

| Nome            | Tipo                                                                               | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| stato           | Stringa<br><br>enumerazione: IN_PROGRESS   CANCELED   SUCCEEDED                    | Filtro opzionale che permette di cercare processi che hanno lo stato specificato.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| targetSelection | Stringa<br><br>Enumerazione: CONTINUOUS   SNAPSHOT                                 | Specifica se l'esecuzione del processo continua (CONTINUOUS) o se il processo viene completato dopo che tutti gli oggetti specificati come target hanno completato il processo (SNAPSHOT). Se è continuo, il processo può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un processo viene eseguito in un oggetto quando l'oggetto viene aggiunto a un gruppo target, anche dopo che il processo è stato completato da tutti gli oggetti originariamente nel gruppo. |
| maxResults      | intero<br><br>Classe Java: java.lang.Integer<br><br>Intervallo – Max: 250, min.: 1 | Numero massimo di risultati da restituire per ogni richiesta.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| nextToken       | Stringa                                                                            | Token usato per recuperare il successivo set di risultati.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| thingGroupName  | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z 0-9 :_-]+       | Filtro che limita i processi restituiti a quelli per il gruppo specificato.                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Nome         | Tipo                                                                | Descrizione                                                                 |
|--------------|---------------------------------------------------------------------|-----------------------------------------------------------------------------|
| thingGroupId | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 -]+ | Filtro che limita i processi restituiti a quelli per il gruppo specificato. |

Output:

```
{
 "jobs": [
 {
 "jobArn": "string",
 "jobId": "string",
 "thingGroupId": "string",
 "targetSelection": "string",
 "status": "string",
 "createdAt": "timestamp",
 "lastUpdatedAt": "timestamp",
 "completedAt": "timestamp"
 }
],
 "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome            | Tipo                                                                | Descrizione                                                                                                                                                                                               |
|-----------------|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobs            | elenco<br>Membro: JobSummary<br>Classe Java: java.util.List         | Elenco di processi.                                                                                                                                                                                       |
| JobSummary      | JobSummary                                                          |                                                                                                                                                                                                           |
| jobArn          | Stringa                                                             | ARN del processo.                                                                                                                                                                                         |
| jobId           | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a–z A–Z 0–9 -]+  | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                                  |
| thingGroupId    | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 -]+ | ID del gruppo di oggetti.                                                                                                                                                                                 |
| targetSelection | Stringa<br>Enumerazione: CONTINUOUS   SNAPSHOT                      | Specifica se l'esecuzione del processo continua (CONTINUOUS) o se il processo viene completato dopo che tutti gli oggetti specificati come target hanno completato il processo (SNAPSHOT). Se è continuo, |

| Nome          | Tipo                                                        | Descrizione                                                                                                                                                                                                                                                                                                  |
|---------------|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                             | il processo può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un processo viene eseguito in un oggetto quando l'oggetto viene aggiunto a un gruppo target, anche dopo che il processo è stato completato da tutti gli oggetti originariamente nel gruppo. |
| stato         | Stringa<br>enumerazione: IN_PROGRESS   CANCELED   SUCCEEDED | Stato di riepilogo del processo.                                                                                                                                                                                                                                                                             |
| createdAt     | Timestamp                                                   | Periodo di tempo, in secondi, dall'epoca (Unix epoch) alla creazione del processo.                                                                                                                                                                                                                           |
| lastUpdatedAt | timestamp                                                   | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento del processo.                                                                                                                                                                                                                 |
| completedAt   | timestamp                                                   | Periodo di tempo, in secondi, dall'epoca al completamento del processo.                                                                                                                                                                                                                                      |
| nextToken     | Stringa                                                     | Token per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi.                                                                                                                                                                                                                    |

## MQTT (12)

Non disponibile.

## UpdateJob

### UpdateJob command

Aggiorna i campi supportati del processo specificato. I valori aggiornati per `timeoutConfig` diventano effettivi solo per le nuove esecuzioni in corso. Attualmente le esecuzioni in corso continuano con la configurazione di timeout precedente.

## HTTPS (13)

Richiesta:

```
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
 }
}
```

#### jobId

Un identificatore del processo che deve essere univoco per l'account AWS. È consigliabile usare un UUID. Qui è possibile usare caratteri alfanumerici "-" e "\_".

#### description

Opzionale. Breve descrizione di testo del processo.

#### presignedUrlConfigData

Opzionale. Informazioni di configurazione per URL Amazon S3 prefirmati.

#### roleArn

ARN del ruolo IAM che contiene le autorizzazioni di accesso al bucket Amazon S3. Si tratta del bucket che contiene i dati che i dispositivi scaricano con gli URL Amazon S3 prefirmati. Questo ruolo deve anche concedere ad AWS IoT l'autorizzazione per assumere il ruolo. Per ulteriori informazioni, consulta [Creazione di processi \(p. 373\)](#).

#### expiresInSec

Periodo di validità (in secondi) degli URL prefirmati. I valori validi sono compresi tra 60 e 3600. Il valore predefinito è 3600 secondi. Gli URL prefirmati vengono generati quando il servizio AWS IoT Jobs riceve una richiesta MQTT per il documento del processo.

#### jobExecutionRolloutConfig

Opzionale. Permette di creare un'implementazione per fasi di un processo.

#### maximumPerMinute

Numero massimo di oggetti in cui il processo viene inviato per l'esecuzione, per ogni minuto. I valori validi sono compresi tra 1 e 1000. Se il valore non viene specificato, viene usato il valore predefinito 1000. Il numero effettivo di oggetti che ricevono il processo può essere inferiore in un determinato intervallo di un minuto (a causa della latenza di sistema), ma non è mai superiore al valore specificato.

#### exponentialRate

Consente di creare una velocità esponenziale di rollout per un processo.

**baseRatePerMinute**

Il numero minimo di oggetti che ricevono una notifica di un processo in sospeso, ogni minuto, all'inizio del rollout di processo. Questo parametro consente di definire la velocità iniziale di un rollout.

**incrementFactor**

Il fattore esponenziale per aumentare la velocità di rollout per un processo.

**rateIncreaseCriteria**

I criteri per avviare l'aumento della velocità di rollout per un processo. Imposta i valori per `numberOfNotifiedThings` oppure `numberOfSucceededThings`, ma non entrambi.

**numberOfNotifiedThings**

La soglia per il numero di oggetti notificati che avvia l'aumento della velocità di rollout.

**numberOfSucceededThings**

La soglia per il numero di oggetti completati che avvia l'aumento della velocità di rollout.

**abortConfig**

Opzionale. Dettagli dei criteri di interruzione per interrompere il processo.

**criteriaList**

L'elenco dei criteri di eliminazione per definire regole per interrompere il processo.

**action**

Il tipo di operazione di eliminazione per avviare l'interruzione di un processo.

**failureType**

Il tipo di errore di esecuzione di processo per definire una regola di avvio dell'interruzione di un processo.

**minNumberOfExecutedThings**

Il numero minimo di oggetti eseguiti prima della valutazione della regola di interruzione.

**thresholdPercentage**

La soglia come percentuale del numero totale di oggetti eseguiti che iniziano l'interruzione di un processo.

**timeoutConfig**

Opzionale. Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione del processo. Il timer viene avviato quando imposti lo stato di esecuzione del processo su `IN_PROGRESS`. Se lo stato di esecuzione del processo non è impostato su un altro stato terminale prima della scadenza del tempo a disposizione, viene automaticamente impostato su `TIMED_OUT`.

**inProgressTimeoutInMinutes**

Specifica l'intervallo di tempo, in minuti, a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Un timer viene avviato o riavviato ogni volta che lo stato di questa esecuzione del processo viene specificato come `IN_PROGRESS`, con il campo compilato. Se lo stato di esecuzione del processo non viene impostato su uno stato terminale prima del timeout o prima che un altro aggiornamento dello stato di esecuzione del processo venga inviato con il campo compilato, lo stato viene impostato su `TIMED_OUT`.

Risposta:

HTTP/1.1 200

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

CLI (13)

Riepilogo:

```
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]
```

Formato di **cli-input-json**:

```
{
 "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
 }
}
```

Campi di **cli-input-json**:

| Nome  | Tipo                                                                     | Descrizione                                                                                                                                                                        |
|-------|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-zA-Z0-9_-]+ | Un identificatore del processo che deve essere univoco per l'account AWS. È consigliabile usare un UUID. I caratteri alfanumerici, "-" e "_" sono i caratteri validi da usare qui. |

| Nome                       | Tipo                                                                                | Descrizione                                                                                                                                                                                                                                                            |
|----------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| description                | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+                        | Breve descrizione di testo del processo.                                                                                                                                                                                                                               |
| presignedUrlConfig         | PresignedUrlConfig                                                                  | Informazioni di configurazione per URL S3 prefirmati.                                                                                                                                                                                                                  |
| roleArn                    | Stringa<br><br>Lunghezza max: 2048, min.: 20                                        | L'ARN di un ruolo IAM che concede l'autorizzazione per scaricare file dal bucket S3 in cui vengono archiviati i dati o gli aggiornamenti del processo. Il ruolo deve anche concedere l'autorizzazione affinché AWS IoT esegua il download dei file.                    |
| expiresInSec               | Long<br><br>Classe Java: java.lang.Long<br><br>Intervallo – Max: 3600, min.: 60     | Periodo di validità (in secondi) degli URL prefirmati. I valori validi sono compresi tra 60 e 3600. Il valore predefinito è 3600 secondi. Gli URL prefirmati vengono generati quando il servizio AWS IoT Jobs riceve una richiesta MQTT per il documento del processo. |
| jobExecutionsRolloutConfig | JobExecutionsRolloutConfig                                                          | Permette di creare un'implementazione per fasi del processo.                                                                                                                                                                                                           |
| maximumPerMinute           | intero<br><br>Classe Java: java.lang.Integer<br><br>Intervallo – Max: 1000, min.: 1 | Numero massimo di oggetti che riceveranno una notifica di un processo in sospeso, ogni minuto. Questo parametro permette di creare un'implementazione per fasi.                                                                                                        |
| exponentialRate            | ExponentialRolloutRate                                                              | La velocità di aumento di un rollout di processo. Questo parametro consente di definire una velocità esponenziale per un rollout di processo.                                                                                                                          |
| baseRatePerMinute          | Classe Java: java.lang.Integer                                                      | Il numero minimo di oggetti che ricevono una notifica di un processo in sospeso, ogni minuto, all'inizio del rollout di processo. Questo parametro consente di definire la velocità iniziale di un rollout.                                                            |
| incrementFactor            | java class: java.lang.Double                                                        | Il fattore esponenziale per aumentare la velocità di rollout per un processo.                                                                                                                                                                                          |

| Nome                      | Tipo                                                               | Descrizione                                                                                                                                                                                                                |
|---------------------------|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rateIncreaseCriteria      | RateIncreaseCriteria                                               | Consente di definire un criterio per avviare l'aumento della velocità di rollout per un processo. Imposta un valore per <code>numberOfNotifiedThings</code> oppure <code>numberOfSucceededThings</code> , ma non entrambi. |
| numberOfNotifiedThings    | java class: java.lang.Double                                       | La soglia per il numero di oggetti notificati che avvia l'aumento della velocità di rollout.                                                                                                                               |
| numberOfSucceededThings   | java class: java.lang.Double                                       | La soglia per il numero di oggetti completati che avvia l'aumento della velocità di rollout.                                                                                                                               |
| abortConfig               | AbortConfig                                                        | Consente di creare criteri per interrompere un processo.                                                                                                                                                                   |
| criteriaList              | AbortCriteria                                                      | L'elenco dei criteri di eliminazione per definire regole per interrompere il processo.                                                                                                                                     |
| action                    | java class: java.lang.String (CANCEL)                              | Il tipo di operazione di eliminazione per avviare l'interruzione di un processo.                                                                                                                                           |
| failureType               | java class: java.lang.String (FAILED   REJECTED   TIMED_OUT   ALL) | Il tipo di errore di esecuzione di processo per definire una regola di avvio dell'interruzione di un processo.                                                                                                             |
| minNumberOfExecutedThings | java class: java.lang.Integer                                      | Il numero minimo di oggetti eseguiti prima della valutazione della regola di interruzione.                                                                                                                                 |
| thresholdPercentage       | java class: java.lang.Double                                       | La soglia come percentuale del numero totale di oggetti eseguiti che iniziano l'interruzione di un processo.<br><br>AWS IoT supporta fino a due cifre dopo il decimale (ad esempio, 10,9 e 10,99, ma non 10,999).          |

| Nome                       | Tipo                                                                       | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| timeoutConfig              | TimeoutConfig                                                              | <p>Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione del processo. Il timer viene avviato quando imposti lo stato di esecuzione del processo su <b>IN_PROGRESS</b>. Se lo stato di esecuzione del processo non è impostato su un altro stato terminale prima della scadenza del tempo a disposizione, viene automaticamente impostato su <b>TIMED_OUT</b>.</p> <p><b>Note</b></p> <p>La caratteristica di timeout del processo non è attualmente disponibile nella regione PDT (us-gov-west-1).</p>                   |
| inProgressTimeoutInMinutes | Long                                                                       | Specifica l'intervallo di tempo, in minuti, a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Un timer viene avviato o riavviato ogni volta che lo stato di questa esecuzione del processo viene specificato come <b>IN_PROGRESS</b> , con il campo compilato. Se lo stato di esecuzione del processo non viene impostato su uno stato terminale prima del timeout o prima che un altro aggiornamento dello stato di esecuzione del processo venga inviato con il campo compilato, lo stato viene impostato su <b>TIMED_OUT</b> . |
| documentParameters         | mappa<br><br>Chiave: ParameterKey<br><br>Valore: ParameterValue            | Parametri per il documento del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ParameterKey               | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z0-9:_-]+ |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Nome           | Tipo                                                                  | Descrizione |
|----------------|-----------------------------------------------------------------------|-------------|
| ParameterValue | Stringa<br><br>Lunghezza max: 1024, min.: 1<br><br>Modello: [^\p{C}]+ |             |

Output:

```
HTTP/1.1 200
```

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.  
MQTT (13)

Non disponibile.

## API MQTT e HTTPS per i dispositivi per il servizio Jobs

### Tipi di dati MQTT e HTTPS per i dispositivi

I tipi di dati seguenti vengono usati per comunicare con il servizio AWS IoT Jobs tramite i protocolli MQTT e HTTPS.

#### JobExecution

JobExecution data type

Contiene i dati sull'esecuzione di un processo.

syntax (7)

```
{
 "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
}
```

description (7)

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

**thingName**

Nome dell'oggetto che sta eseguendo il processo.

**jobDocument**

Contenuto del documento del processo.

**status**

Stato dell'esecuzione del processo. Può essere QUEUED, IN\_PROGRESS, FAILED, SUCCEEDED, CANCELED, TIMED\_OUT, REJECTED o REMOVED.

**statusDetails**

Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo.

**queuedAt**

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.

**startedAt**

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.

**lastUpdatedAt**

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.

**versionNumber**

Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che vengono aggiornate da un dispositivo.

**executionNumber**

Numero che identifica un'esecuzione di un processo in un dispositivo. Può essere usato successivamente in comandi che restituiscono o aggiornano le informazioni sull'esecuzione del processo.

## JobExecutionState

**JobExecutionState** data type

Contiene i dati sullo stato dell'esecuzione di un processo.

**syntax (8)**

```
{
 "status": "QUEUED|IN_PROGRESS|FAILED|SUCCEEDED|CANCELED|TIMED_OUT|REJECTED|
REMOVED",
 "statusDetails": {
 "string": "string"
 ...
 }
 "versionNumber": "number"
}
```

**description (8)**

**status**

Stato dell'esecuzione del processo. Può essere QUEUED, IN\_PROGRESS, FAILED, SUCCEEDED, CANCELED, TIMED\_OUT, REJECTED o REMOVED.

**statusDetails**

Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo.

#### versionNumber

Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che vengono aggiornate da un dispositivo.

### JobExecutionSummary

#### JobExecutionSummary data type

Contiene un sottoinsieme delle informazioni sull'esecuzione di un processo.

#### syntax (9)

```
{
 "jobId": "string",
 "queuedAt": timestamp,
 "startedAt": timestamp,
 "lastUpdatedAt": timestamp,
 "versionNumber": "number",
 "executionNumber": long
}
```

#### description (9)

##### jobId

Identificatore univoco assegnato al processo al momento della creazione.

##### queuedAt

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.

##### startedAt

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.

##### lastUpdatedAt

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.

##### versionNumber

Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che il servizio AWS IoT Jobs riceve un aggiornamento da un dispositivo.

##### executionNumber

Numero che identifica un'esecuzione di un processo in un dispositivo.

### ErrorResponse

#### ErrorResponse data type

Contiene informazioni su un errore che si è verificato durante un'operazione del servizio AWS IoT Jobs.

#### syntax (10)

```
{
 "code": "ErrorCode",
 "message": "string",
 "clientToken": "string",
 "timestamp": timestamp,
}
```

```
 "executionState": JobExecutionState
}
```

description (10)

code

ErrorCode può essere impostato su:

InvalidTopic

La richiesta è stata inviata a un argomento nel namespace di AWS IoT Jobs non mappato ad alcuna API.

InvalidJson

Non è stato possibile interpretare i contenuti della richiesta come contenuto JSON valido con codifica UTF-8.

InvalidRequest

I contenuti della richiesta non sono validi. Ad esempio, questo codice viene restituito quando una richiesta `UpdateJobExecution` contiene dettagli sullo stato non validi. Il messaggio contiene dettagli sull'errore.

InvalidStateTransition

Un aggiornamento ha tentato di modificare l'esecuzione del processo impostando uno stato non valido in base allo stato corrente dell'esecuzione del processo (ad esempio, un tentativo di modificare una richiesta con stato `SUCCEEDED` impostando lo stato `IN_PROGRESS`). In questo caso, il corpo del messaggio di errore contiene anche il campo `executionState`.

ResourceNotFound

Il valore di `JobExecution` specificato dall'argomento della richiesta non esiste.

VersionMismatch

La versione prevista specificata nella richiesta non corrisponde alla versione dell'esecuzione del processo nel servizio AWS IoT Jobs. In questo caso, il corpo del messaggio di errore contiene anche il campo `executionState`.

InternalError

Si è verificato un errore interno durante l'elaborazione della richiesta.

RequestThrottled

La richiesta è stata sottoposta a throttling.

TerminalStateReached

Si verifica quando viene eseguito un comando per descrivere un processo in un processo che si trova in uno stato terminale.

message

Stringa di messaggio di errore.

clientToken

Stringa arbitraria usata per mettere in relazione una richiesta con la relativa risposta.

timestamp

Tempo, in secondi, dall'epoca (Unix epoch).

executionState

Oggetto [JobExecutionState \(p. 454\)](#). Questo campo è incluso solo quando il campo `code` ha il valore `InvalidStateTransition` o `VersionMismatch`. In questi casi, non è necessario

eseguire una richiesta `DescribeJobExecution` separata per ottenere i dati sullo stato dell'esecuzione del processo corrente.

## Comandi per i dispositivi

I comandi seguenti sono disponibili tramite i protocolli MQTT e HTTPS.

### GetPendingJobExecutions

GetPendingJobExecutions command

Ottiene l'elenco di tutti i processi per un oggetto che non si trovano in uno stato terminale.  
MQTT (12)

Per richiamare quest'API, pubblica un messaggio in `$aws/things/thingName/jobs/get`.

Payload della richiesta:

```
{ "clientToken": "string" }
```

`clientToken`

Opzionale. Token client usato per mettere in relazione richieste e risposte. Immetti un valore arbitrario, che viene riportato nella risposta.

Per ricevere la risposta, sottoscrivi:

- `$aws/things/thingName/jobs/get/accepted` e
- `$aws/things/thingName/jobs/get/rejected` o
- `$aws/things/thingName/jobs/get/#` per entrambi.

Payload della risposta:

```
{
 "inProgressJobs" : [JobExecutionSummary ...],
 "queuedJobs" : [JobExecutionSummary ...],
 "timestamp" : 1489096425069,
 "clientToken" : "client-001"
}
```

`inProgressJobs`

Elenco di oggetti `JobExecutionSummary` (p. 455) con stato `IN_PROGRESS`.

`queuedJobs`

Elenco di oggetti `JobExecutionSummary` (p. 455) con stato `QUEUED`.

`clientToken`

Token client usato per mettere in relazione richieste e risposte.

`timestamp`

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'invio del messaggio.

HTTPS (12)

Richiesta:

```
GET /things/thingName/jobs
```

**thingName**

Nome dell'oggetto associato al dispositivo.

Risposta:

```
{
 "inProgressJobs" : [JobExecutionSummary ...],
 "queuedJobs" : [JobExecutionSummary ...]
}
```

**inProgressJobs**

Elenco di oggetti [JobExecutionSummary \(p. 455\)](#).

**queuedJobs**

Elenco di oggetti [JobExecutionSummary \(p. 455\)](#).

CLI (12)

Riepilogo:

```
aws iot-jobs-data get-pending-job-executions \
 --thing-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "thingName": "string"
}
```

Campi di **cli-input-json**:

| Nome      | Tipo                                                               | Descrizione                                      |
|-----------|--------------------------------------------------------------------|--------------------------------------------------|
| thingName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-zA-Z0-9:_-]+ | Nome dell'oggetto che sta eseguendo il processo. |

Output:

```
{
 "inProgressJobs": [
 {
 "jobId": "string",
 "queuedAt": long,
 "startedAt": long,
 "lastUpdatedAt": long,
 "versionNumber": long,
 "executionNumber": long
 }
]
```

```

],
 "queuedJobs": [
 {
 "jobId": "string",
 "queuedAt": long,
 "startedAt": long,
 "lastUpdatedAt": long,
 "versionNumber": long,
 "executionNumber": long
 }
]
 }
}

```

Campi di output dell'interfaccia a riga di comando:

| Nome                | Tipo                                                                            | Descrizione                                                                                                                                                                              |
|---------------------|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| inProgressJobs      | elenco<br><br>Membro:<br>JobExecutionSummary<br><br>Classe Java: java.util.List | Elenco di oggetti JobExecutionSummary con stato IN_PROGRESS.                                                                                                                             |
| JobExecutionSummary | JobExecutionSummary                                                             |                                                                                                                                                                                          |
| jobId               | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+      | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                 |
| queuedAt            | Long                                                                            | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                               |
| startedAt           | Long<br><br>Classe Java: java.lang.Long                                         | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                                            |
| lastUpdatedAt       | Long                                                                            | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                                             |
| versionNumber       | Long                                                                            | Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che il servizio AWS IoT Jobs riceve un aggiornamento da un dispositivo. |
| executionNumber     | Long<br><br>Classe Java: java.lang.Long                                         | Numero che identifica un'esecuzione di un processo in un dispositivo.                                                                                                                    |
| queuedJobs          | elenco                                                                          | Elenco di oggetti JobExecutionSummary con stato QUEUED.                                                                                                                                  |

| Nome                | Tipo                                                                       | Descrizione                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | Membro:<br>JobExecutionSummary<br><br>Classe Java: java.util.List          |                                                                                                                                                                                          |
| JobExecutionSummary | JobExecutionSummary                                                        |                                                                                                                                                                                          |
| jobId               | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a–z A–Z 0–9 _]+ | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                 |
| queuedAt            | Long                                                                       | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                               |
| startedAt           | Long<br><br>Classe Java: java.lang.Long                                    | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                                            |
| lastUpdatedAt       | Long                                                                       | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                                             |
| versionNumber       | Long                                                                       | Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che il servizio AWS IoT Jobs riceve un aggiornamento da un dispositivo. |
| executionNumber     | Long<br><br>Classe Java: java.lang.Long                                    | Numero che identifica un'esecuzione di un processo in un dispositivo.                                                                                                                    |

## StartNextPendingJobExecution

StartNextPendingJobExecution command

Ottiene e avvia l'esecuzione del processo in sospeso successiva (stato IN\_PROGRESS o QUEUED) per un oggetto.

- Le esecuzioni di un processo con stato IN\_PROGRESS vengono restituite per prime.
- Le esecuzioni di un processo vengono restituite in base all'ordine di creazione.
- Se l'esecuzione del processo in sospeso successiva ha stato QUEUED, il relativo stato viene modificato in IN\_PROGRESS e i dettagli dello stato dell'esecuzione del processo vengono impostati come specificato.
- Se l'esecuzione del processo in sospeso successiva ha già stato IN\_PROGRESS, i dettagli dello stato non vengono modificati.
- Se non sono presenti esecuzioni in sospeso, la risposta non include il campo `execution`.

- Se lo desideri, puoi creare un timer della fase impostando un valore per la proprietà `stepTimeoutInMinutes`. Se non aggiorni il valore di questa proprietà eseguendo `UpdateJobExecution`, il timeout dell'esecuzione del processo si verifica alla scadenza del timer della fase.

## MQTT (13)

Per richiamare quest'API, pubblica un messaggio in `$aws/things/thingName/jobs/start-next`.

Payload della richiesta:

```
{
 "statusDetails": {
 "string": "job-execution-state"
 ...
 },
 "stepTimeoutInMinutes": long,
 "clientToken": "string"
}
```

### statusDetails

Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo. Se non è specificato, `statusDetails` resta invariato.

### stepTimeOutInMinutes

Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Se lo stato di esecuzione del processo non è impostato su uno stato terminale prima del timeout o prima della reimpostazione del timer (chiamando `UpdateJobExecution`, impostando lo stato su `IN_PROGRESS` e specificando un nuovo valore di timeout nel campo `stepTimeoutInMinutes`), lo stato di esecuzione del processo viene impostato su `TIMED_OUT`. L'impostazione di questo timeout non ha alcun effetto sul timeout dell'esecuzione del processo, che potresti avere specificato al momento della creazione del processo (`CreateJob` utilizzando il campo `timeoutConfig`).

### clientToken

Token client usato per mettere in relazione richieste e risposte. Immetti un valore arbitrario, che viene riportato nella risposta.

Per ricevere la risposta, sottoscrivi:

- `$aws/things/thingName/jobs/start-next/accepted` e
- `$aws/things/thingName/jobs/start-next/rejected` o
- `$aws/things/thingName/jobs/start-next/#` per entrambi.

Payload della risposta:

```
{
 "execution" : JobExecutionData,
 "timestamp" : timestamp,
 "clientToken" : "string"
}
```

### execution

Oggetto [JobExecution \(p. 453\)](#). Ad esempio:

```
{
 "execution" : {
 "jobId" : "022",
 "thingName" : "MyThing",
 "jobDocument" : "< contents of job document >",
 "status" : "IN_PROGRESS",
 "queuedAt" : 1489096123309,
 "lastUpdatedAt" : 1489096123309,
 "versionNumber" : 1,
 "executionNumber" : 1234567890
 },
 "clientToken" : "client-1",
 "timestamp" : 1489088524284,
}
```

#### timestamp

Periodo di tempo, in millisecondi, dall'epoca (Unix epoch) all'invio del messaggio al dispositivo.

#### clientToken

Token client usato per mettere in relazione richieste e risposte.

## HTTPS (13)

#### Richiesta:

```
PUT /things/thingName/jobs/$next
{
 "statusDetails": {
 "string": "string"
 ...
 },
 "stepTimeoutInMinutes": long
}
```

#### thingName

Nome dell'oggetto associato al dispositivo.

#### statusDetails

Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo. Se non è specificato, statusDetails resta invariato.

#### stepTimeOutInMinutes

Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Se lo stato di esecuzione del processo non è impostato su uno stato terminale prima del timeout o prima della reimpostazione del timer (chiamando UpdateJobExecution, impostando lo stato su IN\_PROGRESS e specificando un nuovo valore di timeout nel campo stepTimeoutInMinutes), lo stato di esecuzione del processo viene impostato su TIMED\_OUT. L'impostazione di questo timeout non ha alcun effetto sul timeout dell'esecuzione del processo, che potresti avere specificato al momento della creazione del processo (CreateJob utilizzando il campo timeoutConfig).

#### Risposta:

```
{
```

```
 "execution" : JobExecution
 }
```

#### execution

Oggetto [JobExecution](#) (p. 453). Ad esempio:

```
{
 "execution" : {
 "jobId" : "022",
 "thingName" : "MyThing",
 "jobDocument" : "< contents of job document >",
 "status" : "IN_PROGRESS",
 "queuedAt" : 1489096123309,
 "lastUpdatedAt" : 1489096123309,
 "versionNumber" : 1,
 "executionNumber" : 1234567890
 },
 "clientToken" : "client-1",
 "timestamp" : 1489088524284,
}
```

### CLI (13)

Riepilogo:

```
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]
```

Formato di `cli-input-json`:

```
{
 "thingName": "string",
 "statusDetails": {
 "string": "string"
 },
 "stepTimeoutInMinutes": long
}
```

Campi di `cli-input-json`:

| Nome          | Tipo    | Descrizione                                                                                                                               |
|---------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------|
| thingName     | Stringa | Nome dell'oggetto associato al dispositivo.<br>Lunghezza max: 128, min.: 1<br>Modello: [a-zA-Z0-9:_-]+                                    |
| statusDetails | mappa   | Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo. Se non è specificato, statusDetails resta invariato. |

| Nome                 | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| stepTimeOutInMinutes | Long                                                                         | Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Se lo stato di esecuzione del processo non è impostato su uno stato terminale prima del timeout o prima della reimpostazione del timer (chiamando <code>UpdateJobExecution</code> , impostando lo stato su <code>IN_PROGRESS</code> e specificando un nuovo valore di timeout nel campo <code>stepTimeoutInMinutes</code> ), lo stato di esecuzione del processo viene impostato su <code>TIMED_OUT</code> . L'impostazione di questo timeout non ha alcun effetto sul timeout dell'esecuzione del processo, che potresti avere specificato al momento della creazione del processo ( <code>CreateJob</code> utilizzando il campo <code>timeoutConfig</code> ). |
| DetailsKey           | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z 0-9 :_-]+ |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| DetailsValue         | Stringa<br><br>Lunghezza max: 1024, min.: 1<br><br>Modello: [^\p{C}]*+       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

Output:

```
{
 "execution": {
 "jobId": "string",
 "thingName": "string",
 "status": "string",
 "statusDetails": {
 "string": "string"
 },
 "queuedAt": long,
 "startedAt": long,
 "lastUpdatedAt": long,
 "versionNumber": long,
 "executionNumber": long,
 "jobDocument": "string"
 }
}
```

}

Campi di output dell'interfaccia a riga di comando:

| Nome          | Tipo                                                                                                               | Descrizione                                                                                                                     |
|---------------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| execution     | JobExecution                                                                                                       | Oggetto JobExecution.                                                                                                           |
| jobId         | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+                                         | Identificatore univoco assegnato al processo al momento della creazione.                                                        |
| thingName     | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+                                      | Nome dell'oggetto che sta eseguendo il processo.                                                                                |
| stato         | Stringa<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED | Stato dell'esecuzione del processo. Può essere QUEUED, IN_PROGRESS, FAILED, SUCCEEDED, CANCELED, TIMED_OUT, REJECTED o REMOVED. |
| statusDetails | mappa<br><br>Chiave: DetailsKey<br><br>Valore: DetailsValue                                                        | Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo.                                            |
| DetailsKey    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+                                      |                                                                                                                                 |
| DetailsValue  | Stringa<br><br>Lunghezza max: 1024, min.: 1<br><br>Modello: [^\p{C}]*+                                             |                                                                                                                                 |
| queuedAt      | Long                                                                                                               | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                      |
| startedAt     | Long<br><br>Classe Java: java.lang.Long                                                                            | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                   |
| lastUpdatedAt | Long                                                                                                               | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                    |

| Nome            | Tipo                                | Descrizione                                                                                                                                                                                    |
|-----------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| versionNumber   | Long                                | Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che vengono aggiornate da un dispositivo.                                     |
| executionNumber | Long<br>Classe Java: java.lang.Long | Numero che identifica un'esecuzione di un processo in un dispositivo. Può essere usato successivamente in comandi che restituiscono o aggiornano le informazioni sull'esecuzione del processo. |
| jobDocument     | Stringa<br>Lunghezza max: 32768     | Contenuto del documento del processo.                                                                                                                                                          |

## DescribeJobExecution

### DescribeJobExecution command

Ottiene informazioni dettagliate sull'esecuzione di un processo.

Puoi impostare jobId su \$next per restituire l'esecuzione del processo in sospeso successiva (stato IN\_PROGRESS o QUEUED) per un oggetto.

#### MQTT (14)

Per richiamare quest'API, pubblica un messaggio in \$aws/things/*thingName*/jobs/*jobId*/get.

**Payload della richiesta:**

```
{
 "executionNumber": long,
 "includeJobDocument": boolean,
 "clientToken": "string"
}
```

**thingName**

Nome dell'oggetto associato al dispositivo.

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

In alternativa, utilizza \$next per restituire l'esecuzione del processo in sospeso successiva (stato IN\_PROGRESS o QUEUED) per un oggetto. In questo caso, le esecuzioni del processo con stato IN\_PROGRESS vengono restituite per prime. Le esecuzioni di un processo vengono restituite in base all'ordine di creazione.

**executionNumber**

Opzionale. Numero che identifica un'esecuzione di un processo in un dispositivo. Se non è specificato, viene restituita l'ultima esecuzione del processo.

`includeJobDocument`

Opzionale. A meno che non sia impostato su `false`, la risposta contiene il documento del processo. Il valore di default è `true`.

`clientToken`

Token client usato per mettere in relazione richieste e risposte. Immetti un valore arbitrario, che viene riportato nella risposta.

Per ricevere la risposta, sottoscrivi:

- `$aws/things/thingName/jobs/jobId/get/accepted` e
- `$aws/things/thingName/jobs/jobId/get/rejected` o
- `$aws/things/thingName/jobs/jobId/get/#` per entrambi.

Payload della risposta:

```
{
 "execution" : JobExecutionData,
 "timestamp": "timestamp",
 "clientToken": "string"
}
```

`execution`

Oggetto [JobExecution \(p. 453\)](#).

`timestamp`

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'invio del messaggio.

`clientToken`

Token client usato per mettere in relazione richieste e risposte.

## HTTPS (14)

Lo stato dell'esecuzione del processo deve essere `QUEUED` o `IN_PROGRESS`.

Richiesta:

```
GET /things/thingName/jobs/jobId?
executionNumber=executionNumber&includeJobDocument=includeJobDocument
```

`thingName`

Nome dell'oggetto associato al dispositivo.

`jobId`

Identificatore univoco assegnato al processo al momento della creazione.

In alternativa, utilizza `$next` per restituire l'esecuzione del processo in sospeso successiva (stato `IN_PROGRESS` o `QUEUED`) per un oggetto. In questo caso, le esecuzioni del processo con stato `IN_PROGRESS` vengono restituite per prime. Le esecuzioni di un processo vengono restituite in base all'ordine di creazione.

**includeJobDocument**

Opzionale. A meno che non sia impostato su `false`, la risposta contiene il documento del processo. Il valore di default è `true`.

**executionNumber**

Opzionale. Numero che identifica un'esecuzione di un processo in un dispositivo. Se non è specificato, viene restituita l'ultima esecuzione del processo.

Risposta:

```
{
 "execution" : JobExecution,
}
```

**execution**

Oggetto [JobExecution \(p. 453\)](#).

**CLI (14)**

Lo stato dell'esecuzione del processo deve essere `QUEUED` o `IN_PROGRESS`.

Riepilogo:

```
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]
```

Formato di `cli-input-json`:

```
{
 "jobId": "string",
 "thingName": "string",
 "includeJobDocument": boolean,
 "executionNumber": long
}
```

Campi di `cli-input-json`:

| Nome  | Tipo                                           | Descrizione                                                                                                                                                                                                                                                                                         |
|-------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId | Stringa<br><br>Modello: [a-zA-Z0-9_-]+ ^\$next | L'identificatore univoco assegnato a questo processo quando è stato creato oppure \$next per restituire l'esecuzione del processo in sospeso successiva (stato IN_PROGRESS o QUEUED) per un oggetto. In questo caso, le esecuzioni del processo con stato IN_PROGRESS vengono restituite per prime. |

| Nome               | Tipo                                                                 | Descrizione                                                                                                                                               |
|--------------------|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    |                                                                      | Le esecuzioni di un processo vengono restituite in base all'ordine di creazione.                                                                          |
| thingName          | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+ | Nome dell'oggetto associato al dispositivo in cui è in corso l'esecuzione del processo.                                                                   |
| includeJobDocument | booleano<br>Classe Java: java.lang.Boolean                           | Opzionale. A meno che non sia impostato su false, la risposta contiene il documento del processo. Il valore predefinito è true.                           |
| executionNumber    | Long<br>Classe Java: java.lang.Long                                  | Opzionale. Numero che identifica un'esecuzione di un processo in un dispositivo. Se non è specificato, viene restituita l'ultima esecuzione del processo. |

Output:

```
{
 "execution": {
 "jobId": "string",
 "thingName": "string",
 "status": "string",
 "statusDetails": {
 "string": "string"
 },
 "queuedAt": long,
 "startedAt": long,
 "lastUpdatedAt": long,
 "versionNumber": long,
 "executionNumber": long,
 "jobDocument": "string"
 }
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome      | Tipo                                                                | Descrizione                                                              |
|-----------|---------------------------------------------------------------------|--------------------------------------------------------------------------|
| execution | JobExecution                                                        | Contiene i dati sull'esecuzione di un processo.                          |
| jobId     | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+ | Identificatore univoco assegnato al processo al momento della creazione. |
| thingName | Stringa<br>Lunghezza max: 128, min.: 1                              | Nome dell'oggetto che sta eseguendo il processo.                         |

| Nome            | Tipo                                                                                                               | Descrizione                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | Modello: [a-z A-Z 0-9 :_-]+                                                                                        |                                                                                                                                                                                                |
| stato           | Stringa<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED | Stato dell'esecuzione del processo. Può essere QUEUED, IN_PROGRESS, FAILED, SUCCEEDED, CANCELED, TIMED_OUT, REJECTED o REMOVED.                                                                |
| statusDetails   | mappa<br><br>Chiave: DetailsKey<br><br>Valore: DetailsValue                                                        | Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo.                                                                                                           |
| DetailsKey      | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+                                      |                                                                                                                                                                                                |
| DetailsValue    | Stringa<br><br>Lunghezza max: 1024, min.: 1<br><br>Modello: [^\p{C}]*+                                             |                                                                                                                                                                                                |
| queuedAt        | Long                                                                                                               | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                                     |
| startedAt       | Long<br><br>Classe Java: java.lang.Long                                                                            | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                                                  |
| lastUpdatedAt   | Long                                                                                                               | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                                                   |
| versionNumber   | Long                                                                                                               | Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che vengono aggiornate da un dispositivo.                                     |
| executionNumber | Long<br><br>Classe Java: java.lang.Long                                                                            | Numero che identifica un'esecuzione di un processo in un dispositivo. Può essere usato successivamente in comandi che restituiscono o aggiornano le informazioni sull'esecuzione del processo. |

| Nome        | Tipo                                | Descrizione                           |
|-------------|-------------------------------------|---------------------------------------|
| jobDocument | Stringa<br><br>Lunghezza max: 32768 | Contenuto del documento del processo. |

## UpdateJobExecution

UpdateJobExecution command

Aggiorna lo stato dell'esecuzione di un processo. Se lo desideri, puoi creare un timer della fase impostando un valore per la proprietà `stepTimeoutInMinutes`. Se non aggiorni il valore di questa proprietà eseguendo nuovamente `UpdateJobExecution`, il timeout dell'esecuzione del processo si verifica alla scadenza del timer della fase.

MQTT (15)

Per richiamare quest'API, pubblica un messaggio in `$aws/things/thingName/jobs/jobID/update`.

Payload della richiesta:

```
{
 "status": "job-execution-state",
 "statusDetails": {
 "string": "string"
 ...
 },
 "expectedVersion": "number",
 "executionNumber": long,
 "includeJobExecutionState": boolean,
 "includeJobDocument": boolean,
 "stepTimeoutInMinutes": long,
 "clientToken": "string"
}
```

**status**

Nuovo stato per l'esecuzione del processo (IN\_PROGRESS, FAILED, SUCCEEDED o REJECTED). Questo valore deve essere specificato per ogni aggiornamento.

**statusDetails**

Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo. Se non è specificato, `statusDetails` resta invariato.

**expectedVersion**

Versione corrente prevista dell'esecuzione del processo. Ogni volta che aggiorni l'esecuzione del processo, la versione viene incrementata. Se la versione dell'esecuzione del processo archiviata nel servizio AWS IoT Jobs non corrisponde, l'aggiornamento viene rifiutato con errore `VersionMismatch` e viene restituita una risposta [ErrorResponse \(p. 455\)](#) che contiene i dati sullo stato di esecuzione del processo corrente. Questo comportamento rende inutile una richiesta `DescribeJobExecution` separata per ottenere i dati sullo stato dell'esecuzione del processo.

**executionNumber**

Opzionale. Numero che identifica un'esecuzione di un processo in un dispositivo. Se non è specificato, viene usata l'ultima esecuzione del processo.

**includeJobExecutionState**

Opzionale. Quando è incluso e impostato su `true`, la risposta contiene il campo `JobExecutionState`. Il valore di default è `false`.

**includeJobDocument**

Opzionale. Quando è incluso e impostato su `true`, la risposta contiene `JobDocument`. Il valore di default è `false`.

**stepTimeoutInMinutes**

Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Se lo stato di esecuzione del processo non è impostato su uno stato terminale prima del timeout o prima della reimpostazione del timer (chiamando nuovamente `UpdateJobExecution`, impostando lo stato su `IN_PROGRESS` e specificando un nuovo valore di timeout in questo campo), lo stato di esecuzione del processo viene impostato su `TIMED_OUT`. L'impostazione o la reimpostazione di questo timeout non ha alcun effetto su quello dell'esecuzione del processo che potresti avere specificato al momento della creazione del processo (utilizzando `CreateJob` con `timeoutConfig`).

**clientToken**

Token client usato per mettere in relazione richieste e risposte. Immetti un valore arbitrario, che viene riportato nella risposta.

Per ricevere la risposta, sottoscriviti:

- `$aws/things/thingName/jobs/jobId/update/accepted` e
- `$aws/things/thingName/jobs/jobId/update/rejected` o
- `$aws/things/thingName/jobs/jobId/update/#` per entrambi.

Payload della risposta:

```
{
 "executionState": JobExecutionState,
 "jobDocument": "string",
 "timestamp": timestamp,
 "clientToken": "string"
}
```

**executionState**

Oggetto [JobExecutionState \(p. 454\)](#).

**jobDocument**

Un oggetto [documento del processo \(p. 368\)](#).

**timestamp**

Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'invio del messaggio.

**clientToken**

Token client usato per mettere in relazione richieste e risposte.

## HTTPS (15)

Richiesta:

```
POST /things/thingName/jobs/jobId
{
 "status": "job-execution-state",
 "statusDetails": {
 "string": "string"
 ...
 },
 "expectedVersion": "number",
 "includeJobExecutionState": boolean,
 "includeJobDocument": boolean,
 "stepTimeoutInMinutes": long,
 "executionNumber": long
}
```

**thingName**

Nome dell'oggetto associato al dispositivo.

**jobId**

Identificatore univoco assegnato al processo al momento della creazione.

**status**

Nuovo stato per l'esecuzione del processo (IN\_PROGRESS, FAILED, SUCCEEDED o REJECTED). Questo valore deve essere specificato per ogni aggiornamento.

**statusDetails**

Opzionale. Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo.  
Se non è specificato, **statusDetails** resta invariato.

**expectedVersion**

Opzionale. Versione corrente prevista dell'esecuzione del processo. Ogni volta che aggiorni l'esecuzione del processo, la versione viene incrementata. Se la versione dell'esecuzione del processo archiviata nel servizio AWS IoT Jobs non corrisponde, l'aggiornamento viene rifiutato con errore **VersionMismatch** e viene restituita una risposta [ErrorResponse \(p. 455\)](#) che contiene i dati sullo stato di esecuzione del processo corrente. Questo comportamento rende inutile una richiesta **DescribeJobExecution** separata per ottenere i dati sullo stato dell'esecuzione del processo.

**includeJobExecutionState**

Opzionale. Quando è incluso e impostato su **true**, la risposta contiene i dati JobExecutionState. Il valore di default è **false**.

**includeJobDocument**

Opzionale. Se è impostato su **true**, la risposta contiene il documento del processo. Il valore di default è **false**.

**stepTimeoutInMinutes**

Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Se lo stato di esecuzione del processo non è impostato su uno stato terminale prima del timeout o prima della reimpostazione del timer (chiamando nuovamente **UpdateJobExecution**, impostando lo stato su IN\_PROGRESS e specificando un nuovo valore di timeout in questo campo), lo stato di esecuzione del processo viene impostato su TIMED\_OUT. L'impostazione o la reimpostazione di questo timeout non ha alcun effetto su quello dell'esecuzione del processo che potresti avere specificato al momento della creazione del processo (utilizzando **CreateJob** con **timeoutConfig**).

**executionNumber**

Opzionale. Numero che identifica un'esecuzione di un processo in un dispositivo.

Risposta:

```
{
 "executionState": JobExecutionState,
 "jobDocument": "string"
}
```

**executionState**

Oggetto [JobExecutionState \(p. 454\)](#).

**jobDocument**

Il contenuto del [documento del processo \(p. 368\)](#).

CLI (15)

Riepilogo:

```
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]
```

Formato di **cli-input-json**:

```
{
 "jobId": "string",
 "thingName": "string",
 "status": "string",
 "statusDetails": {
 "string": "string"
 },
 "stepTimeoutInMinutes": number,
 "expectedVersion": long,
 "includeJobExecutionState": boolean,
 "includeJobDocument": boolean,
 "executionNumber": long
}
```

Campi di **cli-input-json**:

| Nome      | Tipo                                                             | Descrizione                                                                    |
|-----------|------------------------------------------------------------------|--------------------------------------------------------------------------------|
| jobId     | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a-zA-Z0-9_-]+ | Identificatore univoco<br>assegnato al processo al<br>momento della creazione. |
| thingName | Stringa<br>Lunghezza max: 128, min.: 1                           | Nome dell'oggetto associato al<br>dispositivo.                                 |

| Nome          | Tipo                                                                                                               | Descrizione                                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | Modello: [a-z A-Z 0-9 :_-]+                                                                                        |                                                                                                                                                      |
| stato         | Stringa<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED | Nuovo stato per l'esecuzione del processo (IN_PROGRESS, FAILED, SUCCEEDED o REJECTED). Questo valore deve essere specificato per ogni aggiornamento. |
| statusDetails | mappa<br><br>Chiave: DetailsKey<br><br>Valore: DetailsValue                                                        | Opzionale. Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo. Se non è specificato, statusDetails resta invariato. |
| DetailsKey    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+                                      |                                                                                                                                                      |
| DetailsValue  | Stringa<br><br>Lunghezza max: 1024, min.: 1<br><br>Modello: [^\p{C}]*+                                             |                                                                                                                                                      |

| Nome                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Tipo | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| stepTimeoutInMinutes<br><br>Long<br><br>Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Se lo stato di esecuzione del processo non è impostato su uno stato terminale prima del timeout o prima della reimpostazione del timer (chiamando nuovamente <code>UpdateJobExecution</code> , impostando lo stato su <code>IN_PROGRESS</code> e specificando un nuovo valore di timeout in questo campo), lo stato di esecuzione del processo viene impostato su <code>TIMED_OUT</code> . L'impostazione o la reimpostazione di questo timeout non ha alcun effetto su quello dell'esecuzione del processo che potresti avere specificato al momento della creazione del processo (utilizzando <code>CreateJob</code> con <code>timeoutConfig</code> ). |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| expectedVersion<br><br>Long<br><br>Classe Java: <code>java.lang.Long</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |      | Opzionale. Versione corrente prevista dell'esecuzione del processo. Ogni volta che aggiorni l'esecuzione del processo, la versione viene incrementata. Se la versione dell'esecuzione del processo archiviata nel servizio AWS IoT Jobs non corrisponde, l'aggiornamento viene rifiutato con l'errore <code>VersionMismatch</code> e viene restituita una risposta <code>ErrorResponse</code> che contiene i dati sullo stato di esecuzione del processo corrente. (Questo comportamento rende superfluo eseguire una richiesta <code>DescribeJobExecution</code> separata per ottenere i dati sullo stato dell'esecuzione del processo). |

| Nome                     | Tipo                                       | Descrizione                                                                                                                    |
|--------------------------|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| includeJobExecutionState | booleano<br>Classe Java: java.lang.Boolean | Opzionale. Quando è incluso e impostato su true, la risposta contiene i dati JobExecutionState. Il valore predefinito è false. |
| includeJobDocument       | booleano<br>Classe Java: java.lang.Boolean | Opzionale. Se è impostato su true, la risposta contiene il documento del processo. Il valore predefinito è false.              |
| executionNumber          | Long<br>Classe Java: java.lang.Long        | Opzionale. Numero che identifica un'esecuzione di un processo in un dispositivo.                                               |

Output:

```
{
 "executionState": {
 "status": "string",
 "statusDetails": {
 "string": "string"
 },
 "versionNumber": long
 },
 "jobDocument": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome           | Tipo                                                                                                           | Descrizione                                                                                                                     |
|----------------|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| executionState | JobExecutionState                                                                                              | Oggetto JobExecutionState.                                                                                                      |
| stato          | Stringa<br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED | Stato dell'esecuzione del processo. Può essere QUEUED, IN_PROGRESS, FAILED, SUCCEEDED, CANCELED, TIMED_OUT, REJECTED o REMOVED. |
| statusDetails  | mappa<br>Chiave: DetailsKey<br>Valore: DetailsValue                                                            | Raccolta di coppie nome-valore che descrivono lo stato dell'esecuzione del processo.                                            |
| DetailsKey     | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-zA-Z0-9_-]+                                              |                                                                                                                                 |
| DetailsValue   | Stringa<br>Lunghezza max: 1024, min.: 1                                                                        |                                                                                                                                 |

| Nome          | Tipo                            | Descrizione                                                                                                                                                |
|---------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | Modello: [^\p{C}]*+             |                                                                                                                                                            |
| versionNumber | Long                            | Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che vengono aggiornate da un dispositivo. |
| jobDocument   | Stringa<br>Lunghezza max: 32768 | Il contenuto dei documenti dei processi.                                                                                                                   |

## JobExecutionsChanged

JobExecutionsChanged message

Inviato ogni volta che un'esecuzione di un processo viene aggiunta o rimossa dall'elenco di esecuzioni del processo in sospeso per un oggetto.

MQTT (16)

Argomento: \$aws/things/*thingName*/jobs/notify

Payload del messaggio:

```
{
 "jobs" : [
 "JobExecutionState": [JobExecutionSummary \(p. 399\) ...]
],
 "timestamp": timestamp,
}
```

HTTPS (16)

Non disponibile.

CLI (16)

Non disponibile.

## NextJobExecutionChanged

NextJobExecutionChanged message

Inviato ogni volta che cambia l'esecuzione del processo successiva nell'elenco di esecuzioni in sospeso per un oggetto, come definito per [DescribeJobExecution \(p. 466\)](#) con jobId \$next. Questo messaggio non viene inviato quando cambiano i dettagli dell'esecuzione del processo successiva, ma solo quando cambia il processo successivo che verrebbe restituito da [DescribeJobExecution](#) con jobId \$next. Considera le esecuzioni J1 e J2 con stato QUEUED. J1 è l'esecuzione successiva nell'elenco di esecuzioni del processo in sospeso. Se lo stato di J2 viene modificato in IN\_PROGRESS, mentre lo stato di J1 rimane invariato, questa notifica viene inviata e contiene i dettagli di J2.

MQTT (17)

Argomento: \$aws/things/*thingName*/jobs/notify-next

Payload del messaggio:

```
{
 "execution" : JobExecution (p. 398),
 "timestamp": timestamp,
}
```

HTTPS (17)

Non disponibile.

CLI (17)

Non disponibile.

## Configurazione dei rollout e delle interruzioni di processo

I processi AWS IoT possono essere distribuiti usando velocità di rollout variabili quando vengono soddisfatti vari criteri e soglie. I rollout dei processi possono anche essere interrotti nel caso in cui il numero di processi non riusciti corrisponda a una serie di criteri. Queste configurazioni di rollout consentono un maggiore controllo granulare nel raggio di applicazione di un processo. I criteri di velocità di rollout dei processi sono impostati al momento della creazione di un processo mediante l'oggetto [JobExecutionsRolloutConfig](#). I criteri di interruzione dei processi sono impostati al momento della creazione di un processo mediante l'oggetto [AbortConfig](#).

### Utilizzo delle velocità di rollout di un processo

È possibile impostare la velocità di rollout di un processo configurando la proprietà [ExponentialRolloutRate](#) dell'oggetto [JobExecutionsRolloutConfig](#) quando si esegue l'API [CreateJob](#). L'esempio seguente imposta una velocità di rollout variabile utilizzando il parametro `exponentialRate`.

```
{
...
 "jobExecutionsRolloutConfig": {
 "exponentialRate": {
 "baseRatePerMinute": 50,
 "incrementFactor": 2,
 "rateIncreaseCriteria": {
 "numberOfNotifiedThings": 1000, // Set one or the other
 "numberOfSucceededThings": 1000 // of these two values.
 },
 "maximumPerMinute": 1000
 }
 }
}
```

Il parametro `baseRatePerMinute` specifica la velocità con cui i processi vengono eseguiti fino a quando non viene raggiunta la soglia `numberOfSucceededThings` o `numberOfNotifiedThings`.

Il parametro `incrementFactor` specifica il fattore esponenziale per il quale la velocità di rollout aumenta dopo che è stata raggiunta la soglia `numberOfSucceededThings` o `numberOfNotifiedThings`.

Il parametro `rateIncreaseCriteria` è un oggetto che identifica la soglia `numberOfNotifiedThings` o `numberOfSucceededThings`.

Il parametro `maximumPerMinute` specifica il limite superiore della velocità con cui possono verificarsi le esecuzioni dei processi. I valori validi sono compresi tra 1 e 1000. Questo parametro è obbligatorio quando si passa un oggetto `ExponentialRate`. In un rollout di velocità variabile, questo valore stabilisce il limite superiore della velocità di rollout di un processo.

Un rollout di processo con la configurazione in alto inizierebbe a una velocità di 50 esecuzioni al minuto. Continuerrebbe a quella velocità finché 1.000 oggetti non hanno ricevuto le notifiche di esecuzione di processo (se è stato specificato un valore per `numberOfNotifiedThings`) o finché non si verificano 1.000 esecuzioni riuscite (se è stato specificato un valore per `numberOfSucceededThings`).

La tabella riportata di seguito mostra il modo in cui il rollout dovrebbe procedere oltre i primi quattro incrementi.

|                                                              |      |      |      |      |
|--------------------------------------------------------------|------|------|------|------|
| Velocità di rollout al minuto                                | 50   | 100  | 200  | 400  |
| Il numero di dispositivi notificati o esecuzioni di successo | 1000 | 2000 | 3000 | 4000 |

La configurazione seguente imposta la velocità di rollout statica.

```
{
...
 "jobExecutionsRolloutConfig": {
 "maximumPerMinute": 1000
 }
...}
```

Il parametro `maximumPerMinute` specifica il limite superiore della velocità con cui possono verificarsi le esecuzioni dei processi. I valori validi sono compresi tra 1 e 1000. Questo parametro è opzionale. Se non specifichi un valore, viene utilizzato il valore predefinito 1000.

## Utilizzo delle configurazioni dei rollout e delle interruzioni di processo

È possibile impostare una condizione di interruzione di processo configurando l'oggetto `AbortConfig` opzionale quando si esegue l'API `CreateJob`. Questa sezione descrive l'effetto che la configurazione di esempio seguente avrebbe su un rollout del processo per cui si verificano più esecuzioni non riuscite.

```
"abortConfig": {
 "criteriaList": [
 {
 "action": "CANCEL",
 "failureType": "FAILED",
 "minNumberOfExecutedThings": 100,
 "thresholdPercentage": 20
 },
 {
 ...
 }
]
}
```

```
 "action": "CANCEL",
 "failureType": "TIMED_OUT",
 "minNumberOfExecutedThings": 200,
 "thresholdPercentage": 50
 }
}
```

Il parametro `action` specifica l'operazione da eseguire quando vengono soddisfatti i criteri di interruzione. Questo parametro è obbligatorio ed `CANCEL` è il solo valore valido.

Il parametro `failureType` specifica quali tipi di errori devono attivare l'interruzione di un processo. I valori validi sono `FAILED`, `REJECTED`, `TIMED_OUT` e `ALL`.

Il parametro `minNumberOfExecutedThings` specifica il numero di esecuzioni di processo completate che devono verificarsi prima che il servizio verifichi se sono stati soddisfatti i criteri di interruzione del processo. In questo esempio, AWS IoT non verifica se un'interruzione di processo si verifica quando almeno 100 dispositivi hanno completato le esecuzioni di processo.

Il parametro `thresholdPercentage` specifica il numero totale di oggetti eseguiti che hanno avviato l'interruzione del processo. In questo esempio, AWS IoT avvia un'interruzione di processo e annulla rollout di processo se almeno il 20% di tutte le esecuzioni completate non riporta esito negativo dopo il completamento di 100 esecuzioni.

#### Note

L'eliminazione delle esecuzioni di un processo influisce sul valore del calcolo dell'esecuzione totale completata. Quando un processo viene interrotto, il servizio crea codici `comment` e `reasonCode` automaticamente per differenziare una cancellazione dipendente dall'utente o una cancellazione per interruzione di processo.

## Limiti dei processi

Per informazioni sui limiti dei processi, consulta la pagina [Limiti dei processi AWS IoT](#) nella AWS General Reference.

# Provisioning dei dispositivi

Il provisioning dei dispositivi AWS IoT implica la creazione e la registrazione delle seguenti entità:

- Un certificato. Puoi effettuare il provisioning di un dispositivo con un certificato esistente o fare in modo che AWS IoT ne crei e ne registri uno per te.
- Una policy collegata al certificato.
- Un identificatore univoco per questo oggetto (dispositivo)
- Una serie di attributi per l'oggetto, inclusi tipi e gruppi di elementi esistenti.

Per effettuare il provisioning di un dispositivo, devi creare un modello che descriva le risorse necessarie per il dispositivo. I dispositivi richiedono un oggetto, un certificato e una o più policy. Un oggetto è una voce nel registro che contiene attributi che descrivono il dispositivo. I dispositivi usano certificati per eseguire l'autenticazione con AWS IoT. Le policy determinano le operazioni che un dispositivo può eseguire in AWS IoT.

I modelli contengono variabili che vengono sostituite quando il modello viene usato per il provisioning di un dispositivo. Un dizionario (mappa) viene usato per fornire i valori per le variabili specificate in un modello. Puoi usare lo stesso modello per effettuare il provisioning di più dispositivi. Sarà sufficiente passare valori diversi per le variabili del modello nel dizionario.

AWS IoT offre tre modi per effettuare il provisioning di dispositivi:

- Il provisioning Single-thing con un modello di provisioning.

Questa è una buona opzione se è sufficiente effettuare il provisioning di dispositivi uno alla volta.

- Il provisioning Just-in-time (JITP) con un modello che regista ed effettua il provisioning di un dispositivo quando si connette per la prima volta a AWS IoT.

Questa è una buona opzione se è necessario registrare un numero elevato di dispositivi, ma non si dispone di informazioni da assemblare in un elenco di provisioning in blocco.

- Il provisioning in blocco.

Questa opzione consente di specificare un elenco di valori di modelli di provisioning single-thing memorizzati in un file in un bucket S3. Questo approccio è ideale se si dispone di un numero elevato di dispositivi noti le cui caratteristiche desiderate possono essere assemblate in un elenco.

Il provisioning Just-in-time e il provisioning in blocco sono opzioni migliori se devi effettuare il provisioning per un numero elevato di dispositivi. AWS IoT fornisce inoltre un'API [RegisterThing](#) che puoi utilizzare per effettuare il provisioning di singoli dispositivi in modo programmatico.

## Modelli di provisioning

Un modello di provisioning è un documento JSON che usa parametri per descrivere le risorse che il dispositivo deve usare per l'interazione con AWS IoT. Un modello contiene due sezioni: `Parameters` e `Resources`.

### Sezione Parameters

La sezione `Parameters` dichiara i parametri usati all'interno della sezione `Resources`. Ogni parametro dichiara un nome, un tipo e un valore predefinito facoltativo. Il valore predefinito viene usato quando il

dizionario passato con il modello non contiene un valore per il parametro. La sezione **Parameters** del documento di un modello è simile alla seguente:

```
{
 "Parameters" : {
 "ThingName" : {
 "Type" : "String"
 },
 "SerialNumber" : {
 "Type" : "String"
 },
 "Location" : {
 "Type" : "String",
 "Default" : "WA"
 },
 "CSR" : {
 "Type" : "String"
 }
 }
}
```

Il frammento di codice di questo modello dichiara quattro parametri: `ThingName`, `SerialNumber`, `Location` e `CSR`. Tutti questi parametri sono di tipo `String`. Il parametro `Location` dichiara un valore predefinito "WA".

## Sezione Resources

La sezione **Resources** del modello dichiara le risorse necessarie per la comunicazione del dispositivo con AWS IoT: un oggetto, un certificato e una o più policy. Ogni risorsa specifica un nome logico, un tipo e un set di proprietà.

Un nome logico permette di fare riferimento a una risorsa in un'altra parte del modello.

Il tipo specifica il tipo di risorsa che intendi dichiarare. I tipi validi sono:

- `AWS::IoT::Thing`
- `AWS::IoT::Certificate`
- `AWS::IoT::Policy`

Le proprietà specificate dipendono dal tipo di risorsa dichiarato.

### Risorse oggetto

Le risorse oggetto vengono dichiarate usando le proprietà seguenti:

- `ThingName`: stringa.
- `AttributePayload`: facoltativa. elenco di coppie nome/valore.
- `ThingTypeName`: facoltativa. Stringa per un tipo di oggetto associato per l'oggetto.
- `ThingGroups`: facoltativa. Elenco di gruppi cui appartiene l'oggetto.

### Risorse certificato

I certificati possono essere specificati in uno dei modi seguenti:

- Richiesta di firma del certificato.

- ID certificato di un certificato del dispositivo esistente.
- Certificato del dispositivo creato con un certificato CA registrato con AWS IoT. Se esistono più certificati CA registrati con lo stesso campo dell'oggetto, devi passare anche il certificato CA usato per firmare il certificato del dispositivo.

#### Note

Quando dichiari un certificato in un modello, usa solo uno di questi metodi. Ad esempio, se usi una richiesta di firma del certificato, non potrai specificare anche un ID certificato o un certificato del dispositivo.

Per ulteriori informazioni, consulta [AWS IoT e certificati](#).

Le risorse certificato vengono dichiarate usando le proprietà seguenti:

- `CertificateSigningRequest`: stringa.
- `CertificateID`: stringa.
- `CertificatePem`: stringa.
- `CACertificatePem`: stringa.
- `Status`: facoltativa. Stringa che può avere uno di questi valori: ACTIVE, INACTIVE, PENDING\_ACTIVATION. Il valore predefinito è ACTIVE.

Esempi:

- Certificato specificato con una richiesta di firma del certificato (CSR):

```
{
 "certificate" : {
 "Type" : "AWS::IoT::Certificate",
 "Properties" : {
 "CertificateSigningRequest": {"Ref" : "CSR"},
 "Status" : "ACTIVE"
 }
 }
}
```

- Certificato specificato con un ID certificato esistente:

```
{
 "certificate" : {
 "Type" : "AWS::IoT::Certificate",
 "Properties" : {
 "CertificateId": {"Ref" : "CertificateId"}
 }
 }
}
```

- Certificate specificato con un .pem del certificato esistente e un .pem del certificato CA:

```
{
 "certificate" : {
 "Type" : "AWS::IoT::Certificate"
 "Properties" : {
 "CACertificatePem": {"Ref" : "CACertificatePem"},
 "CertificatePem": {"Ref" : "CertificatePem"}
 }
 }
}
```

}

## Risorse policy

Le risorse policy vengono dichiarate con una delle seguenti proprietà:

- **PolicyName**: facoltativa. Stringa. Il valore predefinito è un hash del documento della policy. Se utilizzi una policy IoT esistente, immetti il nome della policy per la proprietà **PolicyName**, senza includere la proprietà **PolicyDocument**.
- **PolicyDocument**: facoltativa. Un oggetto JSON specificato come stringa con carattere di escape. Se la proprietà **PolicyDocument** non è specificata, la policy deve essere già stata creata.

### Note

Se è presente una sezione **Policy**, è necessario specificare la proprietà **PolicyName** o **PolicyDocument**, ma non entrambe.

## Sostituzione delle impostazioni

Se un modello specifica una risorsa già esistente, la sezione **OverrideSettings** permette di specificare l'operazione da eseguire:

**DO NOTHING**

Lascia la risorsa inalterata.

**REPLACE**

Sostituisce la risorsa con quella specificata nel modello.

**FAIL**

La richiesta non riesce con **ResourceConflictException**.

**MERGE**

Valido solo per le proprietà **ThingGroups** e **AttributePayload** di una risorsa thing. Unisce gli attributi o le appartenenze ai gruppi esistenti dell'oggetto a quelli specificati nel modello.

Quando si dichiara una risorsa oggetto, è possibile specificare **OverrideSettings** per le seguenti proprietà:

- **ATTRIBUTE\_PAYLOAD**
- **THING\_TYPE\_NAME**
- **THING\_GROUPS**

Quando si dichiara una risorsa certificato, è possibile specificare **OverrideSettings** per la proprietà **Status**.

**OverrideSettings** non sono disponibili per le risorse policy.

## Esempi di risorsa

Il frammento di codice del modello seguente dichiara un oggetto, un certificato e una policy:

```
{
 "Resources" : {
 "thing" : {
 "Type" : "AWS::IoT::Thing",
 "Properties" : {
 "ThingName" : {"Ref" : "ThingName"},
 "AttributePayload" : { "version" : "v1", "serialNumber" : {"Ref" : "SerialNumber"}},
 "ThingTypeName" : "lightBulb-versionA",
 "ThingGroups" : ["v1-lightbulbs", {"Ref" : "Location"}]
 },
 "OverrideSettings" : {
 "AttributePayload" : "MERGE",
 "ThingTypeName" : "REPLACE",
 "ThingGroups" : "DO_NOTHING"
 }
 },
 "certificate" : {
 "Type" : "AWS::IoT::Certificate",
 "Properties" : {
 "CertificateSigningRequest": {"Ref" : "CSR"},
 "Status" : "ACTIVE"
 },
 "OverrideSettings" : {
 "Status" : "DO_NOTHING"
 }
 },
 "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\"] }] }"
 }
 }
 }
}
```

L'oggetto viene dichiarato con:

- Nome logico "thing".
- Tipo AWS::IoT::Thing.
- Un set di proprietà dell'oggetto.

Le proprietà dell'oggetto includono il nome dell'oggetto, un set di attributi, un nome di tipo di oggetto facoltativo e un elenco facoltativo di gruppi di oggetti cui appartiene l'oggetto.

Ai parametri viene fatto riferimento tramite `{ "Ref": "<parameter-name>" }`. Quando il modello viene valutato, i parametri vengono sostituiti con il valore del parametro specificato nel dizionario passato con il modello.

Il certificato viene dichiarato con:

- Nome logico "certificate".
- Tipo AWS::IoT::Certificate.
- Un set di proprietà.

Le proprietà includono la richiesta di firma per il certificato e l'impostazione dello stato su ACTIVE. Il testo della richiesta di firma del certificato viene passato come parametro nel dizionario a sua volta passato con il modello.

La policy viene dichiarata con:

- Nome logico "policy".
- Tipo AWS::IoT::Policy.
- Nome di una policy esistente o di un documento di policy.

## Esempio di modello

Il seguente file JSON è un esempio di un modello di provisioning completo che specifica il certificato con una CSR:

(Il valore del campo PolicyDocument deve essere un oggetto JSON specificato come stringa con carattere escape).

```
{
 "Parameters" : {
 "ThingName" : {
 "Type" : "String"
 },
 "SerialNumber" : {
 "Type" : "String"
 },
 "Location" : {
 "Type" : "String",
 "Default" : "WA"
 },
 "CSR" : {
 "Type" : "String"
 }
 },
 "Resources" : {
 "thing" : {
 "Type" : "AWS::IoT::Thing",
 "Properties" : {
 "ThingName" : {"Ref" : "ThingName"},
 "AttributePayload" : { "version" : "v1", "serialNumber" : {"Ref" : "SerialNumber"}},
 "ThingTypeName" : "lightBulb-versionA",
 "ThingGroups" : ["v1-lightbulbs", {"Ref" : "Location"}]
 }
 },
 "certificate" : {
 "Type" : "AWS::IoT::Certificate",
 "Properties" : {
 "CertificateSigningRequest": {"Ref" : "CSR"},
 "Status" : "ACTIVE"
 }
 },
 "policy" : {
 "Type" : "AWS::IoT::Policy",
 "Properties" : {
 "PolicyDocument" : "{ \"Version\": \"2012-10-17\", \"Statement\": [{ \"Effect\": \"Allow\", \"Action\": [\"iot:Publish\"], \"Resource\": [\"arn:aws:iot:us-east-1:123456789012:topic/foo/bar\"] }] }"
 }
 }
 }
}
```

Il seguente file JSON è un esempio di un modello di provisioning completo che specifica un certificato esistente con un ID certificato:

```
{
 "Parameters" : {
 "ThingName" : {
 "Type" : "String"
 },
 "SerialNumber" : {
 "Type" : "String"
 },
 "Location" : {
 "Type" : "String",
 "Default" : "WA"
 },
 "CertificateId" : {
 "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" : {
 "CertificateId": {"Ref" : "CertificateId"}
 },
 "OverrideSettings" : {
 "Status" : "DO_NOTHING"
 }
 },
 "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\"] }] }"
 }
 }
 }
}
```

## Provisioning programmatico

Per effettuare il provisioning di un oggetto, usa l'API [RegisterThing](#) o il comando `register-thing` dell'interfaccia a riga di comando. Il comando `register-thing` dell'interfaccia a riga di comando accetta gli argomenti seguenti:

`--template-body`

Modello di provisioning.

`--parameters`

Elenco di coppie nome/valore per i parametri usati nel modello di provisioning, in formato JSON (ad esempio, `{"ThingName" : "MyProvisionedThing", "CSR" : "<csr-text>"}`).

Per informazioni, consulta [Modelli di provisioning \(p. 482\)](#).

`RegisterThing` o `register-thing` restituisce gli ARN per le risorse e il testo del certificato creato:

```
{
 "certificatePem": "<certificate-text>",
 "resourceArns": {
 "PolicyLogicalName": "arn:aws:iot:us-west-2:123456789012:policy/2A6577675B7CD1823E271C7AAD8184F44630FFD7",
 "certificate": "arn:aws:iot:us-west-2:123456789012:cert/cd82bb924d4c6ccbb14986dcba4f40f30d892cc6b3ce7ad5008ed6542eea2b049",
 "thing": "arn:aws:iot:us-west-2:123456789012:thing/MyProvisionedThing"
 }
}
```

Se un parametro viene omesso dal dizionario, viene usato il valore predefinito. Se non è specificato alcun valore predefinito, il parametro non viene sostituito con un valore.

## Provisioning Just-in-Time

Puoi fare in modo che il provisioning dei dispositivi venga effettuato quando i dispositivi tentano di connettersi ad AWS IoT per la prima volta. Le impostazioni di provisioning just-in-time (JITP) vengono eseguite nei certificati CA. Per eseguire il provisioning del dispositivo, devi abilitare la registrazione automatica e associare un modello di provisioning al certificato CA usato per firmare il certificato del dispositivo.

Puoi configurare queste impostazioni durante la registrazione di un nuovo certificato CA con l'API `RegisterCACertificate` o il comando `register-ca-certificate` dell'interfaccia a riga di comando:

```
aws iot register-ca-certificate --ca-certificate <your-ca-cert> --verification-cert <your-verification-cert> --set-as-active --allow-auto-registration --registration-config file://<your-template>
```

Per ulteriori informazioni, consulta la pagina relativa alla [registrazione di un certificato CA](#).

Puoi anche usare l'API [UpdateCACertificate](#) o il comando `update-ca-certificate` dell'interfaccia a riga di comando per aggiornare le impostazioni per un certificato CA:

```
$ aws iot update-ca-certificate --cert-id <caCertificateId> --new-auto-registration-status ENABLE --registration-config file://<your-template>
```

Quando un dispositivo tenta di connettersi ad AWS IoT usando un certificato firmato da un certificato CA registrato, AWS IoT carica il modello dal certificato CA e chiama `RegisterThing` usando il modello. Il flusso di lavoro JITP prima registra un certificato con un valore di stato PENDING\_ACTIVATION. Quando il flusso di provisioning del dispositivo è completo, lo stato del certificato viene modificato in ACTIVE.

AWS IoT definisce i parametri seguenti, che puoi dichiarare e a cui puoi fare riferimento all'interno dei modelli di provisioning:

- `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

I valori per questi parametri del modello di provisioning sono limitati a ciò che JITP può estrarre dal campo oggetto del certificato del dispositivo di cui viene effettuato il provisioning. Il parametro AWS::IoT::Certificate::Id si riferisce a un ID generato internamente, non a un ID contenuto nel certificato. È possibile ottenere il valore di questo ID utilizzando la funzione `principal()` all'interno di una regola AWS IoT.

Il file JSON seguente è un esempio di modello JITP completo. Il valore del campo `templateBody` deve essere un oggetto JSON specificato come stringa con carattere di escape e può utilizzare solo i valori dell'elenco precedente. È possibile utilizzare una serie di strumenti per creare l'oggetto JSON stringified, ad esempio `json.dumps` (Python) o `JSON.stringify` (Nodo). Il valore del campo `roleARN` deve essere l'ARN di un ruolo che ha `AWSIoTThingsRegistration` allegata. Inoltre, il modello può utilizzare un `PolicyName` esistente invece di `PolicyDocument` inline nell'esempio. (Il primo esempio aggiunge interruzioni di riga per la leggibilità, ma è possibile copiare e incollare il modello che appare direttamente al di sotto).

```
{
 "templateBody" : "{
 \"Parameters\" : { \r\n
 \"AWS::IoT::Certificate::CommonName\": { \r\n \"Type\": \"String"
 }, \r\n
 \"AWS::IoT::Certificate::SerialNumber\": { \r\n \"Type\": \"String"
 }, \r\n
 \"AWS::IoT::Certificate::Country\": { \r\n \"Type\": \"String\" \r
 }, \r\n
 \"AWS::IoT::Certificate::Id\": { \r\n \"Type\": \"String\" \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
 }, \r\n
 \"ThingType\": { \r\n
 \"Name\": \"lightBulb-versionA\", \r\n
 \"ThingGroups\": [\r\n
 \"v1-lightbulbs\", \r\n
 \"Ref\": \"AWS::IoT::Certificate::Country\" \r
], \r\n
 \"OverrideSettings\": { \r\n
 \"AttributePayload\": { \r\n
 \"Type\": \"MERGE\", \r\n
 \"ThingType\": { \r\n
 \"Name\": \"REPLACE\", \r\n
 \"ThingGroups\": { \r\n
 \"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
 \"OverrideSettings\": { \r\n
 \"Status\": { \r\n
 \"DO NOTHING\" \r\n
 } \r\n
 }, \r\n
 \"policy\": { \r\n
 \"Ref\": "
 \"AWS::IoT::Policy::Name\" \r\n
 } \r\n
 }, \r\n
 \"PolicyName\": { \r\n
 \"Ref\": "
 \"AWS::IoT::Policy::Name\" \r\n
 } \r\n
 }, \r\n
 \"PolicyDocument\": { \r\n
 \"Version\": \"2012-10-17\", \r\n
 \"Statement\": [\r\n
 { \r\n
 \"Effect\": \"Allow\", \r\n
 \"Action\": \"iot:Connect\", \r\n
 \"Resource\": \"*\" \r\n
 }, \r\n
 { \r\n
 \"Effect\": \"Allow\", \r\n
 \"Action\": \"iot:Publish\", \r\n
 \"Topic\": \"$TopicFilter\", \r\n
 \"Condition\": { \r\n
 \"StringEquals\": { \r\n
 \"aws:sourceArn\": "
 \"AWS::IoT::Certificate::Arn\" \r\n
 } \r\n
 } \r\n
 } \r\n
] \r\n
 } \r\n
 } \r\n
 } \r\n
 } \r\n
 } \r\n
 } \r\n
 } \r\n
 } \r\n
 } \r\n
 } \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\\\"\\\"/sample\\\"\\\"/topic\\\"\\\"] }]}\\r\\n }\\r\\n }\\r\\n
 \"roleArn\" : \"arn:aws:iam::123456789012:role/Provisioning-JITP"
}

```

Versione che puoi copiare e incollare:

```
{
 \"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 \\\"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
 \\\"serialNumber\\\" : {\\r\\n
 \\\"Ref\\\" : \\\"AWS::IoT::Certificate::SerialNumber\\\"\\r\\n
 },\\r\\n \\\"ThingType\\\" : \"lightBulb-versionA\",\\r\\n
 \\\"ThingGroups\\\" : [\\r\\n
 \\\"v1-lightbulbs\\\",\\r\\n
 {\\r\\n
 \\\"Ref\\\" : \\\"AWS::IoT::Certificate::Country\\\"\\r\\n
 },\\r\\n
 \\\"OverrideSettings\\\" : {\\r\\n
 \\\"AttributePayload\\\" : \\\"MERGE\\\",\\r\\n
 \\\"ThingGroups\\\" : \\\"DO NOTHING\\\"\\r\\n
 },\\r\\n
 \\\"certificate\\\" : {\\r\\n
 \\\"Type\\\" : \"AWS::IoT::Certificate\\\",\\r\\n
 \\\"Properties\\\" : {\\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
 \\\"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
 \"roleArn\" : \"arn:aws:iam::123456789012:role/JITPRole"
}

```

Questo modello di esempio dichiara i valori per i parametri di provisioning

`AWS::IoT::Certificate::CommonName`, `AWS::IoT::Certificate::SerialNumber`,  
`AWS::IoT::Certificate::Country` e `AWS::IoT::Certificate::Id` che vengono estratti dal certificato e utilizzati nella sezione Resources. Il flusso di lavoro JITP usa quindi questo modello per eseguire le seguenti operazioni:

- Registrare un certificato e impostare il relativo stato su PENDING\_ACTIVE.
- Creare una risorsa oggetto.
- Creare una risorsa policy.
- Collegare la policy al certificato.
- Collegare il certificato all'oggetto.
- Aggiornare lo stato del certificato ad ACTIVE.

Dovresti visualizzare la registrazione del certificato come un evento registrato ([RegisterCACertificate](#)) in AWS CloudTrail. Puoi inoltre utilizzare CloudTrail per risolvere i problemi con il modello JITP.

## Provisioning in blocco

Puoi usare il comando [start-thing-registration-task](#) per effettuare il provisioning in blocco di più oggetti. Questo comando accetta un modello di provisioning, un nome di bucket Amazon S3, un nome di chiave e un ARN di ruolo che permette di accedere al file nel bucket Amazon S3. Il file nel bucket Amazon S3 contiene i valori usati per sostituire i parametri nel modello. Il file deve essere un file JSON delimitato da righe. Ogni riga contiene tutti i valori dei parametri per il provisioning di un singolo dispositivo. Ad esempio:

```
{"ThingName": "foo", "SerialNumber": "123", "CSR": "csr1"}
{"ThingName": "bar", "SerialNumber": "456", "CSR": "csr2"}
```

Le seguenti API correlate di provisioning in blocco possono risultare utili:

- [ListThingRegistrationTasks](#) – Elenca le attività correnti di provisioning in blocco degli oggetti.
- [DescribeThingRegistrationTask](#) – Fornisce informazioni su una specifica attività di provisioning in blocco degli oggetti.
- [StopThingRegistrationTask](#) – Arresta l'attività di provisioning in blocco degli oggetti.
- [ListThingRegistrationTaskReports](#) – Utilizzata per verificare i risultati e/o gli errori di un'attività di provisioning in blocco degli oggetti.

### Note

Puoi eseguire una sola attività di provisioning in blocco per volta (per account).

# Servizio Fleet Indexing

L'indicizzazione del parco istanze è un servizio gestito che consente di indicizzare e ricercare i dati di registro, i dati shadow e i dati di connettività del dispositivo (eventi del ciclo di vita del dispositivo) nel cloud. Dopo la configurazione dell'indice del parco istanze, il servizio gestisce l'indicizzazione degli aggiornamenti dei gruppi di oggetti, dei registri di oggetti e delle copie shadow dei dispositivi. È possibile utilizzare un semplice linguaggio di query per eseguire ricerche in questi dati. È anche possibile creare un [gruppo di oggetti dinamico](#) con una query di ricerca.

Quando si abilita l'indicizzazione, AWS IoT crea un indice per i tuoi oggetti o gruppi di oggetti. Quando l'indicizzazione è attiva, puoi eseguire query sull'indice, ad esempio cercare tutti i dispositivi palmari e che hanno una durata della batteria superiore al 70%. AWS IoT la mantiene costantemente aggiornata con i dati più recenti.

[AWS\\_Things](#) è l'indice creato per tutti i tuoi oggetti. [AWS\\_ThingGroups](#) è l'indice che contiene tutti i tuoi gruppi di oggetti.

Puoi usare la [console AWS IoT](#) per gestire la configurazione dell'indicizzazione ed eseguire le query di ricerca. Scegli gli indici da utilizzare nella pagina delle impostazioni della console. Se preferisci l'accesso programmatico, puoi usare gli SDK AWS o AWS CLI.

Consulta la pagina dei [prezzi di gestione dei dispositivi AWS IoT](#) per informazioni sui prezzi di questo e altri servizi.

## Gestione dell'indicizzazione degli oggetti

[AWS\\_Things](#) è l'indice creato per tutti gli oggetti. È possibile controllare cosa indicizzare: dati di registro, dati shadow e dati sullo stato della connettività del dispositivo (guidata da eventi del ciclo di vita del dispositivo).

### Abilitazione dell'indicizzazione degli oggetti

Puoi creare l'indice [AWS\\_Things](#) e controllarne la configurazione usando il parametro `--thing-indexing-configuration` nell'API [UpdateIndexingConfiguration](#). Puoi recuperare la configurazione dell'indicizzazione corrente usando l'API [GetIndexingConfiguration](#).

Il comando seguente mostra come usare il comando dell'interfaccia a riga di comando `get-indexing-configuration` per recuperare l'attuale configurazione dell'indicizzazione degli oggetti. In questo esempio, l'indicizzazione degli oggetti è attualmente disabilitato.

```
aws iot get-indexing-configuration
{
 "thingIndexingConfiguration": {
 "thingConnectivityIndexingMode": "OFF"
 "thingIndexingMode": "OFF"
 }
}
```

La tabella seguente fornisce le combinazioni consentite di `thingIndexingMode` e `thingConnectivityIndexingMode` e i relativi effetti. In breve, il parametro `thingIndexingMode` obbligatorio specifica se l'indice [AWS\\_Things](#) includerà solo i dati di registro o i dati shadow e di registro. Il parametro `thingConnectivityIndexingMode` opzionale specifica se l'indice conterrà anche i dati sullo stato di connettività (quando i dispositivi sono stati collegati e scollegati).

| <b>thingIndexingMode</b> | <b>thingConnectivityIndexingMode</b> | Risultato                                                                                                                                                                                  |
|--------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OFF                      | Non specificato.                     | Nessuna indicizzazione o eliminare un indice.                                                                                                                                              |
| OFF                      | OFF                                  | Equivalente alla voce precedente.                                                                                                                                                          |
| REGISTRY                 | Non specificato.                     | Crea o configura l'indice AWS_Things per indicizzare solo i dati del registro.                                                                                                             |
| REGISTRY                 | OFF                                  | Equivalente alla voce precedente. (Solo i dati di registro sono indicizzati).                                                                                                              |
| REGISTRY_AND_SHADOW      | Non specificato.                     | Crea o configura l'indice AWS_Things per indicizzare i dati del registro e i dati shadow.                                                                                                  |
| REGISTRY_AND_SHADOW      | OFF                                  | Equivalente alla voce precedente. (I dati di registro e i dati shadow sono indicizzati).                                                                                                   |
| REGISTRY                 | STATUS                               | Crea o configura l'indice AWS_Things per indicizzare i dati del registro e i dati sullo stato della connettività dell'oggetto (REGISTRY_AND_CONNECTIVITY_STATUS)                           |
| REGISTRY_AND_SHADOW      | STATUS                               | Crea o configura l'indice AWS_Things per indicizzare i dati del registro, i dati shadow e i dati sullo stato della connettività dell'oggetto (REGISTRY_AND_SHADOW_AND_CONNECTIVITY_STATUS) |

Usa il comando dell'interfaccia a riga di comando update-indexing-configuration per aggiornare la configurazione dell'indicizzazione degli oggetti. Nell'esempio seguente, è possibile cercare i dati, dati shadow e dati sullo stato della connettività dell'oggetto utilizzando l'indice AWS\_Things una volta creato, come descritto nella sezione successiva.

```
aws iot update-indexing-configuration --thing-indexing-configuration
 thingIndexingMode=REGISTRY_AND_SHADOW,thingConnectivityIndexingMode=STATUS
```

## Descrizione di un indice dell'oggetto

Il comando seguente mostra come usare il comando dell'interfaccia a riga di comando describe-index per recuperare lo stato corrente dell'indice degli oggetti.

```
aws iot describe-index --index-name "AWS_Things"
{
 "indexName": "AWS_Things",
 "indexStatus": "BUILDING",
 "schema": "REGISTRY_AND_SHADOW_AND_CONNECTIVITY_STATUS"
}
```

Quando abiliti l'indicizzazione per la prima volta, AWS IoT crea l'indice. Non puoi eseguire query sull'indice se `indexStatus` è nello stato `BUILDING`. Il schema per l'indice degli oggetti indica quale tipo di dati (`REGISTRY_AND_SHADOW_AND_CONNECTIVITY_STATUS`) sarà indicizzato.

La modifica della configurazione dell'indice comporta la ricostruzione dell'indice. Durante questo processo, `indexStatus` è `REBUILDING`. È possibile eseguire query sui dati nell'indice degli oggetti, mentre è in fase di ricostruzione. Ad esempio, se modifichi la configurazione dell'indice da `REGISTRY` a `REGISTRY_AND_SHADOW` mentre l'indice è in fase di ricompilazione, puoi eseguire query sui dati del registro, inclusi gli aggiornamenti più recenti. Tuttavia, non puoi eseguire query sui dati shadow fino al completamento della ricompilazione. L'intervallo di tempo necessario per creare o ricostruire l'indice dipende dalla quantità di dati.

## Esecuzione di query su un indice di oggetti

Utilizzare il comando dell'interfaccia a riga di comando `search-index` per eseguire query dei dati nell'indice.

```
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
 }
 },
 {
 "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"
}
```

Nella risposta JSON, "connectivity" (come abilitata dall'impostazione thingConnectivityIndexingMode=STATUS) fornisce un valore booleano e un timestamp che indica se il dispositivo è collegato a Core AWS IoT. Il dispositivo "mything1" scollegato (false) a POSIX time 1556649874716:

```
"connectivity": {
 "connected": false,
 "timestamp": 1556649874716
}
```

Il dispositivo "mything2" connesso (true) a POSIX time 1556649855046:

```
"connectivity": {
 "connected": true,
 "timestamp": 1556649855046
}
```

I timestamp vengono forniti in millisecondi dall'epoch, perciò 1556649855046 rappresenta 6:44:15.046 PM di martedì del 30 aprile 2019 (GMT).

#### Important

Se un dispositivo è stato disconnesso per circa un'ora, il valore "timestamp" dello stato connettività potrebbe essere assente. Per le sessioni permanenti, il valore potrebbe essere assente dopo che un client è stato disconnesso per un periodo più lungo del time-to-live (TTL) configurato per la sessione persistente. I dati solo stato della connessione sono indicizzati solo per le connessioni in cui l'ID client dispone di un nome oggetto corrispondente. (L'ID client è il valore utilizzato per collegare un dispositivo a Core AWS IoT).

## Restrizioni e limitazioni

Queste sono le limitazioni e le restrizioni per AWS\_Things.

### Campi della copia shadow con valori di tipo complesso

Un campo della copia shadow viene indicizzato solo se il relativo valore è di tipo semplice o è composto da una serie di tipi semplici. (Tipo semplice significa una stringa, un numero o uno dei valori letterali `true` o `false`). Se il valore di un campo è un oggetto JSON o un array che contiene un oggetto, l'indicizzazione non viene eseguita su tale campo. Ad esempio, per il seguente stato shadow, il valore del campo `"palette"` non verrà indicizzato perché è una matrice i cui elementi sono "oggetti". Il valore del campo `"colors"` viene indicizzato perché ogni valore della matrice è una stringa.

```
{
 "state": {
 "reported": {
 "switched": "ON",
 "colors": ["RED", "GREEN", "BLUE"],
 "palette": [
 {
 "name": "RED",
 "intensity": 124
 },
 {
 "name": "GREEN",
 "intensity": 68
 },
 {
 "name": "BLUE",
 "intensity": 201
 }
]
 }
 }
}
```

### Metadati delle copie shadow

Un campo nella sezione metadati delle copie shadow viene indicizzato, ma solo se lo è anche il campo corrispondente nella sezione `"state"` della copia shadow. (Nell'esempio precedente, neanche il campo `"palette"` nella sezione dei metadati delle copie shadow verrà indicizzato).

### Copie shadow non registrate

Se crei una copia shadow con [Create Thing \(Crea oggetto\)](#) utilizzando un nome di oggetto che non è stato registrato nel tuo account AWS IoT, i campi in questa copia shadow non verranno indicizzati.

### Valori numerici

Se eventuali dati del registro o dati shadow vengono riconosciuti dal servizio come valori numerici, verranno indicizzati come tali. Puoi formulare delle query che includono intervalli e operatori di confronto in merito ai valori numerici, ad esempio `"attribute.foo<5"` o `"shadow.reported.foo:[ 75 TO 80 ]"`. Per essere riconosciuto come numerico, il valore dei dati deve essere un letterale di tipo "numero" JSON valido (un numero intero compreso nell'intervallo  $-2^{53}...2^{53}-1$  o in virgola mobile a precisione doppia con notazione esponenziale opzionale) oppure una parte di una serie contenente solo questo tipo di valori.

### Valori nulli

I valori nulli non sono indicizzati.

## Autorizzazione

Puoi specificare l'indice degli oggetti come ARN di risorsa in un'operazione di policy AWS IoT come segue.

| Operazione        | Risorsa                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------|
| iot:SearchIndex   | Un indice ARN (ad esempio, <code>arn:aws:iot:&lt;your-aws-region&gt;:index/AWS_Things</code> ). |
| iot:DescribeIndex | Un indice ARN (ad esempio, <code>arn:aws:iot:&lt;your-aws-region&gt;:index/AWS_Things</code> ). |

#### Note

Se si dispone di autorizzazioni per eseguire query all'indice del parco istanze, è possibile accedere ai dati degli oggetti sull'intero parco istanze.

## Gestione dell'indicizzazione di gruppi di oggetti

`AWS_ThingGroups` è l'indice che contiene tutti i tuoi gruppi di oggetti. Questo indice consente di cercare gruppi in base al nome del gruppo, alla descrizione, agli attributi e a tutti i nomi del gruppo padre.

### Abilitazione dell'indicizzazione di gruppi di oggetti

Puoi creare l'indice `AWS_ThingGroups` e controllarne la configurazione usando l'impostazione `thing-group-indexing-configuration` nell'API [UpdateIndexingConfiguration](#). Puoi recuperare la configurazione dell'indicizzazione corrente usando l'API [GetIndexingConfiguration](#).

Utilizzare il comando dell'interfaccia a riga di comando `get-indexing-configuration` per recuperare l'attuale oggetto e le configurazioni di indicizzazione del gruppo di oggetti.

```
aws iot get-indexing-configuration
{
 "thingGroupIndexingConfiguration": {
 "thingGroupIndexingMode": "ON"
 }
}
```

Usa il comando dell'interfaccia a riga di comando `update-indexing-configuration` per aggiornare le configurazioni dell'indicizzazione dei gruppi di oggetti.

```
aws iot update-indexing-configuration --thing-group-indexing-configuration
 thingGroupIndexingMode=ON
```

#### Note

Puoi inoltre aggiornare le configurazioni per l'indicizzazione sia degli oggetti che dei gruppi di oggetti con un unico comando, come descritto di seguito.

```
aws iot update-indexing-configuration --thing-indexing-configuration
 thingIndexingMode=REGISTRY --thing-group-indexing-configuration
 thingGroupIndexingMode=ON
```

Di seguito sono riportati i valori validi per `thingGroupIndexingMode`.

OFF

Nessuna indicizzazione/eliminazione dell'indice.

ATTIVATO

Creazione o configurazione dell'indice AWS\_ThingGroups.

## Descrizione degli indici di gruppi

Utilizzare il comando dell'interfaccia a riga di comando describe-index per recuperare lo stato corrente dell'indice AWS\_ThingGroups.

```
aws iot describe-index --index-name "AWS_ThingGroups"
{
 "indexStatus": "ACTIVE",
 "indexName": "AWS_ThingGroups",
 "schema": "THING_GROUPS"
}
```

Quando abiliti l'indicizzazione per la prima volta, AWS IoT crea l'indice. Non è possibile eseguire query dell'indice se indexStatus è BUILDING.

## Esecuzione di query su un indice di gruppi di oggetti

Utilizzare il comando dell'interfaccia a riga di comando search-index per eseguire query dei dati nell'indice:

```
aws iot search-index --index-name "AWS_ThingGroups" --query-string
"thingGroupName:mythinggroup*"
```

## Autorizzazione

Puoi specificare l'indice di gruppi di oggetti come ARN di risorsa in un'operazione di policy AWS IoT come segue.

| Operazione        | Risorsa                                                                             |
|-------------------|-------------------------------------------------------------------------------------|
| iot:SearchIndex   | ARN di un indice (ad esempio, arn:aws:iot:<your-aws-region>:index/AWS_ThingGroups). |
| iot:DescribeIndex | ARN di un indice (ad esempio, arn:aws:iot:<your-aws-region>:index/AWS_ThingGroups). |

## Ottenimento di statistiche sul parco istanze del dispositivo

È possibile utilizzare il comando CLI get-statistics o l'API [GetStatistics](#) per cercare un indice per i dati di aggregazione. Ad esempio, potrebbe essere necessario trovare il numero di dispositivi attualmente connessi a AWS IoT:

```
aws iot get-statistics --index-name AWS_Things --query-string "connectivity.connected:true".
```

Questo comando restituisce il numero di oggetti che hanno una proprietà denominata `connectivity.connected` impostata su `true` nella copia shadow dell'oggetto:

```
{
 "statistics" : {
 "count" : 1000
 }
}
```

Il comando CLI `get-statistics` accetta i parametri seguenti:

`index-name`

Nome dell'indice su cui eseguire una ricerca. Il valore predefinito è `AWS_Things`.

`query-string`

La query usata per eseguire la ricerca nell'indice. È possibile specificare "\*" per ottenere il numero di tutti gli oggetti indicizzati nel tuo account AWS.

`query-version`

La versione della query da usare. Il valore predefinito è `2017-09-30`.

Il comando CLI `get-statistics` restituisce i dati in un oggetto JSON. Attualmente l'unica statistica restituita è `count`:

```
{
 "statistics" : {
 "count" : 1000
 }
}
```

## Sintassi di query

Le query vengono specificate tramite una sintassi di query.

La sintassi di query supporta le seguenti caratteristiche.

- Termini e frasi
- Ricerca nei campi
- Ricerca di prefissi
- Ricerca di intervalli
- Operatori booleani AND, OR, NOT e - (il trattino viene utilizzato per escludere qualcosa dai risultati di ricerca, ad esempio `thingName:(tv* AND -plasma)`)
- Raggruppamento
- Raggruppamento di campi
- Uso di escape con caratteri speciali

La sintassi di query non supporta le seguenti caratteristiche.

- Principale ricerca jolly (ad esempio `*xyz`). (Ricerca di corrispondenze "\*" per tutte le cose).
- Espressioni regolari
- Aumento priorità
- Classificazione

- Ricerche fuzzy
- Ricerca per prossimità
- Ordinamento
- Aggregazione

Alcune note relative al linguaggio di query:

- L'operatore predefinito è AND. Una query per "thingName:abc thingType:xyz" equivale a "thingName:abc AND thingType:xyz".
- Se non è specificato alcun campo, AWS IoT cerca il termine in tutti i campi.
- Tutti i nomi di campo fanno distinzione tra maiuscole e minuscole.
- La ricerca non fa distinzione tra maiuscole e minuscole. Le parole sono separate da spazi come definito dal metodo Character.isWhitespace(int) di Java.
- L'indicizzazione di dati shadow degli oggetti include le sezioni reported, desired, delta e metadata.
- Non è possibile eseguire ricerche nelle versioni shadow e registro dei dispositivi, ma queste sono presenti nella risposta.
- Il numero massimo di termini in una query è 5.

## Esempio di query per oggetti

Le query vengono specificate in una stringa di query usando una sintassi di query, quindi vengono passate all'API [SearchIndex](#). La tabella seguente elenca alcune stringhe di query di esempio.

| Stringa di query                          | Risultato                                                                                                                                |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| abc                                       | Query per "abc" in qualsiasi campo del registro o della copia shadow.                                                                    |
| thingName: NomeMioOggetto                 | Query per un oggetto con nome "NomeMioOggetto".                                                                                          |
| thingName:mio*                            | Query per oggetti con nomi che iniziano per "mio".                                                                                       |
| thingName:ab?                             | Query per oggetti con nomi che contengono "ab" più un altro carattere, ad esempio, "aba", "abb", "abc" e così via.                       |
| thingTypeNames:aa                         | Query per cose associate al tipo aa.                                                                                                     |
| attributes.MioAttributo:75                | Query per oggetti con un attributo denominato "myAttribute" il cui valore è 75.                                                          |
| attributes.MioAttributo:[75 TO 80]        | Query per oggetti con un attributo denominato "myAttribute" il cui valore è compreso in un intervallo numerico (da 75– a 80 inclusi).    |
| attributes.MioAttributo:{75 TO 80]        | Query per oggetti con un attributo denominato "myAttribute" il cui valore è compreso in un intervallo numerico (tra >75 e <=80).         |
| attributes.NumeroSerie:["abcd" TO "abcf"] | Query per oggetti con un attributo denominato "serialNumber" il cui valore è compreso in un intervallo di stringhe alfanumeriche. Questa |

| Stringa di query                                                                           | Risultato                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                            | query restituisce gli oggetti con un attributo "serialNumber" con i valori "abcd", "abce" o "abcf".                                                                                                                                                                                                                                                                                |
| attributes.MioAttributo:i*t                                                                | Query per oggetti con un attributo denominato "myAttribute" il cui valore è "i", seguito da un numero qualsiasi di caratteri, seguito da "t".                                                                                                                                                                                                                                      |
| attributes.attr1:abc AND attributes.attr2<5 NOT attributes.attr3>10                        | Query per oggetti che combinano termini usando espressioni booleane. Questa query restituisce gli oggetti che hanno un attributo denominato "attr1" con un valore "abc", un attributo denominato "attr2" il cui valore è minore di 5 e un attributo denominato "attr3" che non è maggiore di 10.                                                                                   |
| shadow.hasDelta:true                                                                       | Query per oggetti la cui copia shadow ha un elemento delta.                                                                                                                                                                                                                                                                                                                        |
| NOT attributes.model:legacy                                                                | Query per oggetti in cui l'attributo denominato "model" non è "legacy".                                                                                                                                                                                                                                                                                                            |
| shadow.reported.stats.battery:{70 TO 100} (v2 OR v3) NOT attributes.model:legacy           | Query per oggetti con le caratteristiche seguenti: <ul style="list-style-type: none"> <li>L'attributo stats.battery della copia shadow dell'oggetto ha un valore compreso tra 70 e 100.</li> <li>Il testo "v2" o "v3" è contenuto in un nome di oggetto, un nome di tipo o in valori di attributo.</li> <li>L'attributo model dell'oggetto non è impostato su "legacy".</li> </ul> |
| shadow.reported.myvalues:2                                                                 | Query per oggetti in cui la serie myvalues nella sezione reported della copia shadow contiene un valore pari a 2.                                                                                                                                                                                                                                                                  |
| shadow.reported.location:* NOT shadow.desired.stats.battery:*                              | Query per oggetti con le caratteristiche seguenti: <ul style="list-style-type: none"> <li>L'attributo location è presente nella sezione reported della copia shadow.</li> <li>L'attributo stats.battery non è presente nella sezione desired della copia shadow.</li> </ul>                                                                                                        |
| connectivity.connected:true                                                                | Interroga tutti i dispositivi connessi.                                                                                                                                                                                                                                                                                                                                            |
| connectivity.connected:false                                                               | Interroga tutti i dispositivi disconnessi.                                                                                                                                                                                                                                                                                                                                         |
| connectivity.connected:true AND connectivity.timestamp : [1557651600000 TO 1557867600000]  | Interroga tutti i dispositivi connessi con un timestamp connesso $\geq$ 1557651600000 e $\leq$ 1557867600000. I timestamp vengono forniti in millisecondi dall'epoch.                                                                                                                                                                                                              |
| connectivity.connected:false AND connectivity.timestamp : [1557651600000 TO 1557867600000] | Interroga tutti i dispositivi disconnessi con un timestamp disconnesso $\geq$ 1557651600000 e $\leq$ 1557867600000. I timestamp vengono forniti in millisecondi dall'epoch.                                                                                                                                                                                                        |

| Stringa di query                                                       | Risultato                                                                                                                                                 |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| connectivity.connected:true AND connectivity.timestamp > 1557651600000 | Interroga tutti i dispositivi connessi con un timestamp connesso > 1557651600000 e <= 1540508225. I timestamp vengono forniti in millisecondi dall'epoch. |
| connectivity.connected:*                                               | Ricerche di tutti i dispositivi con informazioni sulla connettività.                                                                                      |

## Esempio di query per gruppi di oggetti

Le query vengono specificate in una stringa di query usando una sintassi di query, quindi vengono passate all'API [SearchIndex](#). La tabella seguente elenca alcune stringhe di query di esempio.

| Stringa di query                                                    | Risultato                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| abc                                                                 | Query per "abc" in qualsiasi campo.                                                                                                                                                                                                                                                                                |
| thingGroupName:myGroupThingName                                     | Query per un gruppo di oggetti con nome "myGroupThingName".                                                                                                                                                                                                                                                        |
| thingGroupName:my*                                                  | Query per gruppi di oggetti con nomi che iniziano per "my".                                                                                                                                                                                                                                                        |
| thingGroupName:ab?                                                  | Query per gruppi di oggetti con nomi che contengono "ab" più un altro carattere, ad esempio, "aba", "abb", "abc" e così via.                                                                                                                                                                                       |
| attributes.MioAttributo:75                                          | Query per gruppi di oggetti con un attributo denominato "myAttribute" il cui valore è 75.                                                                                                                                                                                                                          |
| attributes.MioAttributo:[75 TO 80]                                  | Query per gruppi di oggetti con un attributo denominato "myAttribute" il cui valore è compreso in un intervallo numerico (da 75– a 80 inclusi).                                                                                                                                                                    |
| attributes.MioAttributo:[75 TO 80]                                  | Query per gruppi di oggetti con un attributo denominato "myAttribute" il cui valore è compreso in un intervallo numerico (tra >75 e <=80).                                                                                                                                                                         |
| attributes.myAttribute:["abcd" TO "abcf"]                           | Query per gruppi di oggetti con un attributo denominato "myAttribute" il cui valore è compreso in un intervallo di stringhe alfanumeriche. Questa query restituisce i gruppi di oggetti con un attributo "serialNumber" con i valori "abcd", "abce" o "abcf".                                                      |
| attributes.MioAttributo:i*                                          | Query per gruppi di oggetti con un attributo denominato "myAttribute" il cui valore è "i", seguito da un numero qualsiasi di caratteri, seguito da "t".                                                                                                                                                            |
| attributes.attr1:abc AND attributes.attr2<5 NOT attributes.attr3>10 | Query per gruppi di oggetti che combinano termini usando espressioni booleane. Questa query restituisce i gruppi di oggetti che hanno un attributo denominato "attr1" con un valore "abc", un attributo denominato "attr2" il cui valore è minore di 5 e un attributo denominato "attr3" che non è maggiore di 10. |

| Stringa di query                                                     | Risultato                                                                                                                 |
|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| NOT attributes.myAttribute:cde                                       | Query per gruppi di oggetti in cui l'attributo denominato "myAttribute" non è "cde".                                      |
| parentGroupNames:(myParentThingGroupName)                            | Query per gruppi di oggetti il cui nome del gruppo padre corrisponde a "myParentThingGroupName".                          |
| parentGroupNames:(myParentThingGroupName<br>OR myRootThingGroupName) | Query per gruppi di oggetti il cui nome del gruppo padre corrisponde a "myParentThingGroupName" o "myRootThingGroupName". |
| parentGroupNames:(myParentThingGroupNa*)                             | Query per gruppi di oggetti il cui nome del gruppo padre inizia con "myParentThingGroupNa".                               |

# AWS IoT Device Defender

AWS IoT Device Defender è un servizio di sicurezza che permette di eseguire l'audit della configurazione dei dispositivi, monitorare i dispositivi connessi per rilevare eventuali comportamenti anomali e mitigare i rischi di sicurezza. Offre la possibilità di applicare policy di sicurezza coerenti in tutto il parco istanze di dispositivi AWS IoT e di rispondere rapidamente quando i dispositivi vengono compromessi.

I parchi istanze IoT possono essere costituiti da un numero elevato di dispositivi con funzionalità diverse, usati per lunghi periodi di tempo e distribuiti in varie aree geografiche. Queste caratteristiche rendono la configurazione di un parco istanze complessa e soggetta a errori. E poiché i dispositivi presentano spesso vincoli di potenza di elaborazione, memoria e capacità di storage, ciò limita l'uso della crittografia e di altre forme di sicurezza nei dispositivi stessi. I dispositivi, inoltre, usano spesso software con vulnerabilità note. La combinazione di questi fattori rende i parchi istanze IoT un facile bersaglio per gli hacker e rende difficile la protezione continuativa di un parco istanze di dispositivi.

AWS IoT Device Defender risolve queste sfide fornendo strumenti per identificare i problemi di sicurezza e il mancato rispetto delle best practice. AWS IoT Device Defender è in grado di eseguire l'auditing dei parchi istanze di dispositivi per verificare che vengano rispettate le best practice di sicurezza e per rilevare eventuali comportamenti anomali.

## Note

AWS IoT Device Defender non è disponibile nella regione Cina (Pechino).

## Audit

Un audit di AWS IoT Device Defender analizza le impostazioni e le policy correlate ad account e dispositivi per garantire l'applicazione delle misure di sicurezza. Un audit può aiutarti a individuare eventuali scostamenti dalle best practice di sicurezza o policy di accesso adeguate, come nel caso di più dispositivi che usano la stessa identità, o policy troppo permissive che consentono a un dispositivo di leggere e aggiornare i dati per molti altri dispositivi. È possibile eseguire audit in base alle necessità (audit on demand) oppure pianificarli per l'esecuzione periodica (audit pianificati).

Un audit di AWS IoT Device Defender esegue un set di controlli predefiniti relativi a vulnerabilità dei dispositivi e best practice di sicurezza IoT comuni. Tra i controlli predefiniti vi sono le policy che concedono l'autorizzazione per leggere o aggiornare i dati in più dispositivi, i dispositivi che condividono un'identità (certificato X.509) o i certificati in scadenza o che sono stati revocati ma sono ancora attivi.

## Controlli di auditing

### Note

Quando un controllo viene abilitato, la raccolta dei dati inizia immediatamente. Se nell'account è presente una quantità elevata di dati da raccogliere, i risultati del controllo potrebbero non essere disponibili per alcuni minuti dopo l'abilitazione.

Sono supportati i controlli di auditing seguenti:

REVOKED\_CA\_CERT\_CHECK

Un certificato CA è stato revocato, ma è ancora attivo in AWS IoT.

Gravità: Critico

#### Details (1)

Un certificato CA è contrassegnato come revocato nell'elenco di revoche di certificati gestito dall'autorità emittente, ma è ancora contrassegnato come "ACTIVE" o "PENDING\_TRANSFER" in AWS IoT.

Quando questo controllo trova un certificato CA non conforme, vengono restituiti i codici motivo seguenti:

- CERTIFICATE\_REVOKED\_BY\_ISSUER

#### Why it matters (1)

Un certificato CA revocato non deve più essere usato per firmare i certificati dei dispositivi. È possibile che sia stato revocato perché è compromesso. I nuovi dispositivi aggiunti con certificati firmati utilizzando questo certificato CA possono rappresentare una minaccia per la sicurezza.

#### How to fix it (1)

1. Utilizza [UpdateCACertificate](#) per contrassegnare il certificato CA come INATTIVO AWS IoT .
2. Rivedi l'attività di registrazione del certificato del dispositivo nel periodo successivo alla revoca del certificato CA e prendi in considerazione la possibilità di revocare eventuali certificati del dispositivo che possono essere stati emessi durante tale periodo. Usa [ListCertificatesByCA](#) per elencare i certificati del dispositivo firmati dal certificato CA e [UpdateCertificate](#) per revocare un certificato del dispositivo.

### DEVICE\_CERTIFICATE\_SHARED\_CHECK

Connessioni multiple e simultanee usano lo stesso certificato X.509 per l'autenticazione con AWS IoT.

Gravità: Critico

#### Details (2)

Quando questo controllo viene abilitato, la raccolta di dati viene avviata immediatamente, ma i risultati del controllo non sono disponibili per almeno due ore.

Quando viene eseguito come parte di un audit on demand, questo controllo cerca i certificati e gli ID client usati dai dispositivi per connettersi durante i 31 giorni precedenti l'inizio dell'audit. Per gli audit pianificati, questo controllo analizza i dati dall'ultima esecuzione dell'audit fino all'avvio di questa istanza dell'audit. Se hai eseguito operazioni per mitigare questa condizione nell'intervallo di tempo controllato, esamina quando sono state stabilite le connessioni simultanee per determinare se il problema persiste.

Quando questo controllo trova un certificato non conforme, vengono restituiti i codici motivo seguenti:

- CERTIFICATE\_SHARED\_BY\_MULTIPLE\_DEVICES

I risultati restituiti da questo controllo includono inoltre l'ID del certificato condiviso, gli ID dei client che usano il certificato per connettersi e gli orari di connessione/disconnessione. La maggior parte dei risultati recenti viene elencata per prima.

#### Why it matters (2)

Ogni dispositivo deve avere un certificato univoco per eseguire l'autenticazione con AWS IoT. Quando più dispositivi utilizzano lo stesso certificato, questo può indicare che un dispositivo è stato compromesso. L'identità potrebbe essere stata clonata per compromettere ulteriormente il sistema.

## How to fix it (2)

Verifica che il certificato del dispositivo non sia stato compromesso. In caso affermativo, segui le best practice di sicurezza per mitigare la situazione.

Se stai usando lo stesso certificato in più dispositivi, puoi eseguire queste operazioni:

1. Effettuare il provisioning di nuovi certificati univoci e collegarli a ciascun dispositivo.
2. Verificare che i nuovi certificati siano validi e che i dispositivi siano in grado di usarli per connettersi.
3. Utilizza [UpdateCertificate](#) per contrassegnare il certificato precedente come REVOCATO in AWS IoT.
4. Distaccare il vecchio certificato da ogni dispositivo.

## UNAUTHENTICATED\_COGNITO\_ROLE\_OVERLY\_PERMISSIVE\_CHECK

Una policy collegata a un ruolo di un pool di identità Amazon Cognito non autenticato è considerata troppo permissiva perché concede l'autorizzazione per eseguire le operazioni AWS IoT seguenti:

- gestire o modificare gli oggetti
- leggere i dati amministrativi degli oggetti
- gestire le risorse o i dati non correlati agli oggetti

Oppure, perché concede l'autorizzazione per eseguire le operazioni AWS IoT seguenti su un'ampia gamma di dispositivi:

- usare MQTT per connettersi a/pubblicare/sottoscrivere argomenti riservati (tra cui dati di esecuzione dei processi o copie shadow)
- usare comandi API per leggere o modificare dati di esecuzione dei processi o copie shadow

In generale, i dispositivi che si connettono usando un ruolo di un pool di identità Amazon Cognito non autenticato devono avere solo autorizzazioni limitate per pubblicare/sottoscrivere argomenti MQTT specifici degli oggetti o usare comandi API per leggere/modificare dati specifici degli oggetti correlati a dati di esecuzione dei processi o copie shadow.

Gravità: Critico

## manage or modify things (3)

Le operazioni API di AWS IoT seguenti vengono usate per gestire o modificare gli oggetti in modo che non sia necessario concedere l'autorizzazione per l'esecuzione di queste operazioni ai dispositivi che si connettono tramite un pool di identità Amazon Cognito non autenticato:

- `AddThingToThingGroup`
- `AttachThingPrincipal`
- `CreateThing`
- `DeleteThing`
- `DetachThingPrincipal`
- `ListThings`
- `ListThingsInThingGroup`
- `RegisterThing`
- `RemoveThingFromThingGroup`
- `UpdateThing`

- `UpdateThingGroupsForThing`

Qualsiasi ruolo che concede l'autorizzazione per eseguire queste operazioni anche su una singola risorsa è considerato non conforme.

#### read thing administrative data (3)

Le operazioni API di AWS IoT seguenti vengono usate per leggere o modificare i dati degli oggetti in modo che ai dispositivi che si connettono tramite un pool di identità Amazon Cognito non autenticato non sia necessario concedere l'autorizzazione per l'esecuzione di queste operazioni:

- `DescribeThing`
- `ListJobExecutionsForThing`
- `ListThingGroupsForThing`
- `ListThingPrincipals`

Esempio:

- noncompliant:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iot:DescribeThing",
 "iot>ListJobExecutionsForThing",
 "iot>ListThingGroupsForThing",
 "iot>ListThingPrincipals"
],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:/thing/MyThing"
]
 }
]
}
```

In questo modo il dispositivo può eseguire le operazioni specificate anche se concesse solo per un oggetto specifico.

#### manage non-things (3)

I dispositivi che si connettono tramite un pool di identità Amazon Cognito non autenticato non devono avere il permesso di eseguire azioni API AWS IoT diverse da quelle discusse in queste sezioni. Per gestire l'account con un'applicazione che si connette tramite un pool di identità Amazon Cognito non autenticato, crea un pool di identità separato non usato dai dispositivi.

#### subscribe/publish to MQTT topics (3)

I messaggi MQTT vengono inviati tramite il broker di messaggi AWS IoT e sono usati dai dispositivi per eseguire numerose operazioni, tra cui l'accesso allo stato delle copie shadow e dell'esecuzione dei processi e la modifica di tali stati. Una policy che concede a un dispositivo l'autorizzazione di connessione, pubblicazione o sottoscrizione per i messaggi MQTT deve limitare queste operazioni a risorse specifiche, come illustrato di seguito:

##### Connessione

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:client/*
```

Il carattere jolly \* permette a qualsiasi dispositivo di connettersi a AWS IoT.

```
arn:aws:iot:<region>:<account-id>:client/${iot:ClientId}
```

Se `iot:Connection.Thing.IsAttached` non è impostato su "true" nelle chiavi delle condizioni, questo equivale al carattere jolly\* dell'esempio precedente.

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": ["iot:Connect"],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:client/
${iot:Connection.Thing.ThingName}"
],
 "Condition": {
 "Bool": { "iot:Connection.Thing.IsAttached": "true" }
 }
 }
]
}
```

La risorsa specifica contiene una variabile che corrisponde al nome del dispositivo utilizzato per connettersi. L'istruzione condizionale limita ulteriormente il permesso controllando che il certificato utilizzato dal client MQTT corrisponda a quello associato all'oggetto con il nome utilizzato.

#### Pubblicare

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:topic/$aws/things/*shadow/update
```

Questo esempio permette al dispositivo di aggiornare la copia shadow di qualsiasi dispositivo (\* = tutti i dispositivi).

```
arn:aws:iot:<region>:<account-id>:topic/$aws/things/*
```

Questo esempio permette al dispositivo di leggere/aggiornare/eliminare la copia shadow di qualsiasi dispositivo.

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": ["iot:Publish"],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/*"
],
 }
]
}
```

```
 }
]
}
```

La specifica della risorsa contiene un carattere jolly, che tuttavia corrisponde solo agli argomenti correlati alla copia shadow per il dispositivo il cui nome di oggetto viene usato per la connessione.

#### Sottoscrivi

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

Questo esempio permette al dispositivo di sottoscrivere le copie shadow riservate o gli argomenti dei processi per tutti i dispositivi.

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

Equivale all'esempio precedente, ma con l'uso del carattere jolly #.

```
arn:aws:iot:<region>:<account-id>:topic/$aws/things/#/shadow/update
```

Questo esempio permette al dispositivo di visualizzare gli aggiornamenti delle copie shadow di qualsiasi dispositivo (+ = tutti i dispositivi).

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": ["iot:Subscribe"],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/
 ${iot:Connection.Thing.ThingName}/shadow/*"
 "arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/
 ${iot:Connection.Thing.ThingName}/jobs/*"
],
 }
]
}
```

Le specifiche della risorsa contengono caratteri jolly, che tuttavia corrispondono solo agli argomenti correlati alla copia shadow e agli argomenti correlati ai processi per il dispositivo il cui nome di oggetto viene usato per la connessione.

#### Ricezione

- conforme:

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

Questo esempio è appropriato perché il dispositivo può ricevere solo i messaggi dagli argomenti per i quali ha l'autorizzazione alla sottoscrizione.

### read/modify shadow or job data (3)

Una policy che concede a un dispositivo l'autorizzazione per eseguire un'operazione API per l'accesso a o la modifica di copie shadow dei dispositivi o dati di esecuzione dei processi deve limitare queste operazioni a risorse specifiche. Le operazioni API sono le seguenti:

- `DeleteThingShadow`
- `GetThingShadow`
- `UpdateThingShadow`
- `DescribeJobExecution`
- `GetPendingJobExecutions`
- `StartNextPendingJobExecution`
- `UpdateJobExecution`

Esempi:

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:thing/*
```

Questo esempio permette al dispositivo di eseguire l'operazione specificata su qualsiasi oggetto.

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iot:DeleteThingShadow",
 "iot:GetThingShadow",
 "iot:UpdateThingShadow",
 "iot:DescribeJobExecution",
 "iot:GetPendingJobExecutions",
 "iot:StartNextPendingJobExecution",
 "iot:UpdateJobExecution"
],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:/thing/MyThing1",
 "arn:aws:iot:<region>:<account-id>:/thing/MyThing2"
]
 }
]
}
```

In questo modo il dispositivo può eseguire le operazioni specificate su due oggetti soltanto.

### Details (3)

Per questo controllo, AWS IoT Device Defender esegue l'audit di tutti i pool di identità Amazon Cognito che sono stati usati per la connessione al broker di messaggi AWS IoT durante gli ultimi 31 giorni precedenti l'esecuzione dell'audit. Tutti i pool di identità Amazon Cognito da cui si è connessa un'identità Amazon Cognito autenticata o non autenticata vengono inclusi nell'audit.

Quando questo controllo trova un ruolo di un pool di identità Amazon Cognito non autenticato e non conforme, vengono restituiti i codici motivo seguenti:

- ALLOWS\_ACCESS\_TO\_IOT\_ADMIN\_ACTIONS
- ALLOWS\_BROAD\_ACCESS\_TO\_IOT\_DATA\_PLANE\_ACTIONS

#### Why it matters (3)

Poiché le identità non autenticate non vengono mai autenticate dall'utente, rappresentano un rischio molto maggiore rispetto alle identità Amazon Cognito autenticate. Se un'identità non autenticata viene compromessa, potrebbe usare le operazioni amministrative per modificare le impostazioni dell'account, eliminare le risorse o ottenere l'accesso a dati sensibili. Oppure, con un accesso alle impostazioni dei dispositivi più su vasta scala, potrebbe accedere alle copie shadow e ai processi per tutti i dispositivi nell'account e modificarli. Un utente guest potrebbe usare le autorizzazioni per compromettere l'intero parco istanze o sferrare un attacco DDOS con i messaggi.

#### How to fix it (3)

Una policy collegata a un ruolo di un pool di identità Amazon Cognito non autenticato deve concedere solo le autorizzazioni di cui un dispositivo necessita per eseguire la propria operazione. È consigliabile eseguire le operazioni seguenti:

1. Creare un nuovo ruolo conforme.
2. Creare un nuovo pool di identità Amazon Cognito e collegare a esso il ruolo conforme.
3. Verificare che le identità possano accedere a AWS IoT usando il nuovo pool.
4. Una volta completata la verifica, collegare il nuovo ruolo conforme al pool di identità Amazon Cognito contrassegnato come non conforme.

#### AUTHENTICATED\_COGNITO\_ROLE\_OVERLY\_PERMISSIVE\_CHECK

Una policy collegata a un ruolo di un pool di identità Amazon Cognito autenticato è considerata troppo permissiva perché concede l'autorizzazione per eseguire le operazioni AWS IoT seguenti:

- gestire o modificare gli oggetti
- gestire le risorse o i dati non correlati agli oggetti

Oppure, perché concede l'autorizzazione per eseguire le operazioni AWS IoT seguenti su un'ampia gamma di dispositivi:

- leggere i dati amministrativi degli oggetti
- usare MQTT per connettersi a/pubblicare/sottoscrivere argomenti riservati (tra cui dati di esecuzione dei processi o copie shadow)
- usare comandi API per leggere o modificare dati di esecuzione dei processi o copie shadow

In generale, i dispositivi che si connettono usando un ruolo di un pool di identità Amazon Cognito autenticato devono avere solo autorizzazioni limitate per leggere i dati amministrativi specifici degli oggetti, pubblicare/sottoscrivere argomenti MQTT specifici degli oggetti o usare comandi API per leggere/modificare dati specifici degli oggetti correlati a dati di esecuzione dei processi o copie shadow.

Gravità: Critico

#### Manage or modify things (4)

Le operazioni API di AWS IoT seguenti vengono usate per gestire o modificare gli oggetti in modo che non sia necessario concedere le autorizzazioni per l'esecuzione di queste operazioni ai dispositivi che si connettono tramite un pool di identità Amazon Cognito autenticato:

- AddThingToThingGroup
- AttachThingPrincipal
- CreateThing
- DeleteThing
- DetachThingPrincipal
- ListThings
- ListThingsInThingGroup
- RegisterThing
- RemoveThingFromThingGroup
- UpdateThing
- UpdateThingGroupsForThing

Qualsiasi ruolo che concede l'autorizzazione per eseguire queste operazioni anche su una singola risorsa è considerato non conforme.

#### manage non-things (4)

I dispositivi che si connettono tramite un pool di identità di Amazon Cognito autenticato non devono avere il permesso di eseguire operazioni API AWS IoT diverse da quelle discusse in queste sezioni. Per gestire l'account con un'applicazione che si connette tramite un pool di identità Amazon Cognito autenticato, crea un pool di identità separato non usato dai dispositivi.

#### read thing administrative data (4)

Le operazioni API di AWS IoT seguenti vengono usate per leggere i dati degli oggetti in modo che ai dispositivi che si connettono tramite un pool di identità Amazon Cognito autenticato vengano concesse le autorizzazioni per l'esecuzione di queste operazioni solo su un set limitato di oggetti:

- DescribeThing
- ListJobExecutionsForThing
- ListThingGroupsForThing
- ListThingPrincipals

Esempi:

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:thing/*
```

Questo esempio permette al dispositivo di eseguire l'operazione specificata su qualsiasi oggetto.

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iot:DescribeThing",
 "iot>ListJobExecutionsForThing",
 "iot>ListThingGroupsForThing",
 "iot>ListThingPrincipals"
],
 }
]
}
```

```
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:/thing/MyThing"
]
}
}
```

Questo esempio permette al dispositivo di eseguire le operazioni specificate solo su un oggetto specifico.

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iot:DescribeThing",
 "iot>ListJobExecutionsForThing",
 "iot>ListThingGroupsForThing",
 "iot>ListThingPrincipals"
],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:/thing/MyThing*"
]
 }
]
}
```

Questo esempio è conforme perché, sebbene la risorsa sia specificata con un carattere jolly (\*), il carattere è preceduto da una stringa specifica, che limita il set di oggetti accessibili a quelli con i nomi che hanno il prefisso specificato.

#### subscribe/publish to MQTT topics (4)

I messaggi MQTT vengono inviati tramite il broker di messaggi AWS IoT e sono usati dai dispositivi per eseguire numerose operazioni, tra cui l'accesso allo stato delle copie shadow e dell'esecuzione dei processi e la modifica di tali stati. Una policy che concede a un dispositivo l'autorizzazione di connessione, pubblicazione o sottoscrizione per i messaggi MQTT deve limitare queste operazioni a risorse specifiche, come illustrato di seguito:

##### Connessione

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:client/*
```

Il carattere jolly \* permette a qualsiasi dispositivo di connettersi a AWS IoT.

```
arn:aws:iot:<region>:<account-id>:client/${iot:ClientId}
```

Se `iot:Connection.Thing.IsAttached` non è impostato su "true" nelle chiavi delle condizioni, questo equivale al carattere jolly\* dell'esempio precedente.

- conforme:

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

```
{
 "Effect": "Allow",
 "Action": ["iot:Connect"],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:client/
 ${iot:Connection.Thing.ThingName}"
],
 "Condition": {
 "Bool": { "iot:Connection.Thing.IsAttached": "true" }
 }
}
```

La specifica della risorsa contiene una variabile che corrisponde al nome del dispositivo usato per la connessione e l'istruzione di condizione limita ulteriormente l'autorizzazione controllando che il certificato usato dal client MQTT corrisponda a quello collegato all'oggetto con il nome usato.

#### Pubblicare

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:topic/$aws/things/*/shadow/update
```

Questo esempio permette al dispositivo di aggiornare la copia shadow di qualsiasi dispositivo (\* = tutti i dispositivi).

```
arn:aws:iot:<region>:<account-id>:topic/$aws/things/*
```

Questo esempio permette al dispositivo di leggere/aggiornare/eliminare la copia shadow di qualsiasi dispositivo.

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": ["iot:Publish"],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:topic/$aws/things/
 ${iot:Connection.Thing.ThingName}/shadow/*"
],
 }
]
}
```

La specifica della risorsa contiene un carattere jolly, che tuttavia corrisponde solo agli argomenti correlati alla copia shadow per il dispositivo il cui nome di oggetto viene usato per la connessione.

#### Sottoscrivere

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

Questo esempio permette al dispositivo di sottoscrivere le copie shadow riservate o gli argomenti dei processi per tutti i dispositivi.

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/#
```

Equivale all'esempio precedente, ma con l'uso del carattere jolly #.

```
arn:aws:iot:<region>:<account-id>:topic/$aws/things/+/_shadow/update
```

Questo esempio permette al dispositivo di visualizzare gli aggiornamenti delle copie shadow di qualsiasi dispositivo (+ = tutti i dispositivi).

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": ["iot:Subscribe"],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/
 ${iot:Connection.Thing.ThingName}/shadow/*"
 "arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/
 ${iot:Connection.Thing.ThingName}/jobs/*"
],
 }
]
}
```

Le specifiche della risorsa contengono caratteri jolly, che tuttavia corrispondono solo agli argomenti correlati alla copia shadow e agli argomenti correlati ai processi per il dispositivo il cui nome di oggetto viene usato per la connessione.

#### Ricezione

- conforme:

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

Questo esempio è appropriato perché il dispositivo può ricevere solo i messaggi dagli argomenti per i quali ha l'autorizzazione alla sottoscrizione.

#### read/modify shadow or job data (4)

Una policy che concede a un dispositivo l'autorizzazione per eseguire un'operazione API per l'accesso a o la modifica di copie shadow dei dispositivi o dati di esecuzione dei processi deve limitare queste operazioni a risorse specifiche. Le operazioni API sono le seguenti:

- DeleteThingShadow
- GetThingShadow
- UpdateThingShadow
- DescribeJobExecution
- GetPendingJobExecutions
- StartNextPendingJobExecution
- UpdateJobExecution

Esempi:

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:thing/*
```

Questo esempio permette al dispositivo di eseguire l'operazione specificata su qualsiasi oggetto.

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iot:DeleteThingShadow",
 "iot:GetThingShadow",
 "iot:UpdateThingShadow",
 "iot:DescribeJobExecution",
 "iot:GetPendingJobExecutions",
 "iot:StartNextPendingJobExecution",
 "iot:UpdateJobExecution"
],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:/thing/MyThing1",
 "arn:aws:iot:<region>:<account-id>:/thing/MyThing2"
]
 }
]
}
```

Questo esempio permette al dispositivo di eseguire le operazioni specificate solo su due oggetti specifici.

#### Details (4)

Per questo controllo, AWS IoT Device Defender esegue l'audit di tutti i pool di identità Amazon Cognito che sono stati usati per la connessione al broker di messaggi AWS IoT durante gli ultimi 31 giorni precedenti l'esecuzione dell'audit. Tutti i pool di identità Amazon Cognito da cui si è connessa un'identità Amazon Cognito autenticata o non autenticata vengono inclusi nell'audit.

Quando questo controllo trova un ruolo di un pool di identità Amazon Cognito autenticato non conforme, vengono restituiti i codici motivo seguenti:

- ALLOWS\_BROAD\_ACCESS\_TO\_IOT\_THING\_ADMIN\_READ\_ACTIONS
- ALLOWS\_ACCESS\_TO\_IOT\_NON\_THING\_ADMIN\_ACTIONS
- ALLOWS\_ACCESS\_TO\_IOT\_THING\_ADMIN\_WRITE\_ACTIONS

#### Why it matters (4)

Se un'identità autenticata viene compromessa, potrebbe usare le operazioni amministrative per modificare le impostazioni dell'account, eliminare le risorse o ottenere l'accesso ai dati sensibili.

#### How to fix it (4)

Una policy collegata a un ruolo di un pool di identità Amazon Cognito autenticato deve concedere solo le autorizzazioni di cui un dispositivo necessita. È consigliabile eseguire le operazioni seguenti:

1. Creare un nuovo ruolo conforme.
2. Creare un nuovo pool di identità Amazon Cognito e collegare a esso il ruolo conforme.

3. Verificare che le identità possano accedere a AWS IoT usando il nuovo pool.
4. Una volta completata la verifica, collegare il ruolo per il pool di identità Amazon Cognito che è stato contrassegnato come non compatibile.

## IOT\_POLICY\_OVERLY\_PERMISSIVE\_CHECK

Una policy AWS IoT concede autorizzazioni troppo ampie/illimitate. Concede l'autorizzazione per inviare o ricevere messaggi MQTT per un'ampia gamma di dispositivi oppure concede l'autorizzazione per accedere ai dati di esecuzione dei processi o alle copie shadow o per modificare tali dati per un'ampia gamma di dispositivi.

In generale, una policy per un dispositivo deve concedere l'accesso a risorse associate solo al dispositivo interessato e a nessun altro dispositivo oppure a pochi altri. Con alcune eccezioni, l'uso di un carattere jolly (ad esempio`"*"`) per specificare le risorse in una policy è considerato troppo ampio/illimitato.

Gravità: Critico

### MQTT permissions (5)

I messaggi MQTT vengono inviati tramite il broker di messaggi AWS IoT e sono usati dai dispositivi per eseguire numerose operazioni, tra cui l'accesso allo stato delle copie shadow e dell'esecuzione dei processi e la modifica di tali stati. Una policy che concede a un dispositivo l'autorizzazione di connessione, pubblicazione o sottoscrizione per i messaggi MQTT deve limitare queste operazioni a risorse specifiche, come illustrato di seguito:

#### Connessione

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:client/*
```

Il carattere jolly `*` permette a qualsiasi dispositivo di connettersi a AWS IoT.

```
arn:aws:iot:<region>:<account-id>:client/${iot:ClientId}
```

Se `iot:Connection.Thing.IsAttached` non è impostato su "true" nelle chiavi delle condizioni, questo equivale al carattere jolly `*` come nell'esempio precedente.

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": ["iot:Connect"],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:client/
${iot:Connection.Thing.ThingName}"
],
 "Condition": {
 "Bool": { "iot:Connection.Thing.IsAttached": "true" }
 }
 }
]
}
```

La risorsa specifica contiene una variabile che corrisponde al nome del dispositivo utilizzato per connettersi. L'istruzione condizionale limita ulteriormente il permesso controllando che il certificato utilizzato dal client MQTT corrisponda a quello associato all'oggetto con il nome utilizzato.

#### Pubblicare

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:topic/$aws/things/*/shadow/update
```

Questo esempio permette al dispositivo di aggiornare la copia shadow di qualsiasi dispositivo (\* = tutti i dispositivi).

```
arn:aws:iot:<region>:<account-id>:topic/$aws/things/*
```

Questo esempio permette al dispositivo di leggere/aggiornare/eliminare la copia shadow di qualsiasi dispositivo.

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": ["iot:Publish"],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/*"
],
 }
]
}
```

La specifica della risorsa contiene un carattere jolly, che tuttavia corrisponde solo agli argomenti correlati alla copia shadow per il dispositivo il cui nome di oggetto viene usato per la connessione.

#### Sottoscrivere

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

Questo esempio permette al dispositivo di sottoscrivere le copie shadow riservate o gli argomenti dei processi per tutti i dispositivi.

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

Equivale all'esempio precedente, ma con l'uso del carattere jolly #.

```
arn:aws:iot:<region>:<account-id>:topic/$aws/things/+shadow/update
```

Questo esempio permette al dispositivo di visualizzare gli aggiornamenti delle copie shadow di qualsiasi dispositivo (+ = tutti i dispositivi).

- conforme:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": ["iot:Subscribe"],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/*"
 "arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/jobs/*"
],
 }
]
}
```

Le specifiche della risorsa contengono caratteri jolly, che tuttavia corrispondono solo agli argomenti correlati alla copia shadow e agli argomenti correlati ai processi per il dispositivo il cui nome di oggetto viene usato per la connessione.

#### Ricezione

- conforme:

```
arn:aws:iot:<region>:<account-id>:topicfilter/$aws/things/*
```

Questo esempio è appropriato perché il dispositivo può ricevere solo i messaggi dagli argomenti per i quali ha l'autorizzazione di sottoscrizione.

#### shadow and job permissions (5)

Una policy che concede a un dispositivo l'autorizzazione per eseguire un'operazione API per l'accesso a o la modifica di copie shadow dei dispositivi o dati di esecuzione dei processi deve limitare queste operazioni a risorse specifiche. Le operazioni API sono le seguenti:

- DeleteThingShadow
- GetThingShadow
- UpdateThingShadow
- DescribeJobExecution
- GetPendingJobExecutions
- StartNextPendingJobExecution
- UpdateJobExecution

Esempi:

- noncompliant:

```
arn:aws:iot:<region>:<account-id>:thing/*
```

Questo esempio permette al dispositivo di eseguire l'operazione specificata su qualsiasi oggetto.

- conforme:

```
{
 "Version": "2012-10-17",
}
```

```
"Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iot:DeleteThingShadow",
 "iot:GetThingShadow",
 "iot:UpdateThingShadow",
 "iot:DescribeJobExecution",
 "iot:GetPendingJobExecutions",
 "iot:StartNextPendingJobExecution",
 "iot:UpdateJobExecution"
],
 "Resource": [
 "arn:aws:iot:<region>:<account-id>:/thing/MyThing1",
 "arn:aws:iot:<region>:<account-id>:/thing/MyThing2"
]
 }
]
```

Questo esempio permette al dispositivo di eseguire le operazioni specificate solo su due oggetti specifici.

#### Details (5)

Quando questo controllo trova una policy IoT non conforme, viene restituito il codice motivo seguente:

- ALLOWS\_BROAD\_ACCESS\_TO\_IOT\_DATA\_PLANE\_ACTIONS

#### Why it matters (5)

Un certificato, un'identità Amazon Cognito o un gruppo di oggetti con una policy eccessivamente permissiva può, se compromesso, avere un impatto sulla sicurezza di tutto l'account. Un utente malintenzionato potrebbe sfruttare tale accesso ampio per leggere o modificare copie shadow, processi o esecuzioni dei processi per tutti i dispositivi. Oppure un utente malintenzionato potrebbe usare un certificato compromesso per connettere dispositivi dannosi o sferrare un attacco DDOS nella rete.

#### How to fix it (5)

Segui queste fasi per correggere eventuali policy non conformi collegate a oggetti, gruppi di oggetti o altre entità:

1. Utilizza [CreatePolicyVersion](#) per creare una nuova versione conforme ai requisiti della policy. Imposta il flag `setAsDefault` su "true". (In questo modo questa nuova versione è operativa per tutte le entità che utilizzano la policy.)
2. Utilizza [ListTargetsForPolicy](#) per ottenere un elenco dei target (certificati, gruppi di oggetti) a cui è collegata la policy e stabilire quali dispositivi sono inclusi nei gruppi o quali utilizzano i certificati per connettersi.
3. Verificare che tutti i dispositivi associati possano connettersi a AWS IoT. Se un dispositivo non è in grado di connettersi, eseguire il rollback della policy predefinita alla versione precedente usando [SetPolicyVersion](#), rivedere la policy e riprovare.

Usare le [variabili delle policy AWS IoT](#) per fare riferimento in modo dinamico a risorse AWS IoT specifiche nelle policy.

## CA\_CERT\_APPROACHING\_EXPIRATION\_CHECK

Un certificato CA è in scadenza tra 30 giorni o è scaduto.

Gravità: Medium (media)

### Details (6)

Questo controllo si applica ai certificati CA contrassegnati come "ACTIVE" o "PENDING\_TRANSFER".

Quando questo controllo trova un certificato CA non conforme, vengono restituiti i codici motivo seguenti:

- CERTIFICATE\_APPROACHING\_EXPIRATION
- CERTIFICATE\_PAST\_EXPIRATION

### Why it matters (6)

Un certificato CA scaduto non deve più essere usato per firmare i nuovi certificati dei dispositivi.

### How to fix it (6)

Consulta le best practice sulla sicurezza per sapere come procedere. È possibile:

1. Registrare un nuovo certificato CA con AWS IoT.
2. Verificare di poter accedere ai certificati del dispositivo utilizzando il nuovo certificato CA.
3. Utilizzare [UpdateCACertificate](#) per contrassegnare i precedenti certificati CA come INATTIVI in AWS IoT.

## CONFLICTING\_CLIENT\_IDS\_CHECK

Più dispositivi si connettono usando lo stesso ID client.

Gravità: High (alta)

### Details (7)

Sono state stabilite diverse connessioni usando lo stesso ID client e di conseguenza un dispositivo già connesso è stato disconnesso. La specifica MQTT permette una sola connessione attiva per ID client, pertanto quando un altro dispositivo si connette usando lo stesso ID client, la connessione del dispositivo precedente viene interrotta.

Quando viene eseguito come parte di un audit on demand, questo controllo esamina come sono stati usati gli ID client per le connessioni durante i 31 giorni precedenti l'inizio dell'audit. Per gli audit pianificati, questo controllo analizza i dati dall'ultima esecuzione dell'audit fino all'avvio di questa istanza dell'audit. Se hai eseguito operazioni per mitigare questa condizione nell'intervallo di tempo controllato, esamina quando sono avvenute le connessioni/disconnessioni per determinare se il problema persiste.

Quando questo controllo trova una condizione di non conformità, vengono restituiti i codici motivo seguenti:

- DUPLICATE\_CLIENT\_ID\_ACROSS\_CONNECTIONS

I risultati restituiti da questo controllo includono inoltre l'ID client usato per connettersi, gli ID delle entità principali e gli orari di disconnessione. I risultati più recenti sono elencati per primi.

#### Why it matters (7)

I dispositivi con ID in conflitto sono costretti a riconnettersi continuamente e questo potrebbe causare la perdita di messaggi o l'impossibilità di connettersi da parte di un dispositivo.

Ciò può indicare che un dispositivo o le sue credenziali sono state compromesse e la causa potrebbe essere un attacco DDoS. È anche possibile che i dispositivi siano configurati in modo errato nell'account o che un dispositivo abbia una connessione malfunzionante e debba riconnettersi più volte al minuto.

#### How to fix it (7)

Registra ogni dispositivo come oggetto univoco in AWS IoT e usa il nome dell'oggetto come ID client per la connessione. In alternativa, usa un UUID come ID client per la connessione del dispositivo tramite MQTT.

### DEVICE\_CERT\_APPROACHING\_EXPIRATION\_CHECK

Un certificato di un dispositivo è in scadenza tra 30 giorni o è scaduto.

Gravità: Medium (media)

#### Details (8)

Questo controllo si applica ai certificati dei dispositivi contrassegnati come "ACTIVE" o "PENDING\_TRANSFER".

Quando questo controllo trova un certificato di un dispositivo non conforme, vengono restituiti i codici motivo seguenti:

- CERTIFICATE\_APPROACHING\_EXPIRATION
- CERTIFICATE\_PAST\_EXPIRATION

#### Why it matters (8)

Un certificato di un dispositivo non deve essere usato dopo la scadenza.

#### How to fix it (8)

Consulta le best practice sulla sicurezza per sapere come procedere. È possibile:

1. Effettuare il provisioning di un nuovo certificato e collegarlo al dispositivo.
2. Verificare che il nuovo certificato sia valido e che il dispositivo sia in grado di usarlo per connettersi.
3. Utilizzare [UpdateCertificate](#) per contrassegnare il certificato vecchio come INATTIVO in AWS IoT.
4. Scollegare il vecchio certificato dal dispositivo. (Consultare [DetachThingPrincipal](#)).

### REVOKED\_DEVICE\_CERT\_CHECK

Un certificato del dispositivo revocato è ancora attivo.

Gravità: Medium (media)

#### Details (9)

Un certificato del dispositivo si trova nell'[elenco di revoche di certificati](#) della CA, ma è ancora attivo in AWS IoT.

Questo controllo si applica ai certificati dei dispositivi contrassegnati come "ACTIVE" o "PENDING\_TRANSFER".

Quando questo controllo trova una condizione di non conformità, vengono restituiti i codici motivo seguenti:

- CERTIFICATE\_REVOKED\_BY\_ISSUER

#### Why it matters (9)

Un certificato di un dispositivo viene in genere revocato perché è stato compromesso. È possibile che non sia stato ancora revocato in AWS IoT a causa di un errore o di una svista.

#### How to fix it (9)

Verifica che il certificato del dispositivo non sia stato compromesso. In caso affermativo, seguì le best practice di sicurezza per mitigare la situazione. È possibile:

1. Effettuare il provisioning di un nuovo certificato per il dispositivo.
2. Verificare che il nuovo certificato sia valido e che il dispositivo sia in grado di usarlo per connettersi.
3. Utilizzare [UpdateCertificate](#) per contrassegnare il certificato precedente come "REVOCATO" in AWS IoT.
4. Scollegare il vecchio certificato dal dispositivo. (Consultare [DetachThingPrincipal](#)).

#### LOGGING\_DISABLED\_CHECK

I log AWS IoT non sono abilitati in CloudWatch.

Gravità: Low (bassa)

#### Details (10)

Quando questo controllo trova una condizione di non conformità, vengono restituiti i codici motivo seguenti:

- LOGGING\_DISABLED

#### Why it matters (10)

I log AWS IoT in CloudWatch forniscono visibilità sui comportamenti in AWS IoT, inclusi errori di autenticazione e connessioni e disconnessioni inattese che potrebbero indicare che un dispositivo è stato compromesso.

#### How to fix it (10)

Abilitare i log AWS IoT in CloudWatch. Consulta [Strumenti di monitoraggio](#).

## Come eseguire gli audit

1. Configurare le impostazioni di auditing per l'account. Usare [UpdateAccountAuditConfiguration](#) (p. 532) per abilitare i controlli da rendere disponibili per gli audit, configurare le notifiche opzionali e configurare le autorizzazioni.

Per alcuni controlli, AWS IoT avvia la raccolta di dati non appena il controllo è abilitato.

2. Creare una o più pianificazioni di audit. Usare [CreateScheduledAudit \(p. 536\)](#) per specificare i controlli da eseguire durante un audit e la frequenza di esecuzione degli audit.

In alternativa, è possibile eseguire un audit on demand, quando necessario. Usare [StartOnDemandAuditTask \(p. 545\)](#) per specificare i controlli da eseguire e avviare un audit immediatamente. (Se di recente è stato abilitato un controllo incluso nell'audit on demand, affinché i risultati siano pronti potrebbe essere necessario un po' di tempo).

3. È possibile usare la [console AWS IoT](#) per visualizzare i risultati degli audit.

In alternativa, è possibile visualizzare i risultati degli audit con [ListAuditFindings \(p. 552\)](#). Con questo comando, è possibile filtrare i risultati in base al tipo di controllo, a una risorsa specifica o a quando è stato eseguito l'audit. È possibile utilizzare queste informazioni per mitigare gli eventuali problemi rilevati.

## Notifiche

Quando un audit viene completato, è possibile inviare una notifica SNS con un riepilogo dei risultati di ogni controllo di eseguito, inclusi i dettagli relativi al numero di risorse non conformi trovate. Usa il campo `auditNotificationTargetConfigurations` nell'input del comando [UpdateAccountAuditConfiguration \(p. 532\)](#). La notifica SNS ha il payload seguente:

esempio di payload

```
{
 "accountId": "123456789012",
 "taskId": "4e2bcd1ccbc2a5dd15292a82ab80c380",
 "taskStatus": "FAILED|CANCELED|COMPLETED",
 "taskType": "ON_DEMAND_AUDIT_TASK|SCHEDULED_AUDIT_TASK",
 "scheduledAuditName": "myWeeklyAudit",
 "failedChecksCount": 0,
 "canceledChecksCount": 0,
 "nonCompliantChecksCount": 1,
 "compliantChecksCount": 0,
 "totalChecksCount": 1,
 "taskStartTime": 1524740766191,
 "auditDetails": [
 {
 "checkName": "DEVICE_CERT_APPROACHING_EXPIRATION_CHECK |
 REVOKED_DEVICE_CERT_CHECK |
 CA_CERT_APPROACHING_EXPIRATION_CHECK |
 REVOKED_CA_CERT_CHECK |
 DEVICE_CERTIFICATE_SHARED_CHECK |
 IOT_POLICY_UNRESTRICTED_CHECK |
 UNAUTHENTICATED_COGNITO_IDENTITY_UNRESTRICTED_ACCESS_CHECK |
 AUTHENTICATED_COGNITO_IDENTITY_UNRESTRICTED_ACCESS_CHECK |
 CONFLICTING_CLIENT_IDS_CHECK |
 LOGGING_DISABLED_CHECK",

 "checkRunStatus": "FAILED |
 CANCELED |
 COMPLETED_COMPLIANT |
 COMPLETED_NON_COMPLIANT",

 "nonCompliantResourcesCount": 1,
 "totalResourcesCount": 1,

 "message": "optional message if an error occurred",
 "errorCode": "INSUFFICIENT_PERMISSIONS|AUDIT_CHECK_DISABLED"
 }
]
}
```

}

#### schema JSON del payload

```

{
 "$schema": "http://json-schema.org/draft-07/schema#",
 "$id": "arn:aws:iot::::schema:auditnotification/1.0",
 "type": "object",
 "properties": {
 "accountId": {
 "type": "string"
 },
 "taskId": {
 "type": "string"
 },
 "taskStatus": {
 "type": "string",
 "enum": [
 "FAILED",
 "CANCELED",
 "COMPLETED"
]
 },
 "taskType": {
 "type": "string",
 "enum": [
 "SCHEDULED_AUDIT_TASK",
 "ON_DEMAND_AUDIT_TASK"
]
 },
 "scheduledAuditName": {
 "type": "string"
 },
 "failedChecksCount": {
 "type": "integer"
 },
 "canceledChecksCount": {
 "type": "integer"
 },
 "nonCompliantChecksCount": {
 "type": "integer"
 },
 "compliantChecksCount": {
 "type": "integer"
 },
 "totalChecksCount": {
 "type": "integer"
 },
 "taskStartTime": {
 "type": "integer"
 },
 "auditDetails": {
 "type": "array",
 "items": [
 {
 "type": "object",
 "properties": {
 "checkName": {
 "type": "string",
 "enum": [
 "DEVICE_CERT_APPROACHING_EXPIRATION_CHECK",
 "REVOKED_DEVICE_CERT_CHECK",
 "CA_CERT_APPROACHING_EXPIRATION_CHECK",
 "REVOKED_CA_CERT_CHECK",
 "REVOKED_CA_CERT_CHECK"
]
 }
 }
 }
]
 }
 }
}

```

```
 "LOGGING_DISABLED_CHECK"
],
},
"checkRunStatus": {
 "type": "string",
 "enum": [
 "FAILED",
 "CANCELED",
 "COMPLETED_COMPLIANT",
 "COMPLETED_NON_COMPLIANT"
]
},
"nonCompliantResourcesCount": {
 "type": "integer"
},
"totalResourcesCount": {
 "type": "integer"
},
"message": {
 "type": "string"
},
"errorCode": {
 "type": "string",
 "enum": [
 "INSUFFICIENT_PERMISSIONS",
 "AUDIT_CHECK_DISABLED"
]
},
"required": [
 "checkName",
 "checkRunStatus",
 "nonCompliantResourcesCount",
 "totalResourcesCount"
]
}
],
},
"required": [
 "accountId",
 "taskId",
 "taskStatus",
 "taskType",
 "failedChecksCount",
 "canceledChecksCount",
 "nonCompliantChecksCount",
 "compliantChecksCount",
 "totalChecksCount",
 "taskStartTime",
 "auditDetails"
]
}
```

Le notifiche possono anche essere visualizzate nella console AWS IoT insieme a informazioni aggiuntive sul dispositivo, statistiche del dispositivo (ad esempio, ora dell'ultima connessione, numero di connessioni attive, velocità di trasferimento dati) e avvisi cronologici per il dispositivo.

## Autorizzazioni

Questa sezione contiene informazioni su come configurare le policy e i ruoli AWS IoT Device Defender necessari per creare, eseguire e gestire gli audit di IAM. Per ulteriori informazioni, consulta la [Guida per l'utente di AWS Identity and Access Management](#).

## Concessione a AWS IoT Device Defender dell'autorizzazione per la raccolta dei dati per l'esecuzione di un audit.

Quando chiavi [UpdateAccountAuditConfiguration \(p. 532\)](#), devi specificare un ruolo IAM con due policy, una policy di autorizzazioni e una policy di trust. La policy di autorizzazioni concede a AWS IoT Device Defender l'autorizzazione per accedere ai dati dell'account, usando le API di AWS IoT, quando esegue un audit. La policy di attendibilità concede a AWS IoT Device Defender l'autorizzazione per assumere il ruolo richiesto.

[policy di autorizzazioni](#)

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iot:GetLoggingOptions",
 "iot:GetV2LoggingOptions",
 "iot>ListCACertificates",
 "iot>ListCertificates",
 "iot:DescribeCACertificate",
 "iot:DescribeCertificate",
 "iot>ListPolicies",
 "iot:GetPolicy",
 "iot:GetEffectivePolicies",
 "cognito-identity:GetIdentityPoolRoles",
 "iam>ListRolePolicies",
 "iam>ListAttachedRolePolicies",
 "iam:GetPolicy",
 "iam:GetPolicyVersion",
 "iam:GetRolePolicy"
],
 "Resource": [
 "*"
]
 }
]
}
```

[policy di attendibilità](#)

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "",
 "Effect": "Allow",
 "Principal": {
 "Service": "iot.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
```

## Concessione a AWS IoT Device Defender dell'autorizzazione per pubblicare le notifiche in un argomento SNS.

Se usi il parametro `auditNotificationTargetConfigurations` in [UpdateAccountAuditConfiguration \(p. 532\)](#), devi specificare un ruolo IAM con due policy, una policy di autorizzazioni e una policy di trust. La policy di autorizzazioni concede a AWS IoT Device Defender l'autorizzazione per pubblicare le notifiche nell'argomento SNS. La policy di attendibilità concede a AWS IoT Device Defender l'autorizzazione per assumere il ruolo richiesto.

[policy di autorizzazioni](#)

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "sns:Publish"
],
 "Resource": [
 "arn:aws:sns:region:account-id:your-topic-name"
]
 }
]
}
```

[policy di attendibilità](#)

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "",
 "Effect": "Allow",
 "Principal": {
 "Service": "iot.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
```

## Concessione ai gruppi o agli utenti IAM dell'autorizzazione per eseguire i comandi di auditing di AWS IoT Device Defender

Per permettere ai gruppi o agli utenti IAM di gestire, eseguire o visualizzare i risultati degli audit di AWS IoT Device Defender, devi creare e assegnare ruoli con policy collegate che concedono l'autorizzazione per eseguire i comandi appropriati. Il contenuto di ciascuna policy dipende da quali comandi si desidera che l'utente o il gruppo eseguano.

- [UpdateAccountAuditConfiguration](#)

[policy](#)

NOTA: devi creare il ruolo IAM con la policy collegata nello stesso account da cui viene eseguito il comando. L'accesso tra account non è permesso. La policy deve avere le autorizzazioni `iam:PassRole` (autorizzazioni per passare il ruolo).

Nel modello di policy seguente `audit-permissions-role-arn` è il ruolo Arn passato a AWS IoT Device Defender nella richiesta `UpdateAccountAuditConfiguration` usando il parametro `roleArn`. `audit-notifications-permissions-role-arn` è il ruolo Arn passato a AWS IoT Device Defender nella richiesta `UpdateAccountAuditConfiguration` usando il parametro `auditNotificationTargetConfigurations`.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iot:UpdateAccountAuditConfiguration"
],
 "Resource": [
 "*"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "iam:PassRole"
],
 "Resource": [
 "arn:aws:iam::account-id:role/audit-permissions-role-arn",
 "arn:aws:iam::account-id:role/audit-notifications-permissions-role-arn"
]
 }
]
}
```

- `DescribeAccountAuditConfiguration`
- `DeleteAccountAuditConfiguration`
- `StartOnDemandAuditTask`
- `CancelAuditTask`
- `DescribeAuditTask`
- `ListAuditTasks`
- `ListScheduledAudits`
- `ListAuditFindings`

#### policy

Tutti questi comandi richiedono \* nel Resource campo della policy.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iot:DescribeAccountAuditConfiguration",
 "iot:DeleteAccountAuditConfiguration",
 "iot:StartOnDemandAuditTask",
 "iot:CancelAuditTask",
 "iot:DescribeAuditTask",
 "iot>ListAuditTasks",
 "iot>ListScheduledAudits",
 "iot>ListAuditFindings"
],
 "Resource": "*"
 }
]
}
```

```
 "Resource": [
 "*"
]
 }
}
```

- `CreateScheduledAudit`
- `UpdateScheduledAudit`
- `DeleteScheduledAudit`
- `DescribeScheduledAudit`

policy

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iot:CreateScheduledAudit",
 "iot:UpdateScheduledAudit",
 "iot:DeleteScheduledAudit",
 "iot:DescribeScheduledAudit"
],
 "Resource": [
 "arn:aws:iot:region:account-id:scheduledaudit/scheduled-audit-name"
]
 }
]
}
```

Il formato per un ARN del ruolo di audit pianificato di AWS IoT Device Defender è:

```
arn:aws:iot:region:account-id:scheduledaudit/scheduled-audit-name
```

## Restrizioni dei servizi

| Risorsa                               | Limite     | Descrizione                                                                                                |
|---------------------------------------|------------|------------------------------------------------------------------------------------------------------------|
| audit pianificati                     | Massimo 5  | Puoi creare fino a 5 audit pianificati prima che venga generata un'eccezione <code>LimitExceeded</code> .  |
| audit "on-demand" simultanei in corso | Massimo 10 | Puoi creare fino a 10 audit "on-demand" prima che venga generata un'eccezione <code>LimitExceeded</code> . |

# Comandi di auditing

## Gestione delle impostazioni di auditing

Utilizzare `UpdateAccountAuditConfiguration` per configurare le impostazioni di audit per l'account. Questo comando permette di abilitare i controlli che desideri siano disponibili per gli audit, configurare le notifiche optionali e configurare le autorizzazioni.

Controlla queste impostazioni con `DescribeAccountAuditConfiguration`.

Usa `DeleteAccountAuditConfiguration` per eliminare le impostazioni di auditing. In questo modo, vengono ripristinati tutti i valori predefiniti e vengono disabilitati in modo efficace tutti gli audit in quanto tutti i controlli sono disabilitati per impostazione predefinita.

### UpdateAccountAuditConfiguration

Configura o riconfigura le impostazioni di auditing di Device Defender per l'account. Le impostazioni includono la modalità di invio delle notifiche degli audit e i controlli di auditing abilitati o disabilitati.

Riepilogo

```
aws iot update-account-audit-configuration \
[--role-arn <value>] \
[--audit-notification-target-configurations <value>] \
[--audit-check-configurations <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "roleArn": "string",
 "auditNotificationTargetConfigurations": {
 "string": {
 "targetArn": "string",
 "roleArn": "string",
 "enabled": "boolean"
 }
 },
 "auditCheckConfigurations": {
 "string": {
 "enabled": "boolean"
 }
 }
}
```

Campi di `cli-input-json`

| Nome    | Tipo                                     | Descrizione                                                                                                                                                                 |
|---------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn | Stringa<br>Lunghezza max: 2048, min.: 20 | L'ARN del ruolo che concede a AWS IoT l'autorizzazione per accedere alle informazioni su dispositivi, policy, certificati e altri elementi necessari per eseguire un audit. |

| Nome                                  | Tipo     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auditNotificationTargetConfigurations | mappa    | Informazioni sui target a cui vengono inviate le notifiche di auditing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| targetArn                             | Stringa  | ARN del target (argomento SNS) a cui vengono inviate le notifiche di auditing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| roleArn                               | Stringa  | ARN del ruolo che concede l'autorizzazione per l'invio delle notifiche al target.<br>Lunghezza max: 2048, min.: 20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| enabled                               | booleano | True se le notifiche per il target sono abilitate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| auditCheckConfigurations              | mappa    | <p>Specifica i controlli di auditing abilitati e disabilitati per l'account. Usa <code>DescribeAccountAuditConfiguration</code> per visualizzare l'elenco di tutti i controlli, inclusi quelli attualmente abilitati.</p> <p>Alcune raccolte di dati potrebbero iniziare subito quando alcuni controlli sono abilitati. Quando un controllo viene disabilitato, i dati raccolti fino a quel momento in relazione al controllo vengono eliminati.</p> <p>Non è possibile disabilitare un controllo se viene usato da un audit pianificato. È prima necessario eliminare il controllo dall'audit pianificato oppure eliminare l'audit pianificato stesso.</p> <p>Nella prima chiamata a <code>UpdateAccountAuditConfiguration</code> questo parametro è obbligatorio e deve specificare almeno un controllo abilitato.</p> |
| enabled                               | booleano | True se il controllo di auditing è abilitato per l'account.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

#### Output

Nessuna

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

#### ThrottlingException

La velocità supera il limite.

#### InternalFailureException

Si è verificato un errore imprevisto.

## DescribeAccountAuditConfiguration

Ottiene informazioni sulle impostazioni di Device Defender Audit per l'account. Le impostazioni includono la modalità di invio delle notifiche degli audit e i controlli di auditing abilitati o disabilitati.

### Riepilogo

```
aws iot describe-account-audit-configuration \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
}
```

### Output

```
{
 "roleArn": "string",
 "auditNotificationTargetConfigurations": {
 "string": {
 "targetArn": "string",
 "roleArn": "string",
 "enabled": "boolean"
 }
 },
 "auditCheckConfigurations": {
 "string": {
 "enabled": "boolean"
 }
 }
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome    | Tipo                                     | Descrizione                                                                                                                                                                                                                                                                             |
|---------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn | Stringa<br>Lunghezza max: 2048, min.: 20 | L'ARN del ruolo che concede a AWS IoT l'autorizzazione per accedere alle informazioni su dispositivi, policy, certificati e altri elementi necessari per eseguire un audit.<br><br>Nella prima chiamata a <code>UpdateAccountAuditConfiguration</code> questo parametro è obbligatorio. |

| Nome                                  | Tipo     | Descrizione                                                                                                        |
|---------------------------------------|----------|--------------------------------------------------------------------------------------------------------------------|
| auditNotificationTargetConfigurations | mappa    | Informazioni sui target a cui vengono inviate le notifiche di auditing per l'account.                              |
| targetArn                             | Stringa  | ARN del target (argomento SNS) a cui vengono inviate le notifiche di auditing.                                     |
| roleArn                               | Stringa  | ARN del ruolo che concede l'autorizzazione per l'invio delle notifiche al target.<br>Lunghezza max: 2048, min.: 20 |
| enabled                               | booleano | True se le notifiche per il target sono abilitate.                                                                 |
| auditCheckConfigurations              | mappa    | Specifica i controlli di auditing abilitati e disabilitati per l'account.                                          |
| enabled                               | booleano | True se il controllo di auditing è abilitato per l'account.                                                        |

#### Errori

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DeleteAccountAuditConfiguration

Ripristina le impostazioni predefinite per gli audit di Device Defender per l'account. I dati di configurazione immessi vengono eliminati e tutti i controlli di auditing vengono reimpostati come disabilitati.

#### Riepilogo

```
aws iot delete-account-audit-configuration \
[--delete-scheduled-audits | --no-delete-scheduled-audits] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "deleteScheduledAudits": "boolean"
}
```

#### Campi di **cli-input-json**

| Nome                  | Tipo     | Descrizione                                             |
|-----------------------|----------|---------------------------------------------------------|
| deleteScheduledAudits | booleano | Se true, tutti gli audit pianificati vengono eliminati. |

Output

Nessuna

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceNotFoundException`

La risorsa specificata non esiste.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

## Pianificazione di audit

Crea uno o più audit pianificati usando `CreateScheduledAudit`. Questo comando ti permette di specificare i controlli da eseguire durante un audit e la frequenza di esecuzione dell'audit.

Tieni traccia degli audit pianificati con `ListScheduledAudits` e `DescribeScheduledAudit`.

Cambia un audit pianificato esistente con `UpdateScheduledAudit` o eliminalo con `DeleteScheduledAudit`.

### CreateScheduledAudit

Crea un audit pianificato che viene eseguito con un intervallo di tempo specificato.

Riepilogo

```
aws iot create-scheduled-audit \
 --frequency <value> \
 [--day-of-month <value>] \
 [--day-of-week <value>] \
 --target-check-names <value> \
 [--tags <value>] \
 --scheduled-audit-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "frequency": "string",
 "dayOfMonth": "string",
 "dayOfWeek": "string",
 "targetCheckNames": [
 "string"
],
 "tags": [
 {
 "Key": "string",
 "Value": "string"
 }
]
}
```

```

 "Value": "string"
 }
],
"scheduledAuditName": "string"
}

```

### Campi di **cli-input-json**

| Nome             | Tipo                                                           | Descrizione                                                                                                                                                                                                                                                                                                                                                  |
|------------------|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| frequenza        | Stringa                                                        | Frequenza di esecuzione dell'audit. I valori possibili sono "DAILY", "WEEKLY", "BIWEEKLY" o "MONTHLY". L'ora di inizio effettiva di ogni audit è determinata dal sistema.<br><br>enumerazione: DAILY   WEEKLY   BIWEEKLY   MONTHLY                                                                                                                           |
| dayOfMonth       | Stringa<br><br>modello: ^([1-9] [12][0-9] 3[01])\$ <br>^LAST\$ | Giorno del mese in cui viene eseguito l'audit pianificato. Il valore può essere compreso tra "1" e "31" oppure può essere "LAST". Questo campo è obbligatorio se il parametro <code>frequency</code> è impostato su "MONTHLY". Se vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese. |
| dayOfWeek        | Stringa                                                        | Giorno della settimana in cui viene eseguito l'audit pianificato. I valori possibili sono "SUN", "MON", "TUE", "WED", "THU", "FRI" o "SAT". Questo campo è obbligatorio se il parametro <code>frequency</code> è impostato su "WEEKLY" o "BIWEEKLY".<br><br>enumerazione: SUN   MON   TUE   WED   THU   FRI   SAT                                            |
| targetCheckNames | elenco<br><br>membro: AuditCheckName                           | Controlli eseguiti durante l'audit pianificato. I controlli devono essere abilitati per l'account. Usa <code>DescribeAccountAuditConfiguration</code> per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati, o <code>UpdateAccountAuditConfiguration</code> per selezionare i controlli abilitati.                                        |
| tags             | elenco<br><br>member: Tag<br><br>Classe Java: java.util.List   | Metadati utilizzabili per la gestione dell'audit pianificato.                                                                                                                                                                                                                                                                                                |

| Nome               | Tipo    | Descrizione                                                                                                                                 |
|--------------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Chiave             | Stringa | La chiave del tag.                                                                                                                          |
| Valore             | Stringa | Il valore del tag.                                                                                                                          |
| scheduledAuditName | Stringa | Nome da assegnare all'audit pianificato. (numero massimo pari a 128 caratteri)<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+ |

#### Output

```
{
 "scheduledAuditArn": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome              | Tipo    | Descrizione                 |
|-------------------|---------|-----------------------------|
| scheduledAuditArn | Stringa | ARN dell'audit pianificato. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### InternalFailureException

Si è verificato un errore imprevisto.

##### LimitExceededException

È stato superato un limite.

## ListScheduledAudits

Elenca tutti gli audit pianificati.

#### Riepilogo

```
aws iot list-scheduled-audits \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
```

```
{
 "nextToken": "string",
 "maxResults": "integer"
}
```

#### Campi di **cli-input-json**

| Nome       | Tipo                                      | Descrizione                                                                      |
|------------|-------------------------------------------|----------------------------------------------------------------------------------|
| nextToken  | Stringa                                   | Token per il set di risultati successivo.                                        |
| maxResults | integer<br>Intervallo – Max: 250, min.: 1 | Numero massimo di risultati da restituire per volta. Il valore predefinito è 25. |

#### Output

```
{
 "scheduledAudits": [
 {
 "scheduledAuditName": "string",
 "scheduledAuditArn": "string",
 "frequency": "string",
 "dayOfMonth": "string",
 "dayOfWeek": "string"
 }
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome               | Tipo                                                                       | Descrizione                                                                                     |
|--------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| scheduledAudits    | elenco<br>membro:<br>ScheduledAuditMetadata<br>Classe Java: java.util.List | Elenco di audit pianificati.                                                                    |
| scheduledAuditName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-zA-Z0-9_-]+          | Nome dell'audit pianificato.                                                                    |
| scheduledAuditArn  | Stringa                                                                    | ARN dell'audit pianificato.                                                                     |
| frequenza          | Stringa                                                                    | Frequenza di esecuzione dell'audit.<br>enumerazione: DAILY   WEEKLY   BIWEEKLY   MONTHLY        |
| dayOfMonth         | Stringa<br>modello: ^([1-9] 1[2][0-9] 3[01])\$ ^LAST\$                     | Giorno del mese in cui viene eseguito l'audit pianificato (se <b>frequency</b> è "MONTHLY"). Se |

| Nome      | Tipo    | Descrizione                                                                                                                                                           |
|-----------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           |         | vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese.                                            |
| dayOfWeek | Stringa | Giorno della settimana in cui viene eseguito l'audit pianificato (se frequency è "WEEKLY" o "BIWEEKLY").<br><br>enumerazione: SUN   MON   TUE   WED   THU   FRI   SAT |
| nextToken | Stringa | Token che è possibile usare per recuperare il set di risultati successivo oppure null se non ci sono risultati aggiuntivi.                                            |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### InternalFailureException

Si è verificato un errore imprevisto.

## DescribeScheduledAudit

Ottiene le informazioni su un audit pianificato.

#### Riepilogo

```
aws iot describe-scheduled-audit \
--scheduled-audit-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "scheduledAuditName": "string"
}
```

#### Campi di cli-input-json

| Nome               | Tipo    | Descrizione                                                  |
|--------------------|---------|--------------------------------------------------------------|
| scheduledAuditName | Stringa | Nome dell'audit pianificato di cui ottenere le informazioni. |

| Nome | Tipo                                                     | Descrizione |
|------|----------------------------------------------------------|-------------|
|      | Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 _]+ |             |

#### Output

```
{
 "frequency": "string",
 "dayOfMonth": "string",
 "dayOfWeek": "string",
 "targetCheckNames": [
 "string"
],
 "scheduledAuditName": "string",
 "scheduledAuditArn": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome             | Tipo                                                           | Descrizione                                                                                                                                                                                                                                                     |
|------------------|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| frequenza        | Stringa                                                        | Frequenza di esecuzione dell'audit. Un valore tra "DAILY", "WEEKLY", "BIWEEKLY" o "MONTHLY". L'ora di inizio effettiva di ogni audit è determinata dal sistema.<br><br>enumerazione: DAILY   WEEKLY   BIWEEKLY   MONTHLY                                        |
| dayOfMonth       | Stringa<br><br>modello: ^([1-9] 1[2][0-9] 3[01])\$ <br>^LAST\$ | Giorno del mese in cui viene eseguito l'audit pianificato. Il valore può essere compreso tra "1" e "31" oppure può essere "LAST". Se vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese. |
| dayOfWeek        | Stringa                                                        | Giorno della settimana in cui viene eseguito l'audit pianificato. Un valore tra "SUN", "MON", "TUE", "WED", "THU", "FRI" o "SAT".<br><br>enumerazione: SUN   MON   TUE   WED   THU   FRI   SAT                                                                  |
| targetCheckNames | elenco<br><br>membro: AuditCheckName                           | Controlli eseguiti durante l'audit pianificato. I controlli devono essere abilitati per l'account. (Usa <a href="#">DescribeAccountAuditConfiguration</a> per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati o                            |

| Nome               | Tipo                                                                         | Descrizione                                                             |
|--------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------|
|                    |                                                                              | UpdateAccountAuditConfiguration per selezionare i controlli abilitati). |
| scheduledAuditName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Nome dell'audit pianificato.                                            |
| scheduledAuditArn  | Stringa                                                                      | ARN dell'audit pianificato.                                             |

Errori

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### ResourceNotFoundException

La risorsa specificata non esiste.

#### ThrottlingException

La velocità supera il limite.

#### InternalFailureException

Si è verificato un errore imprevisto.

## UpdateScheduledAudit

Aggiorna un audit pianificato, inclusi i controlli eseguiti e la frequenza di esecuzione dell'audit.

Riepilogo

```
aws iot update-scheduled-audit \
[--frequency <value>] \
[--day-of-month <value>] \
[--day-of-week <value>] \
[--target-check-names <value>] \
--scheduled-audit-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di cli-input-json

```
{
 "frequency": "string",
 "dayOfMonth": "string",
 "dayOfWeek": "string",
 "targetCheckNames": [
 "string"
],
 "scheduledAuditName": "string"
}
```

### Campi di `cli-input-json`

| Nome               | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| frequenza          | Stringa                                                                      | Frequenza di esecuzione dell'audit. I valori possibili sono "DAILY", "WEEKLY", "BIWEEKLY" o "MONTHLY". L'ora di inizio effettiva di ogni audit è determinata dal sistema.<br><br>enumerazione: DAILY   WEEKLY   BIWEEKLY   MONTHLY                                                                                                                           |
| dayOfMonth         | Stringa<br><br>modello: ^([1-9] [12][0-9] 3[01])\$ ^LAST\$                   | Giorno del mese in cui viene eseguito l'audit pianificato. Il valore può essere compreso tra "1" e "31" oppure può essere "LAST". Questo campo è obbligatorio se il parametro <code>frequency</code> è impostato su "MONTHLY". Se vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese. |
| dayOfWeek          | Stringa                                                                      | Giorno della settimana in cui viene eseguito l'audit pianificato. I valori possibili sono "SUN", "MON", "TUE", "WED", "THU", "FRI" o "SAT". Questo campo è obbligatorio se il parametro <code>frequency</code> è impostato su "WEEKLY" o "BIWEEKLY".<br><br>enumerazione: SUN   MON   TUE   WED   THU   FRI   SAT                                            |
| targetCheckNames   | elenco<br><br>membro: AuditCheckName                                         | Controlli eseguiti durante l'audit pianificato. I controlli devono essere abilitati per l'account. (Usa <code>DescribeAccountAuditConfiguration</code> per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati o <code>UpdateAccountAuditConfiguration</code> per selezionare i controlli abilitati).                                       |
| scheduledAuditName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Nome dell'audit pianificato. (numero massimo pari a 128 caratteri)                                                                                                                                                                                                                                                                                           |

### Output

```
{
 "scheduledAuditArn": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome              | Tipo    | Descrizione                 |
|-------------------|---------|-----------------------------|
| scheduledAuditArn | Stringa | ARN dell'audit pianificato. |

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DeleteScheduledAudit

Elimina un audit pianificato.

Riepilogo

```
aws iot delete-scheduled-audit \
 --scheduled-audit-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "scheduledAuditName": "string"
}
```

Campi di **cli-input-json**

| Nome               | Tipo    | Descrizione                                                                                            |
|--------------------|---------|--------------------------------------------------------------------------------------------------------|
| scheduledAuditName | Stringa | Nome dell'audit pianificato da eliminare.<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+ |

Output

Nessuna

## Errori

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ResourceNotFoundException

La risorsa specificata non esiste.

### ThrottlingException

La velocità supera il limite.

### InternalFailureException

Si è verificato un errore imprevisto.

## Esecuzione di un audit on demand

Usare `StartOnDemandAuditTask` per specificare i controlli da eseguire e avviare un audit immediatamente.

### StartOnDemandAuditTask

Avvia un audit di Device Defender on demand.

#### Riepilogo

```
aws iot start-on-demand-audit-task \
--target-check-names <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "targetCheckNames": [
 "string"
]
}
```

#### Campi di `cli-input-json`

| Nome             | Tipo                             | Descrizione                                                                                                                                                                                                                                                                                                                                               |
|------------------|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| targetCheckNames | elenco<br>membro: AuditCheckName | Controlli eseguiti durante l'audit. I controlli specificati devono essere abilitati per l'account, altrimenti si verifica un'eccezione. Usa <code>DescribeAccountAuditConfiguration</code> per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati o <code>UpdateAccountAuditConfiguration</code> per selezionare i controlli abilitati. |

#### Output

```
{
 "taskId": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome   | Tipo                                                                    | Descrizione                      |
|--------|-------------------------------------------------------------------------|----------------------------------|
| taskId | Stringa<br><br>Lunghezza max: 40, min.: 1<br><br>Modello: [a-zA-Z0-9-]+ | ID dell'audit on demand avviato. |

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

**LimitExceededException**

È stato superato un limite.

## Gestione di istanze di audit

Usa `DescribeAuditTask` per ottenere informazioni su un'istanza di audit specifica. Se l'esecuzione è già avvenuta, i risultati includono i controlli con esito negativo e quelli con esito positivo, quelli che il sistema non è stato in grado di completare e, se l'audit è ancora in corso, quelli ancora in fase di elaborazione.

Usa `ListAuditTasks` per trovare gli audit eseguiti durante un intervallo di tempo specifico.

Usa `CancelAuditTask` per arrestare un audit in corso.

### DescribeAuditTask

Ottiene le informazioni su un audit di Device Defender.

Riepilogo

```
aws iot describe-audit-task \
 --task-id <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "taskId": "string"
}
```

### Campi di **cli-input-json**

| Nome   | Tipo                                                                       | Descrizione                                    |
|--------|----------------------------------------------------------------------------|------------------------------------------------|
| taskId | Stringa<br><br>Lunghezza max: 40, min.: 1<br><br>Modello: [a-z A-Z 0-9 -]+ | ID dell'audit di cui ottenere le informazioni. |

### Output

```
{
 "taskStatus": "string",
 "taskType": "string",
 "taskStartTime": "timestamp",
 "taskStatistics": {
 "totalChecks": "integer",
 "inProgressChecks": "integer",
 "waitingForDataCollectionChecks": "integer",
 "compliantChecks": "integer",
 "nonCompliantChecks": "integer",
 "failedChecks": "integer",
 "canceledChecks": "integer"
 },
 "scheduledAuditName": "string",
 "auditDetails": {
 "string": {
 "checkRunStatus": "string",
 "checkCompliant": "boolean",
 "totalResourcesCount": "long",
 "nonCompliantResourcesCount": "long",
 "errorCode": "string",
 "message": "string"
 }
 }
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome          | Tipo      | Descrizione                                                                                                                                         |
|---------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| taskStatus    | Stringa   | Stato dell'audit: un valore tra "IN_PROGRESS", "COMPLETED", "FAILED" o "CANCELED".<br><br>enumerazione: IN_PROGRESS   COMPLETED   FAILED   CANCELED |
| taskType      | Stringa   | Tipo di audit: "ON_DEMAND_AUDIT_TASK" o "SCHEDULED_AUDIT_TASK".<br><br>enumerazione:<br>ON_DEMAND_AUDIT_TASK   SCHEDULED_AUDIT_TASK                 |
| taskStartTime | timestamp | Ora di inizio dell'audit.                                                                                                                           |

| Nome                           | Tipo                                                                        | Descrizione                                                                                                                                                                                                                                                                                                   |
|--------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| taskStatistics                 | TaskStatistics                                                              | Informazioni statistiche sull'audit.                                                                                                                                                                                                                                                                          |
| totalChecks                    | intero                                                                      | Numero di controlli nell'audit.                                                                                                                                                                                                                                                                               |
| inProgressChecks               | intero                                                                      | Numero di controlli in corso.                                                                                                                                                                                                                                                                                 |
| waitingForDataCollectionChecks | intero                                                                      | Numero di controlli in attesa della raccolta dei dati.                                                                                                                                                                                                                                                        |
| compliantChecks                | intero                                                                      | Numero di controlli che hanno trovato risorse conformi.                                                                                                                                                                                                                                                       |
| nonCompliantChecks             | integer                                                                     | Numero di controlli che hanno trovato risorse non conformi.                                                                                                                                                                                                                                                   |
| failedChecks                   | integer                                                                     | Numero di controlli.                                                                                                                                                                                                                                                                                          |
| canceledChecks                 | integer                                                                     | Numero di controlli non eseguiti perché l'audit è stato annullato.                                                                                                                                                                                                                                            |
| scheduledAuditName             | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 _]+ | Nome dell'audit pianificato (solo se l'audit è di tipo pianificato).                                                                                                                                                                                                                                          |
| auditDetails                   | mappa                                                                       | Informazioni dettagliate su ogni controllo eseguito durante l'audit.                                                                                                                                                                                                                                          |
| checkRunStatus                 | Stringa                                                                     | Stato di completamento del controllo. Un valore tra "IN_PROGRESS", "WAITING_FOR_DATA_COLLECTION", "CANCELED", "COMPLETED_COMPLIANT", "COMPLETED_NON_COMPLIANT" o "FAILED".<br><br>enumerazione: IN_PROGRESS   WAITING_FOR_DATA_COLLECTION   CANCELED   COMPLETED_COMPLIANT   COMPLETED_NON_COMPLIANT   FAILED |
| checkCompliant                 | booleano                                                                    | True se il controllo è stato completato e ha trovato tutte le risorse conformi.                                                                                                                                                                                                                               |
| totalResourcesCount            | Long                                                                        | Numero di risorse su cui è stato eseguito il controllo.                                                                                                                                                                                                                                                       |
| nonCompliantResourcesCount     | Long                                                                        | Numero di risorse che dal controllo sono risultate non conformi.                                                                                                                                                                                                                                              |

| Nome      | Tipo                           | Descrizione                                                                                                                                              |
|-----------|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| errorCode | Stringa                        | Codice degli errori rilevati durante l'esecuzione del controllo nel corso dell'audit. Un valore tra "INSUFFICIENT_PERMISSIONS" o "AUDIT_CHECK_DISABLED". |
| message   | Stringa<br>Lunghezza max: 2048 | Messaggio associato agli errori rilevati durante l'esecuzione del controllo nel corso dell'audit.                                                        |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

## ListAuditTasks

Elenca gli audit di Device Defender eseguiti durante un determinato periodo di tempo.

#### Riepilogo

```
aws iot list-audit-tasks \
--start-time <value> \
--end-time <value> \
[--task-type <value>] \
[--task-status <value>] \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "startTime": "timestamp",
 "endTime": "timestamp",
 "taskType": "string",
 "taskStatus": "string",
 "nextToken": "string",
 "maxResults": "integer"
}
```

### Campi di **cli-input-json**

| Nome       | Tipo                                      | Descrizione                                                                                                                                                                                                                                         |
|------------|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| startTime  | Timestamp                                 | Inizio del periodo di tempo. Le informazioni sull'audit vengono conservate per un periodo di tempo limitato (180 giorni). Richiesta di un orario di inizio precedente a ciò che viene conservato comporta un <code>InvalidRequestException</code> . |
| endTime    | timestamp                                 | Fine del periodo di tempo.                                                                                                                                                                                                                          |
| taskType   | Stringa                                   | Filtro che limita l'output al tipo di audit specificato: può essere un valore tra "ON_DEMAND_AUDIT_TASK" o "SCHEDULED_AUDIT_TASK".<br><br>enumerazione:<br>ON_DEMAND_AUDIT_TASK   SCHEDULED_AUDIT_TASK                                              |
| taskStatus | Stringa                                   | Filtro che limita l'output agli audit con lo stato di completamento specificato: può essere un valore tra "IN_PROGRESS", "COMPLETED", "FAILED" o "CANCELED".<br><br>enumerazione: IN_PROGRESS   COMPLETED   FAILED   CANCELED                       |
| nextToken  | Stringa                                   | Token per il set di risultati successivo.                                                                                                                                                                                                           |
| maxResults | integer<br>Intervallo – Max: 250, min.: 1 | Numero massimo di risultati da restituire per volta. Il valore predefinito è 25.                                                                                                                                                                    |

### Output

```
{
 "tasks": [
 {
 "taskId": "string",
 "taskStatus": "string",
 "taskType": "string"
 }
],
 "nextToken": "string"
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome       | Tipo                                                               | Descrizione                                                                                                                                         |
|------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| attività   | elenco<br>membro: AuditTaskMetadata<br>Classe Java: java.util.List | Audit eseguiti durante il periodo di tempo specificato.                                                                                             |
| taskId     | Stringa<br>Lunghezza max: 40, min.: 1<br>Modello: [a–z A–Z 0–9 -]+ | ID dell'audit.                                                                                                                                      |
| taskStatus | Stringa                                                            | Stato dell'audit: un valore tra "IN_PROGRESS", "COMPLETED", "FAILED" o "CANCELED".<br><br>enumerazione: IN_PROGRESS   COMPLETED   FAILED   CANCELED |
| taskType   | Stringa                                                            | Tipo di audit: un valore tra "ON_DEMAND_AUDIT_TASK" o "SCHEDULED_AUDIT_TASK".<br><br>enumerazione:<br>ON_DEMAND_AUDIT_TASK   SCHEDULED_AUDIT_TASK   |
| nextToken  | Stringa                                                            | Token che è possibile usare per recuperare il set di risultati successivo oppure null se non ci sono risultati aggiuntivi.                          |

### Errori

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### ThrottlingException

La velocità supera il limite.

#### InternalFailureException

Si è verificato un errore imprevisto.

## CancelAuditTask

Annulla un audit in corso. L'audit può essere pianificato o on demand. Se l'audit non è in corso, si verifica InvalidRequestException.

#### Riepilogo

```
aws iot cancel-audit-task \
```

```
--task-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "taskId": "string"
}
```

Campi di **cli-input-json**

| Nome   | Tipo                                                               | Descrizione                                                                              |
|--------|--------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| taskId | Stringa<br>Lunghezza max: 40, min.: 1<br>Modello: [a-z A-Z 0-9 -]+ | ID dell'audit da annullare. È possibile annullare solo un audit con stato "IN_PROGRESS". |

Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## Controllo dei risultati dell'audit

Usa **ListAuditFindings** per visualizzare i risultati di un audit. Puoi filtrare i risultati in base al tipo di controllo, a una risorsa specifica o a quando è stato eseguito l'audit. È possibile utilizzare queste informazioni per mitigare gli eventuali problemi rilevati.

### ListAuditFindings

Elenca i risultati di un audit di Device Defender o degli audit eseguiti durante un periodo di tempo specificato. I risultati vengono conservati per 180 giorni.

Riepilogo

```
aws iot list-audit-findings \
[--task-id <value>] \
[--check-name <value>] \
[--resource-identifier <value>] \
```

```
[--max-results <value>] \
[--next-token <value>] \
[--start-time <value>] \
[--end-time <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "taskId": "string",
 "checkName": "string",
 "resourceIdentifier": {
 "deviceCertificateId": "string",
 "caCertificateId": "string",
 "cognitoIdentityPoolId": "string",
 "clientId": "string",
 "policyVersionIdentifier": {
 "policyName": "string",
 "policyVersionId": "string"
 },
 "account": "string"
 },
 "maxResults": "integer",
 "nextToken": "string",
 "startTime": "timestamp",
 "endTime": "timestamp"
}
```

#### Campi di cli-input-json

| Nome                  | Tipo               | Descrizione                                                                                                                                                                                                            |
|-----------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| taskId                | Stringa            | Filtro che limita i risultati all'audit con l'ID specificato. Devi specificare il valore di taskId oppure di startTime ed endTime, ma non entrambi.<br><br>Lunghezza max: 40, min.: 1<br><br>Modello: [a-z A-Z 0-9 -]+ |
| checkName             | Stringa            | Filtro che limita i risultati al controllo di auditing specificato.                                                                                                                                                    |
| resourceIdentifier    | ResourceIdentifier | Informazioni che identificano le risorse non conformi.                                                                                                                                                                 |
| deviceCertificateId   | Stringa            | ID del certificato collegato alla risorsa.<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+                                                                                                      |
| caCertificateId       | Stringa            | ID del certificato CA usato per autorizzare il certificato.<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+                                                                                     |
| cognitoIdentityPoolId | Stringa            | L'ID del pool di identità Amazon Cognito.                                                                                                                                                                              |
| clientId              | Stringa            | ID client.                                                                                                                                                                                                             |

| Nome                    | Tipo                                                                  | Descrizione                                                                                                                                                      |
|-------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| policyVersionIdentifier | PolicyVersionIdentifier                                               | Versione della policy associata alla risorsa.                                                                                                                    |
| policyName              | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w+=,.@-]+ | Nome della policy.                                                                                                                                               |
| policyVersionId         | Stringa<br><br>Modello: [0-9]+                                        | ID della versione della policy associata alla risorsa.                                                                                                           |
| account                 | Stringa<br><br>Lunghezza max: 12, min.: 12<br><br>Modello: [0-9]+     | Account a cui è associata la risorsa.                                                                                                                            |
| maxResults              | integer<br><br>Intervallo – Max: 250, min.: 1                         | Numero massimo di risultati da restituire per volta. Il valore predefinito è 25.                                                                                 |
| nextToken               | Stringa                                                               | Token per il set di risultati successivo.                                                                                                                        |
| startTime               | timestamp                                                             | Filtro che limita i risultati a quelli trovati dopo l'ora specificata. Devi specificare il valore di startTime ed endTime oppure di taskId, ma non entrambi.     |
| endTime                 | timestamp                                                             | Filtro che limita i risultati a quelli trovati prima dell'ora specificata. Devi specificare il valore di startTime ed endTime oppure di taskId, ma non entrambi. |

## Output

```
{
 "findings": [
 {
 "taskId": "string",
 "checkName": "string",
 "taskStartTime": "timestamp",
 "findingTime": "timestamp",
 "severity": "string",
 "nonCompliantResource": {
 "resourceType": "string",
 "resourceIdentifier": {
 "deviceCertificateId": "string",
 "caCertificateId": "string",
 "cognitoIdentityPoolId": "string",
 "clientId": "string",
 "policyVersionIdentifier": {
 "policyName": "string",
 "policyVersionId": "string"
 }
 }
 }
 }
]
}
```

```

 },
 "account": "string"
 },
 "additionalInfo": {
 "string": "string"
 }
},
"relatedResources": [
{
 "resourceType": "string",
 "resourceIdentifier": {
 "deviceCertificateId": "string",
 "caCertificateId": "string",
 "cognitoIdentityPoolId": "string",
 "clientId": "string",
 "policyVersionIdentifier": {
 "policyName": "string",
 "policyVersionId": "string"
 },
 "account": "string"
 },
 "additionalInfo": {
 "string": "string"
 }
}
],
"reasonForNonCompliance": "string",
"reasonForNonComplianceCode": "string"
}
],
"nextToken": "string"
}
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome                 | Tipo                                                                       | Descrizione                                                                |
|----------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------|
| risultati            | elenco<br><br>membro: AuditFinding                                         | Risultati dell'audit.                                                      |
| taskId               | Stringa<br><br>Lunghezza max: 40, min.: 1<br><br>Modello: [a–z A–Z 0–9 -]+ | ID dell'audit che ha generato il risultato (ricerca)                       |
| checkName            | Stringa                                                                    | Controllo di auditing che ha generato il risultato.                        |
| taskStartTime        | timestamp                                                                  | Ora di inizio dell'audit.                                                  |
| findingTime          | timestamp                                                                  | Ora in cui è stato trovato il risultato.                                   |
| severity             | Stringa                                                                    | Gravità del risultato.<br><br>enumerazione: CRITICAL   HIGH   MEDIUM   LOW |
| nonCompliantResource | NonCompliantResource                                                       | Risorsa risultata non conforme dal controllo di audit.                     |

| Nome                    | Tipo                                                                           | Descrizione                                                                                                                                                                     |
|-------------------------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| resourceType            | Stringa                                                                        | Tipo della risorsa non conforme.<br><br>enumerazione:<br>DEVICE_CERTIFICATE<br>  CA_CERTIFICATE<br>  IOT_POLICY  <br>COGNITO_IDENTITY_POOL<br>  CLIENT_ID  <br>ACCOUNT_SETTINGS |
| resourceIdentifier      | ResourceIdentifier                                                             | Informazioni che identificano le risorse non conformi.                                                                                                                          |
| deviceCertificateId     | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato collegato alla risorsa.                                                                                                                                      |
| caCertificateId         | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato CA usato per autorizzare il certificato.                                                                                                                     |
| cognitoIdentityPoolId   | Stringa                                                                        | L'ID del pool di identità Amazon Cognito.                                                                                                                                       |
| clientId                | Stringa                                                                        | ID client.                                                                                                                                                                      |
| policyVersionIdentifier | PolicyVersionIdentifier                                                        | Versione della policy associata alla risorsa.                                                                                                                                   |
| policyName              | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+          | Nome della policy.                                                                                                                                                              |
| policyVersionId         | Stringa<br><br>Modello: [0-9]+                                                 | ID della versione della policy associata alla risorsa.                                                                                                                          |
| account                 | Stringa<br><br>Lunghezza max: 12, min.: 12<br><br>Modello: [0-9]+              | Account a cui è associata la risorsa.                                                                                                                                           |
| additionalInfo          | mappa                                                                          | Altre informazioni sulla risorsa non conforme.                                                                                                                                  |
| relatedResources        | elenco<br><br>membro: RelatedResource                                          | Elenco delle risorse correlate.                                                                                                                                                 |

| Nome                       | Tipo                                                                           | Descrizione                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| resourceType               | Stringa                                                                        | Il tipo di risorsa.<br><br>enumerazione:<br>DEVICE_CERTIFICATE<br>  CA_CERTIFICATE<br>  IOT_POLICY  <br>COGNITO_IDENTITY_POOL<br>  CLIENT_ID  <br>ACCOUNT_SETTINGS |
| resourceIdentifier         | ResourceIdentifier                                                             | Informazioni che identificano la risorsa.                                                                                                                          |
| deviceCertificateId        | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato collegato alla risorsa.                                                                                                                         |
| caCertificateId            | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato CA usato per autorizzare il certificato.                                                                                                        |
| cognitoIdentityPoolId      | Stringa                                                                        | L'ID del pool di identità Amazon Cognito.                                                                                                                          |
| clientId                   | Stringa                                                                        | ID client.                                                                                                                                                         |
| policyVersionIdentifier    | PolicyVersionIdentifier                                                        | Versione della policy associata alla risorsa.                                                                                                                      |
| policyName                 | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+          | Nome della policy.                                                                                                                                                 |
| policyVersionId            | Stringa<br><br>Modello: [0-9]+                                                 | ID della versione della policy associata alla risorsa.                                                                                                             |
| account                    | Stringa<br><br>Lunghezza max: 12, min.: 12<br><br>Modello: [0-9]+              | Account a cui è associata la risorsa.                                                                                                                              |
| additionalInfo             | mappa                                                                          | Altre informazioni sulla risorsa.                                                                                                                                  |
| reasonForNonCompliance     | Stringa                                                                        | Motivo per cui la risorsa è risultata non conforme.                                                                                                                |
| reasonForNonComplianceCode | Stringa                                                                        | Codice che indica il motivo per cui la risorsa è risultata non conforme.                                                                                           |

| Nome      | Tipo    | Descrizione                                                                                                                             |
|-----------|---------|-----------------------------------------------------------------------------------------------------------------------------------------|
| nextToken | Stringa | Token che è possibile usare per recuperare il set di risultati successivo oppure <code>null</code> se non ci sono risultati aggiuntivi. |

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

## Rilevamento

AWS IoT Device Defender Detect permette di identificare un comportamento insolito che può indicare un dispositivo compromesso monitorando il comportamento dei dispositivi. Usando una combinazione di parametri lato cloud (da AWS IoT) e parametri lato dispositivo (dagli agenti installati nei dispositivi), puoi rilevare le modifiche nei modelli di connessione, i dispositivi che comunicano con endpoint non autorizzati o non riconosciuti e le modifiche nei modelli di traffico dei dispositivi in entrata e in uscita. È possibile creare profili di sicurezza, che contengono definizioni dei comportamenti dei dispositivi previsti, e assegnarli a un gruppo di dispositivi o a tutti i dispositivi del parco istanze. AWS IoT Device Defender Detect utilizza questi profili di sicurezza per rilevare le anomalie e inviare allarmi tramite i parametri Amazon CloudWatch e le notifiche Amazon Simple Notification Service.

AWS IoT Device Defender Detect è in grado di rilevare una serie di problemi di sicurezza frequenti nei dispositivi connessi:

- Traffico da un dispositivo verso un indirizzo IP dannoso noto o verso un endpoint non autorizzato, che indica un canale di controllo e un comando potenzialmente dannoso.
- Traffico anomalo, ad esempio un picco del traffico in uscita, che indica che un dispositivo sta prendendo parte a un attacco DDoS.
- Dispositivi con interfacce di gestione remote e porte accessibili in remoto.
- Un picco nella frequenza dei messaggi inviati all'account— affinché un dispositivo non autorizzato non comporti spese legate ai messaggi.

Casi d'uso:

Misurazione della superficie di attacco

Puoi usare AWS IoT Device Defender Detect per misurare la superficie di attacco dei dispositivi. Puoi ad esempio identificare i dispositivi con porte di servizio che sono spesso l'obiettivo di campagne di attacchi (servizio telnet in esecuzione sulle porte 23/2323, servizio SSH in esecuzione sulla porta 22, servizi HTTP/S in esecuzione sulle porte 80/443/8080/8081). Sebbene ci possano essere motivi legittimi per usare queste porte di servizio nei dispositivi, spesso tali porte fanno parte della superficie di attacco per gli avversari e comportano rischi. Quando Detect segnala una superficie di attacco, puoi scegliere di ridurla al minimo (eliminando i servizi di rete inutilizzati) oppure di eseguire ulteriori

valutazioni per identificare le vulnerabilità della sicurezza (ad esempio, telnet configurato con password comuni, predefinite o poco sicure).

Rilevamento di anomalie nel comportamento dei dispositivi con le possibili cause principali legate alla sicurezza

Puoi usare AWS IoT Device Defender Detect per ricevere avvisi in caso di parametri imprevisti relativi al comportamento dei dispositivi (numero di porte aperte, numero di connessioni, presenza di una porta aperta non prevista, connessioni a indirizzi IP non previsti) che potrebbero indicare una violazione della sicurezza. Un numero di connessioni TCP maggiore del previsto può ad esempio indicare un dispositivo usato per un attacco DDoS. Un processo in ascolto su una porta diversa da quella prevista può indicare una backdoor installata in un dispositivo per il controllo remoto. Puoi usare Detect per esaminare lo stato del parco istanze di dispositivi e verificare i presupposti di sicurezza (ad esempio, nessun dispositivo deve essere in ascolto sulla porta 23 o 2323).

Rileva un dispositivo non configurato correttamente

Un picco nel numero o nelle dimensioni dei messaggi inviati da un dispositivo all'account può indicare un'errata configurazione del dispositivo. Tale dispositivo potrebbe causare un aumento dei costi per i messaggi. Analogamente, un dispositivo con numerosi errori di autorizzazione potrebbe richiedere una nuova configurazione della policy.

## Concetti

metric

AWS IoT Device Defender Detect usa i parametri per rilevare un comportamento anomalo. Detect confronta il valore segnalato per un parametro con il valore previsto fornito. Questi parametri possono essere ricavati da due origini: parametri lato cloud e parametri lato dispositivo:

Un comportamento anomalo nella rete AWS IoT viene rilevato usando i parametri lato cloud, come il numero di errori di autorizzazione oppure il numero o la dimensione dei messaggi inviati o ricevuti da un dispositivo tramite AWS IoT.

AWS IoT Device Defender Detect, inoltre, è in grado di raccogliere, aggregare e monitorare i dati dei parametri generati dai dispositivi, ad esempio le porte su cui un dispositivo è in ascolto, il numero di byte o di pacchetti inviatiAWS IoT o le connessioni TCP del dispositivo.

Puoi usare AWS IoT Device Defender Detect solo con i parametri lato cloud. Per usare i parametri lato dispositivo, devi prima distribuire un SDK AWS IoT nei gateway dei dispositivi o nei dispositivi connessi a AWS IoT per raccogliere i parametri e inviarli a AWS IoT. Consulta [Invio di parametri dai dispositivi \(p. 575\)](#).

profilo di sicurezza

Un profilo di sicurezza definisce i comportamenti anomali per un gruppo di dispositivi (un [gruppo di oggetti](#)) o per tutti i dispositivi nell'account e specifica le operazioni da eseguire quando viene rilevata un'anomalia. È possibile utilizzare la console AWS IoT o i comandi API per creare un profilo di sicurezza e associarlo a un gruppo di dispositivi. AWS IoT Device Defender Detect avvia la registrazione dei dati correlati alla sicurezza e usa i comportamenti definiti nel profilo di sicurezza per rilevare le anomalie nel comportamento dei dispositivi.

behavior

Un comportamento indica a AWS IoT Device Defender Detect come riconoscere se il dispositivo si sta comportando in modo anomalo. Ciascun comportamento consiste di un nome, un parametro, un operatore e un valore o una soglia statistica. Per alcuni parametri è richiesto anche un periodo di tempo (`durationSeconds`). Qualsiasi operazione del dispositivo che non corrisponde a un'istruzione di comportamento definita attiva un avviso.

## avviso

Quando viene rilevata un'anomalia, è possibile inviare una notifica di avviso tramite un parametro CloudWatch (consulta [Parametri di AWS IoT \(p. 646\)](#)) o una notifica SNS. Una notifica di avviso viene visualizzata anche nella console CDM AWS IoT insieme a informazioni aggiuntive sull'avviso e a una cronologia degli avvisi per il dispositivo. Viene inviato un avviso anche quando un dispositivo monitorato smette di presentare un comportamento anomalo oppure quando ha provocato la generazione di un avviso ma la segnalazione non avviene più per un lungo periodo di tempo.

# Comportamenti

Un profilo di sicurezza contiene un set di comportamenti. Ciascun comportamento contiene un parametro che specifica il comportamento normale per un gruppo di dispositivi o per tutti i dispositivi nell'account. (Consulta [Parametri \(p. 561\)](#) e ) [CreateSecurityProfile \(p. 582\)](#).

Di seguito sono descritti alcuni dei campi utilizzati nella definizione di behavior:

### name

Il nome per il comportamento.

### metric

Il nome del parametro utilizzato (ovvero, ciò che è misurato dal comportamento).

### criteria

Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a metric.

#### comparisonOperator

Operatore che mette in correlazione l'oggetto misurato (metric) e i criteri (value o statisticalThreshold).

I possibili valori sono: "less-than", "less-than-equals", "greater-than", "greater-than-equals", "in-cidr-set", "not-in-cidr-set", "in-port-set", and "not-in-port-set". Non tutti gli operatori sono validi per ogni parametro. Operatori per set di CIDR e porte sono solo per l'uso con i parametri che riguardano tali entità.

#### value

Valore da confrontare con metric. A seconda del tipo di parametro, questo dovrebbe contenere un count (un valore), cidrs (un elenco di CIDR) o ports (un elenco di porte).

#### statisticalThreshold

La soglia statistica in base alla quale viene determinata una violazione del comportamento. Il campo contiene un campo statistic che dispone dei seguenti valori possibili: "p0", "p0.1", "p0.01", "p1", "p10", "p50", "p90", "p99", "p99.9", "p99.99" o "p100".

statistic indica un percentile. Restituisce un valore in base al quale viene determinata la conformità con il comportamento. I parametri vengono raccolti una o più volte nell'arco della durata specificata (durationSeconds) da tutti i dispositivi di segnalazione associati a questo profilo di sicurezza e i percentili vengono calcolati in base a tali dati. Dopotutto, le misure vengono raccolte per un dispositivo e accumulate nell'arco della stessa durata. Se il valore risultante per il dispositivo è sopra o sotto (comparisonOperator) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario viola il comportamento.

Un percentile indica la percentuale di tutte le misurazioni considerate che sono inferiori al valore associato. Ad esempio, se il valore associato a "p90" (il novantesimo percentile) è 123, il 90% di tutte le misurazioni è inferiore a 123.

#### durationSeconds

Usa questo parametro per specificare il periodo di tempo durante cui viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, `NUM_MESSAGES_SENT`). Per un confronto di parametri `statisticalThreshold`, questo è il periodo di tempo durante il quale le misurazioni vengono raccolte per tutti i dispositivi per determinare i valori `statisticalThreshold` e quindi per ogni dispositivo per determinare come si posiziona il comportamento nel confronto.

#### consecutiveDatapointsToAlarm

Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1. (Notare che questo differisce dalla console AWS IoT in cui il valore 3 viene visualizzato per impostazione predefinita, ma può essere sovrascritto.)

#### consecutiveDatapointsToClear

Se si è verificato un avviso e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1. (Notare che questo differisce dalla console AWS IoT in cui il valore 3 viene visualizzato per impostazione predefinita, ma può essere sovrascritto.)

## Parametri

### aws:message-byte-size

Numero di byte in un messaggio.

more info (1)

Usa questo parametro per specificare la dimensione massima o minima (in byte) di ogni messaggio trasmesso da un dispositivo a AWS IoT.

Origine: lato cloud

Operatori: `less-than` | `less-than-equals` | `greater-than` | `greater-than-equals`

Valore: intero non negativo

Unità: byte

Esempio:

```
{
 "name": "Max Message Size",
 "metric": "aws:message-byte-size",
 "criteria": {
 "comparisonOperator": "less-than",
 "value": {
 "count": 1024
 },
 "consecutiveDatapointsToAlarm": 3,
 "consecutiveDatapointsToClear": 3
 }
}
```

Esempio utilizzando un `statisticalThreshold`:

```
{
```

```
 "name": "Large Message Size",
 "metric": "aws:message-byte-size",
 "criteria": {
 "comparisonOperator": "less-than",
 "statisticalThreshold": {
 "statistic": "p90"
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 3,
 "consecutiveDatapointsToClear": 3
 }
 }
```

Si verifica un allarme per un dispositivo se, durante tre periodi di 5 minuti consecutivi, vengono trasmessi messaggi la cui dimensione cumulativa è superiore a quella misurata del 90% per tutti gli altri dispositivi che segnalano questo comportamento del profilo di sicurezza.

#### aws:num-messages-received / aws:num-messages-sent

Numero di messaggi ricevuti o inviati da un dispositivo durante un determinato periodo di tempo.

[more info \(2\)](#)

Usa questo parametro per specificare il numero massimo o minimo di messaggi che possono essere inviati o ricevuti tra AWS IoT e ogni dispositivo in un determinato periodo di tempo.

Origine: lato cloud

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: messaggi

Durata: integer non negativo, i valori validi sono 300, 600, 900, 1800 o 3600 secondi

Esempio:

```
{
 "name": "Out bound message count",
 "metric": "aws:num-messages-sent",
 "criteria": {
 "comparisonOperator": "less-than",
 "value": {
 "count": 50
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 2,
 "consecutiveDatapointsToClear": 2
 }
}
```

Esempio utilizzando un **statisticalThreshold**:

```
{
 "name": "Out bound message rate",
 "metric": "aws:num-messages-sent",
 "criteria": {
```

```
 "comparisonOperator": "less-than",
 "statisticalThreshold": {
 "statistic": "p99"
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 2,
 "consecutiveDatapointsToClear": 2
 }
}
```

#### aws:all-bytes-out

Numero di byte in uscita da un dispositivo durante un determinato periodo di tempo.

[more info \(3\)](#)

Usa questo parametro per specificare la quantità massima o minima di traffico in uscita che un dispositivo può inviare, misurata in byte, in un determinato periodo di tempo.

Origine: lato dispositivo

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: byte

Durata: integer non negativo, i valori validi sono 300, 600, 900, 1800 o 3600 secondi

Esempio:

```
{
 "name": "TCP outbound traffic",
 "metric": "aws:all-bytes-out",
 "criteria": {
 "comparisonOperator": "less-than",
 "value": {
 "count": 4096
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 5,
 "consecutiveDatapointsToClear": 4
 }
}
```

Esempio utilizzando un `statisticalThreshold`:

```
{
 "name": "TCP outbound traffic",
 "metric": "aws:all-bytes-out",
 "criteria": {
 "comparisonOperator": "less-than",
 "statisticalThreshold": {
 "statistic": "p50"
 },
 "durationSeconds": 900,
 "consecutiveDatapointsToAlarm": 5,
 "consecutiveDatapointsToClear": 4
 }
}
```

```
}
```

#### aws:all-bytes-in

Numero di byte in entrata in un dispositivo durante un determinato periodo di tempo.

more info (4)

Usa questo parametro per specificare la quantità massima o minima di traffico in entrata che un dispositivo può ricevere, misurata in byte, in un determinato periodo di tempo.

Origine: lato dispositivo

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: byte

Durata: integer non negativo, i valori validi sono 300, 600, 900, 1800 o 3600 secondi

Esempio:

```
{
 "name": "TCP inbound traffic",
 "metric": "aws:all-bytes-in",
 "criteria": {
 "comparisonOperator": "less-than",
 "value": {
 "count": 4096
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 1,
 "consecutiveDatapointsToClear": 3
 }
}
```

Esempio utilizzando un `statisticalThreshold`:

```
{
 "name": "TCP inbound traffic",
 "metric": "aws:all-bytes-in",
 "criteria": {
 "comparisonOperator": "less-than",
 "statisticalThreshold": {
 "statistic": "p90"
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 1,
 "consecutiveDatapointsToClear": 3
 }
}
```

#### aws:all-packets-out

Numero di pacchetti in uscita da un dispositivo durante un determinato periodo di tempo.

more info (5)

Usa questo parametro per specificare la quantità massima o minima di traffico in uscita totale che un dispositivo può inviare in un determinato periodo di tempo.

Origine: lato dispositivo

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: pacchetti

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Esempio:

```
{
 "name": "TCP outbound traffic",
 "metric": "aws:all-packets-out",
 "criteria": {
 "comparisonOperator": "less-than",
 "value": {
 "count": 100
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 1,
 "consecutiveDatapointsToClear": 3
 }
}
```

Esempio utilizzando un `statisticalThreshold`:

```
{
 "name": "TCP outbound traffic",
 "metric": "aws:all-packets-out",
 "criteria": {
 "comparisonOperator": "less-than",
 "statisticalThreshold": {
 "statistic": "p90"
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 1,
 "consecutiveDatapointsToClear": 3
 }
}
```

`aws:all-packets-in`

Numero di pacchetti in entrata in un dispositivo durante un determinato periodo di tempo.

more info (6)

Usa questo parametro per specificare la quantità massima o minima di traffico in entrata totale che un dispositivo può ricevere in un determinato periodo di tempo.

Origine: lato dispositivo

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: pacchetti

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Esempio:

```
{
 "name": "TCP inbound traffic",
 "metric": "aws:all-packets-in",
 "criteria": {
 "comparisonOperator": "less-than",
 "value": {
 "count": 100
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 2,
 "consecutiveDatapointsToClear": 1
 }
}
```

Esempio utilizzando un **statisticalThreshold**:

```
{
 "name": "TCP inbound traffic",
 "metric": "aws:all-packets-in",
 "criteria": {
 "comparisonOperator": "less-than",
 "statisticalThreshold": {
 "statistic": "p90"
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 2,
 "consecutiveDatapointsToClear": 1
 }
}
```

#### aws:num-authorization-failures

Numero di errori di autorizzazione durante un determinato periodo di tempo.

[more info \(7\)](#)

Usa questo parametro per specificare il numero massimo di errori di autorizzazione permessi per ogni dispositivo in un determinato periodo di tempo. Un errore di autorizzazione si verifica quando una richiesta da un dispositivo a AWS IoT viene negata, ad esempio se un dispositivo tenta di eseguire la pubblicazione in un argomento per cui non dispone di autorizzazioni sufficienti.

Origine: lato cloud

Unità: errori

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: errori

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Esempio:

```
{
 "name": "Authorization Failures",
 "metric": "aws:num-authorization-failures",
 "criteria": {
 "comparisonOperator": "less-than",
 "value": {
 "count": 5
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 2,
 "consecutiveDatapointsToClear": 1
 }
}
```

Esempio utilizzando un `statisticalThreshold`:

```
{
 "name": "Authorization Failures",
 "metric": "aws:num-authorization-failures",
 "criteria": {
 "comparisonOperator": "less-than",
 "statisticalThreshold": {
 "statistic": "p50"
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 2,
 "consecutiveDatapointsToClear": 1
 }
}
```

#### aws:source-ip-address

Indirizzo IP da cui un dispositivo si è connesso a AWS IoT.

[more info \(8\)](#)

Usa questo parametro per specificare un set di CIDR permessi o non permessi da cui ciascun dispositivo deve o non deve connettersi a AWS IoT.

Origine: lato cloud

Operatori: `in-cidr-set` | `not-in-cidr-set`

Valori: elenco di CIDR

Unità: n/d

Esempio:

```
{
 "name": "Blacklisted source IPs",
 "metric": "aws:source-ip-address",
 "criteria": {
 "comparisonOperator": "not-in-cidr-set",
 "value": {
 "cidrSet": ["192.168.1.1/32", "192.168.1.2/32"]
 }
 }
}
```

```
 "cidrs": ["12.8.0.0/16", "15.102.16.0/24"]
 }
}
```

#### aws:destination-ip-addresses

Set di destinazioni IP.

[more info \(9\)](#)

Usa questo parametro per specificare un set di CIDR permessi o non permessi con cui ciascun dispositivo deve o non deve comunicare.

Origine: lato dispositivo

Operatori: in-cidr-set | not-in-cidr-set

Valori: elenco di CIDR

Unità: n/d

Esempio:

```
{
 "name": "Blacklisted destination IPs",
 "metric": "aws:destination-ip-addresses",
 "criteria": {
 "comparisonOperator": "not-in-cidr-set",
 "value": {
 "cidrs": ["12.8.0.0/16", "15.102.16.0/24"]
 }
 }
}
```

#### aws:listening-tcp-ports / aws:listening-udp-ports

Porte TCP o UDP su cui il dispositivo è in ascolto.

[more info \(10\)](#)

Usa questo parametro per specificare un set di porte TCP/UDP permesse o non permesse su cui ciascun dispositivo deve o non essere in ascolto.

Origine: lato dispositivo

Operatori: in-port-set | not-in-port-set

Valori: elenco di porte

Unità: n/d

Esempio:

```
{
 "name": "Listening TCP Ports",
```

```
 "metric": "aws:listening-tcp-ports",
 "criteria": {
 "comparisonOperator": "in-port-set",
 "value": {
 "ports": [443, 80]
 }
 }
}
```

#### aws:num-listening-tcp-ports / aws:num-listening-udp-ports

Numero delle porte TCP o UDP su cui il dispositivo è in ascolto.

[more info \(11\)](#)

Usa questo parametro per specificare il numero massimo o minimo di porte TCP o UDP su cui ciascun dispositivo può essere in ascolto.

Origine: lato dispositivo

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: porte

Esempio:

```
{
 "name": "Max TCP Ports",
 "metric": "aws:num-listening-tcp-ports",
 "criteria": {
 "comparisonOperator": "less-than-equals",
 "value": {
 "count": 4
 },
 "consecutiveDatapointsToAlarm": 2,
 "consecutiveDatapointsToClear": 1
 }
}
```

Esempio utilizzando un `statisticalThreshold`:

```
{
 "name": "Max TCP Ports",
 "metric": "aws:num-listening-tcp-ports",
 "criteria": {
 "comparisonOperator": "less-than-equals",
 "statisticalThreshold": {
 "statistic": "p90"
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 2,
 "consecutiveDatapointsToClear": 1
 }
}
```

**aws:num-established-tcp-connections**

Numero di connessioni TCP per un dispositivo.

[more info \(12\)](#)

Usa questo parametro per specificare il numero massimo o minimo di connessioni TCP attive che ciascun dispositivo può avere. (Tutti gli stati TCP)

Origine: lato dispositivo

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: connessioni

Esempio:

```
{
 "name": "TCP Connection Count",
 "metric": "aws:num-established-tcp-connections",
 "criteria": {
 "comparisonOperator": "less-than",
 "value": {
 "count": 3
 },
 "consecutiveDatapointsToAlarm": 3,
 "consecutiveDatapointsToClear": 3
 }
}
```

Esempio utilizzando un `statisticalThreshold`:

```
{
 "name": "TCP Connection Count",
 "metric": "aws:num-established-tcp-connections",
 "criteria": {
 "comparisonOperator": "less-than",
 "statisticalThreshold": {
 "statistic": "p90"
 },
 "durationSeconds": 900,
 "consecutiveDatapointsToAlarm": 3,
 "consecutiveDatapointsToClear": 3
 }
}
```

**aws:num-connection-attempts**

il numero di tentativi di connessione di un dispositivo in un determinato periodo di tempo.

[more info \(13\)](#)

Usa questo parametro per specificare il numero massimo o minimo di tentativi di connessione per ciascun dispositivo. Vengono conteggiati sia i tentativi riusciti che quelli non riusciti.

Origine: lato cloud

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: tentativi di connessione

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Esempio:

```
{
 "name": "Connection Attempts",
 "metric": "aws:num-connection-attempts",
 "criteria": {
 "comparisonOperator": "greater-than",
 "value": {
 "count": 5
 },
 "durationSeconds": 600,
 "consecutiveDatapointsToAlarm": 1,
 "consecutiveDatapointsToClear": 2
 }
}
```

Esempio utilizzando un **statisticalThreshold**:

```
{
 "name": "Connection Attempts",
 "metric": "aws:num-connection-attempts",
 "criteria": {
 "comparisonOperator": "greater-than",
 "statisticalThreshold": {
 "statistic": "p10"
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 1,
 "consecutiveDatapointsToClear": 2
 }
}
```

#### aws:num-disconnects

Il numero di disconnessioni da AWS IoT di un dispositivo durante un determinato periodo di tempo.

[more info \(14\)](#)

Utilizza questo parametro per specificare il numero massimo o minimo di disconnessioni di un dispositivo da AWS IoT durante un determinato periodo di tempo.

Origine: lato cloud

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: disconnessioni

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Esempio:

```
{
 "name": "Disconnections",
 "metric": "aws:num-disconnects",
 "criteria": {
 "comparisonOperator": "greater-than",
 "value": {
 "count": 5
 },
 "durationSeconds": 600,
 "consecutiveDatapointsToAlarm": 1,
 "consecutiveDatapointsToClear": 2
 }
}
```

Esempio di utilizzo di un statisticalThreshold:

```
{
 "name": "Disconnections",
 "metric": "aws:num-disconnects",
 "criteria": {
 "comparisonOperator": "greater-than",
 "statisticalThreshold": {
 "statistic": "p10"
 },
 "durationSeconds": 300,
 "consecutiveDatapointsToAlarm": 1,
 "consecutiveDatapointsToClear": 2
 }
}
```

## Monitoraggio del comportamento dei dispositivi non registrati

AWS IoT Device Defender consente di identificare comportamenti insoliti per i dispositivi che non vengono registrati nel registro AWS IoT. È possibile definire i profili di sicurezza specifici per uno dei seguenti tipi di destinazione:

- Tutti i dispositivi
- Tutti i dispositivi registrati (oggetti nel registro AWS IoT)
- Tutti i dispositivi non registrati
- Dispositivi in un gruppo di oggetti

Un profilo di sicurezza definisce una serie di comportamenti attesi per i dispositivi nel tuo account e specifica le azioni da eseguire quando viene rilevata un'anomalia. I profili di sicurezza devono essere collegati ai target più specifici per conferirti il controllo granulare su quali dispositivi sono valutati rispetto a tale profilo.

I dispositivi non registrati devono fornire un identificatore client MQTT coerente o un nome oggetto (per dispositivi che segnalano i parametri di dispositivo) per la durata di vita del dispositivo, in modo che tutte le violazioni e i parametri siano attribuiti allo stesso dispositivo.

### Important

I messaggi riportati dai dispositivi sono rifiutati se il nome dell'oggetto contiene caratteri di controllo oppure se il nome dell'oggetto è più lungo di 128 byte di codifica UTF-8.

## Come utilizzare AWS IoT Device Defender Detect

1. Puoi usare AWS IoT Device Defender Detect con solo i parametri lato cloud, ma se prevedi di usare parametri segnalati dai dispositivi, dovrà innanzitutto distribuire un SDK AWS IoT nei gateway dei dispositivi o nei dispositivi connessi a AWS IoT. Per ulteriori informazioni, consulta [Invio di parametri dai dispositivi \(p. 575\)](#).
2. Considerare di visualizzare le metriche generate dai dispositivi prima di definire i comportamenti e creare gli allarmi. AWS IoT è in grado di raccogliere i parametri dai tuoi dispositivi in modo da identificare innanzitutto un comportamento consueto o insolito per un gruppo di dispositivi o per tutti i dispositivi nel tuo account. Utilizza [CreateSecurityProfile \(p. 582\)](#) ma specifica solo quei additionalMetricsToRetain cui sei interessato. Non specificare alcun behaviors in questa fase.

Utilizza la console AWS IoT per vedere i parametri del tuo dispositivo e definire in cosa consiste il comportamento tipico dei tuoi dispositivi.

3. Crea un set di comportamenti per il profilo di sicurezza. I comportamenti contengono parametri che specificano il comportamento normale per un gruppo di dispositivi o per tutti i dispositivi nell'account. Per ulteriori informazioni, inclusi gli esempi, vedere [Parametri \(p. 561\)](#). Dopo aver creato un set di comportamenti, puoi convalidarli con [ValidateSecurityProfileBehaviors \(p. 616\)](#).
4. Usa [CreateSecurityProfile \(p. 582\)](#) per creare un profilo di sicurezza che includa i comportamenti. Puoi fare in modo che vengano inviati avvisi a un target (un argomento SNS) quando un dispositivo viola un comportamento usando il parametro alertTargets. Se invii avvisi tramite SNS, tieni presente che verranno conteggiati per il raggiungimento del limite SNS per l'account. In caso di violazioni su vasta scala si potrebbe esaurire la capacità disponibile. È inoltre possibile utilizzare i parametri CloudWatch per verificare la presenza di violazioni. Per ulteriori informazioni, consulta [Parametri di AWS IoT \(p. 646\)](#).
5. Utilizzare [AttachSecurityProfile \(p. 580\)](#) per collegare il profilo di sicurezza a un gruppo di dispositivi (un gruppo di oggetti), tutti gli elementi registrati nel tuo account, tutti gli oggetti non registrati o tutti i dispositivi. AWS IoT Device Defender Detect inizia a verificare la presenza di comportamenti anomali e, se viene rilevato il comportamento di eventuali violazioni, invia avvisi. È possibile allegare un profilo di sicurezza a tutti gli oggetti non registrati se, ad esempio, si prevede di interagire con dispositivi mobili che non sono nel registro degli oggetti del tuo account. È possibile definire comportamenti diversi per i diversi gruppi di dispositivi per soddisfare le tue esigenze.

Per collegare un profilo di sicurezza a un gruppo di dispositivi, è necessario specificare l'ARN del gruppo di oggetti che li contiene. L'ARN di un gruppo di oggetti ha il formato seguente:

```
arn:aws:iot:<region>:<accountid>:thinggroup/<thing-group-name>
```

Per allegare un profilo di sicurezza a tutti gli oggetti registrati in un account (ignorando gli oggetti non registrati), è necessario specificare un ARN con il seguente formato:

```
arn:aws:iot:<region>:<accountid>:all/registered-things
```

Per allegare un profilo di sicurezza a tutti gli oggetti non registrati, è necessario specificare un ARN con il seguente formato:

```
arn:aws:iot:<region>:<accountid>:all/unregistered-things
```

Per allegare un profilo di sicurezza a tutti i dispositivi, è necessario specificare un ARN con il seguente formato:

```
arn:aws:iot:<region>:<accountid>:all/things
```

6. Puoi anche tenere traccia delle violazioni con [ListActiveViolations \(p. 593\)](#), che ti permette di visualizzare le violazioni rilevate per un determinato profilo di sicurezza o dispositivo target.  
Usa [ListViolationEvents \(p. 603\)](#) per visualizzare le violazioni rilevate in un periodo di tempo specificato. È possibile filtrare i risultati in base a un determinato profilo di sicurezza o dispositivo.  
7. Se i tuoi dispositivi violano i comportamenti definiti troppo spesso o non abbastanza spesso, è consigliabile affinare il comportamento definizioni.  
8. Per esaminare i profili di sicurezza configurati e i dispositivi monitorati, usa [ListSecurityProfiles \(p. 598\)](#), [ListSecurityProfilesForTarget \(p. 600\)](#) e [ListTargetsForSecurityProfile \(p. 601\)](#).  
Usa [DescribeSecurityProfile \(p. 588\)](#) per ottenere ulteriori dettagli su un profilo di sicurezza.
9. Per apportare modifiche a un profilo di sicurezza, usa [UpdateSecurityProfile \(p. 608\)](#). Utilizza [DetachSecurityProfile \(p. 592\)](#) per distaccare un profilo di sicurezza da parte di un account o di un gruppo di oggetti target. Usa [DeleteSecurityProfile \(p. 587\)](#) per eliminare un profilo di sicurezza in modo completo.

## Autorizzazioni

Questa sezione contiene informazioni su come configurare le policy e i ruoli IAM necessari per gestire AWS IoT Device Defender Detect. Per ulteriori informazioni, consulta la [Guida per l'utente di AWS Identity and Access Management](#).

### Concessione a AWS IoT Device Defender Detect dell'autorizzazione per pubblicare gli avvisi in un argomento SNS.

Se usi il parametro `alertTargets` in [CreateSecurityProfile \(p. 582\)](#), devi specificare un ruolo IAM con due policy, una policy di autorizzazioni e una policy di trust. La policy di autorizzazioni concede a AWS IoT Device Defender l'autorizzazione per pubblicare le notifiche nell'argomento SNS. La policy di attendibilità concede a AWS IoT Device Defender l'autorizzazione per assumere il ruolo richiesto.

[Policy delle autorizzazioni](#)

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "sns:Publish"
],
 "Resource": [
 "arn:aws:sns:region:account-id:your-topic-name"
]
 }
]
}
```

[Policy di trust](#)

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "",
 "Effect": "Allow",
 "Action": [
 "sts:AssumeRole"
],
 "Principal": "arn:aws:iot:region:account-id:device-id"
 }
]
}
```

```
 "Principal": {
 "Service": "iot.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
}
```

policy per il passaggio di ruoli

È necessaria anche una policy di autorizzazioni IAM collegata all'utente IAM che consenta all'utente di passare i ruoli. Consulta [Concessione di autorizzazioni utente per il passaggio di un ruolo a un servizio AWS](#).

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "",
 "Effect": "Allow",
 "Action": [
 "iam:GetRole",
 "iam:PassRole"
],
 "Resource": "arn:aws:iam::>account-id<:role/Role_To_Pass"
 }
]
}
```

## Restrizioni dei servizi

- Il numero massimo di profili di sicurezza per ogni target (gruppo di oggetti o account utente) è 5.
- Il numero massimo di comportamenti per ogni profilo di sicurezza è 100.
- Il numero massimo di elementi value (conteggi, indirizzi IP, porte) per il profilo di sicurezza è 1000.
- La segnalazione dei parametri dei dispositivi potrebbe essere limitata a una ogni 5 minuti per dispositivo. Per evitare il throttling, limita la segnalazione dei parametri dei dispositivi a una ogni 5 minuti.
- Le violazioni di AWS IoT Device Defender Detect vengono archiviate per 30 giorni dopo che sono state generate.

## Invio di parametri dai dispositivi

AWS IoT Device Defender Detect permette di raccogliere, aggregare e monitorare i dati dei parametri generati dai dispositivi AWS IoT per identificare i dispositivi che presentano un comportamento anomalo. Questa sezione contiene informazioni su come inviare i parametri da un dispositivo a AWS IoT Device Defender.

Devi distribuire in modo sicuro un SDK AWS IoT nei gateway dei dispositivi o nei dispositivi connessi a AWS IoT per raccogliere i parametri lato dispositivo. AWS IoT Device Defender fornisce agenti di esempio da usare come esempi per la creazione di un agente personalizzato. Se non sei in grado di fornire i parametri dei dispositivi, puoi continuare a usufruire di funzionalità limitate basate sui parametri lato cloud.

Tieni presente quanto segue:

- Un agente di segnalazione dei parametri dei dispositivi di esempio è attualmente disponibile in C all'indirizzo <https://github.com/aws-samples/aws-iot-device-defender-agent-c>. Un agente di segnalazione dei parametri dei dispositivi di esempio è disponibile anche in Python su GitHub all'indirizzo <https://github.com/aws-samples/aws-iot-device-defender-agent-sdk-python> (in modo specifico [qui](#)).

- Per utilizzare agenti di esempio o creare il tuo agente personalizzato, è necessario installare Device SDK per AWS IoT. Per visualizzare i collegamenti per la tua lingua di sviluppo preferita, visita [Risorse AWS IoT Core](#).
- Tutti gli agenti devono creare una connessione a AWS IoT e pubblicare parametri in uno di questi argomenti MQTT Device Defender riservati:

```
$aws/things/THING_NAME/Defender/metrics/json
```

oppure

```
$aws/things/THING_NAME/Defender/metrics/cbor
```

Device Defender replicherà con lo stato di ricezione dei report di parametri utilizzando uno di questi argomenti:

```
$aws/things/THING_NAME/Defender/metrics/json/accepted
```

```
$aws/things/THING_NAME/Defender/metrics/cbor/accepted
```

```
$aws/things/THING_NAME/Defender/metrics/json/rejected
```

```
$aws/things/THING_NAME/Defender/metrics/cbor/rejected
```

- Per segnalare i parametri, un dispositivo deve essere registrato come oggetto in AWS IoT.
- Un dispositivo deve, in genere, inviare una segnalazione una volta ogni 5 minuti. I dispositivi sono limitati a un report sui parametri ogni 5 minuti. Un dispositivo non è in grado di eseguire più di un report di parametri ogni 5 minuti).
- I dispositivi devono segnalare i parametri correnti. Il report sui parametri storici non è supportato.
- Puoi utilizzare [Processi \(p. 368\)](#) per impostare l'intervallo per la segnalazione dei parametri delle tue istanze di agenti di segnalazione dei parametri dei dispositivi. Un esempio è incluso negli esempi Device Defender Agent C. Per ulteriori informazioni, consulta il file [README.md](#).

## Specifiche del documento di parametri dei dispositivi

Struttura generale:

| Nome lungo | Nome breve | Campo obbligatorio | Tipo    | Vincoli | Note                                                          |
|------------|------------|--------------------|---------|---------|---------------------------------------------------------------|
| header     | hed        | Y                  | Oggetto |         | Blocco completo necessario per un report in formato corretto. |
| metrics    | met        | Y                  | Oggetto |         | Blocco completo necessario per un report in formato corretto. |

Blocco di intestazione:

| Nome lungo | Nome breve | Campo obbligatorio | Tipo    | Vincoli     | Note                                                                                         |
|------------|------------|--------------------|---------|-------------|----------------------------------------------------------------------------------------------|
| report_id  | rid        | Y                  | Integer |             | Valore crescente in maniera monotona. Timestamp epoch consigliato.                           |
| Versione   | v          | Y                  | Stringa | Major.Minor | Incrementi minori con aggiunta di campo. Incrementi maggiori se i parametri vengono rimossi. |

Blocco dei parametri:

Connessioni TCP:

| Nome lungo              | Nome breve | Elemento padre          | Campo obbligatorio | Tipo                | Vincoli  | Note                             |
|-------------------------|------------|-------------------------|--------------------|---------------------|----------|----------------------------------|
| tcp_connection\$c       |            | metrics                 | N                  | Oggetto             |          |                                  |
| established_connections |            | tcp_connections\$N      |                    | Elenco<Connessione> |          | Stato connessione TCP stabilità  |
| connections             | cs         | established_connections |                    | Elenco<Oggetto>     |          |                                  |
| remote_addr             | rad        | connections             | Y                  | Numero              | ip:porta | ip può essere ipv6 o ipv4        |
| local_port              | lp         | connections             | N                  | Numero              | >= 0     |                                  |
| local_interface         | li         | connections             | N                  | Stringa             |          | nome interfaccia                 |
| total                   | t          | established_connections |                    | Numero              | >= 0     | Numero di connessioni stabilite. |

Porte TCP in ascolto:

| Nome lungo          | Nome breve | Elemento padre | Campo obbligatorio | Tipo    | Vincoli | Note |
|---------------------|------------|----------------|--------------------|---------|---------|------|
| listening_tcp_ports |            | metrics        | N                  | Oggetto |         |      |

| Nome lungo | Nome breve | Elemento padre      | Campo obbligatorio | Tipo          | Vincoli | Note                                |
|------------|------------|---------------------|--------------------|---------------|---------|-------------------------------------|
| ports      | pts        | listening_tcp_ports | N                  | Elenco<Porta> | > 0     |                                     |
| port       | pt         | ports               | N                  | Numero        | > 0     | i numeri di porta devono essere > 0 |
| interface  | if         | ports               | N                  | Stringa       |         | nome interfaccia                    |
| total      | t          | listening_tcp_ports | N                  | Numero        | >= 0    |                                     |

Porte UDP in ascolto:

| Nome lungo          | Nome breve | Elemento padre      | Campo obbligatorio | Tipo          | Vincoli | Note                                |
|---------------------|------------|---------------------|--------------------|---------------|---------|-------------------------------------|
| listening_udp_ports |            | metrics             | N                  | Oggetto       |         |                                     |
| ports               | pts        | listening_udp_ports | N                  | Elenco<Porta> | > 0     |                                     |
| port                | pt         | ports               | N                  | Numero        | > 0     | i numeri di porta devono essere > 0 |
| interface           | if         | ports               | N                  | Stringa       |         | nome interfaccia                    |
| total               | t          | listening_udp_ports | N                  | Numero        | >= 0    |                                     |

Statistiche di rete:

| Nome lungo    | Nome breve | Elemento padre | Campo obbligatorio | Tipo    | Vincoli               | Note |
|---------------|------------|----------------|--------------------|---------|-----------------------|------|
| network_stats | ns         | metrics        | N                  | Oggetto |                       |      |
| bytes_in      | bi         | network_stats  | N                  | Numero  | Parametro delta, >= 0 |      |
| bytes_out     | bo         | network_stats  | N                  | Numero  | Parametro delta, >= 0 |      |
| packets_in    | pi         | network_stats  | N                  | Numero  | Parametro delta, >= 0 |      |
| packets_out   | po         | network_stats  | N                  | Numero  | Parametro delta, >= 0 |      |

Esempio di struttura JSON con nomi lunghi:

```
{
 "header": {
 "report_id": 1530304554,
 "version": "1.0"
 }
}
```

```
},
"metrics": {
 "listening_tcp_ports": {
 "ports": [
 {
 "interface": "eth0",
 "port": 24800
 },
 {
 "interface": "eth0",
 "port": 22
 },
 {
 "interface": "eth0",
 "port": 53
 }
],
 "total": 3
 },
 "listening_udp_ports": {
 "ports": [
 {
 "interface": "eth0",
 "port": 5353
 },
 {
 "interface": "eth0",
 "port": 67
 }
],
 "total": 2
 },
 "network_stats": {
 "bytes_in": 29358693495,
 "bytes_out": 26485035,
 "packets_in": 10013573555,
 "packets_out": 11382615
 },
 "tcp_connections": {
 "established_connections": {
 "connections": [
 {
 "local_interface": "eth0",
 "local_port": 80,
 "remote_addr": "192.168.0.1:8000"
 },
 {
 "local_interface": "eth0",
 "local_port": 80,
 "remote_addr": "192.168.0.1:8000"
 }
],
 "total": 2
 }
 }
}
```

Esempio di struttura JSON con nomi brevi:

```
{
 "hed": {
 "rid": 1530305228,
 "v": "1.0"
 },
}
```

```
"met": {
 "tp": {
 "pts": [
 {
 "if": "eth0",
 "pt": 24800
 },
 {
 "if": "eth0",
 "pt": 22
 },
 {
 "if": "eth0",
 "pt": 53
 }
],
 "t": 3
 },
 "up": {
 "pts": [
 {
 "if": "eth0",
 "pt": 5353
 },
 {
 "if": "eth0",
 "pt": 67
 }
],
 "t": 2
 },
 "ns": {
 "bi": 29359307173,
 "bo": 26490711,
 "pi": 10014614051,
 "po": 11387620
 },
 "tc": {
 "ec": {
 "cs": [
 {
 "li": "eth0",
 "lp": 80,
 "rad": "192.168.0.1:8000"
 },
 {
 "li": "eth0",
 "lp": 80,
 "rad": "192.168.0.1:8000"
 }
],
 "t": 2
 }
 }
}
```

## Comandi di rilevamento

### AttachSecurityProfile

Associa un profilo di sicurezza AWS IoT Device Defender a uno dei seguenti tipi di target:

- Tutti i dispositivi
- Tutti i dispositivi registrati (oggetti nel registro AWS IoT)
- Tutti i dispositivi non registrati
- Dispositivi in un gruppo di oggetti

Ogni tipo di target può avere fino a cinque profili di sicurezza associati.

Riepilogo:

```
aws iot attach-security-profile \
 --security-profile-name <value> \
 --security-profile-target-arn <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "securityProfileName": "string",
 "securityProfileTargetArn": "string"
}
```

Campi di **cli-input-json**:

| Nome                     | Tipo                                                                          | Descrizione                                                                   |
|--------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| securityProfileName      | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Profilo di sicurezza collegato.                                               |
| securityProfileTargetArn | Stringa                                                                       | ARN del target (gruppo di oggetti) a cui è collegato il profilo di sicurezza. |

Per collegare un profilo di sicurezza a un gruppo di dispositivi, è necessario specificare l'ARN del gruppo di oggetti che li contiene. L'ARN di un gruppo di oggetti ha il formato seguente:

```
arn:aws:iot:<region>:<accountid>:thinggroup/<thing-group-name>
```

Per allegare un profilo di sicurezza a tutti gli oggetti registrati in un account (ignorando gli oggetti non registrati), è necessario specificare un ARN con il seguente formato:

```
arn:aws:iot:<region>:<accountid>:all/registered-things
```

Per allegare un profilo di sicurezza a tutti gli oggetti non registrati, è necessario specificare un ARN con il seguente formato:

```
arn:aws:iot:<region>:<accountid>:all/unregistered-things
```

Per allegare un profilo di sicurezza a tutti i dispositivi, è necessario specificare un ARN con il seguente formato:

```
arn:aws:iot:<region>:<accountid>:all/things
```

Output:

Nessuna

Errori:

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**LimitExceededException**

È stato superato un limite.

**VersionConflictException**

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## CreateSecurityProfile

Crea un profilo di sicurezza di Device Defender.

Riepilogo:

```
aws iot create-security-profile \
 --security-profile-name <value> \
 [--security-profile-description <value>] \
 [--behaviors <value>] \
 [--alert-targets <value>] \
 [--additional-metrics-to-retain <value>] \
 [--tags <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di cli-input-json:

```
{
 "securityProfileName": "string",
 "securityProfileDescription": "string",
 "behaviors": [
 {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
]
 }
 }
 }
]
}
```

```

],
 "ports": [
 "integer"
]
 },
 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "statistic": "string"
 }
}
],
"alertTargets": {
 "string": {
 "alertTargetArn": "string",
 "roleArn": "string"
 }
},
"additionalMetricsToRetain": [
 "string"
],
"tags": [
 {
 "Key": "string",
 "Value": "string"
 }
]
}

```

Campi di **cli-input-json**:

| Nome                       | Tipo                                                                          | Descrizione                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| securityProfileName        | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome da assegnare al profilo di sicurezza.                                                                      |
| securityProfileDescription | Stringa<br><br>Lunghezza max: 1000<br><br>Modello: [\p{Graph}]*               | Descrizione del profilo di sicurezza.                                                                           |
| behaviors                  | elenco<br><br>membro: Behavior                                                | Specifica i comportamenti che, quando violati da un dispositivo (oggetto), causano la generazione di un avviso. |
| name                       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome assegnato al comportamento.                                                                                |
| metric                     | Stringa                                                                       | Valore misurato dal comportamento.                                                                              |
| criteria                   | BehaviorCriteria                                                              | Criteri che determinano se un dispositivo presenta un                                                           |

| Nome               | Tipo                             | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    |                                  | comportamento normale in relazione a <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| comparisonOperator | Stringa                          | Operatore che mette in correlazione l'oggetto misurato ( <code>metric</code> ) e i criteri (contenenti un <code>value</code> o <code>statisticalThreshold</code> ).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set                                                                                                                                                                                                                                                            |
| value              | MetricValue                      | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count              | Long<br><br>Intervallo - min.: 0 | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cidrs              | elenco<br><br>membro: Cidr       | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports              | elenco<br><br>membro: Port       | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds    | integer                          | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |

| Nome                         | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| consecutiveDatapointsToAlarm | integer<br><br>Intervallo – Max: 10, min.: 1                                 | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| consecutiveDatapointsToClear | integer<br><br>Intervallo – Max: 10, min.: 1                                 | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| statisticalThreshold         | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistic                    | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato ( <code>durationSeconds</code> ) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto ( <code>comparisonOperator</code> ) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario si verifica una violazione. |
| alertTargets                 | mappa                                                                        | Specifica le destinazioni di invio degli avvisi. Gli avvisi vengono sempre inviati alla console. Gli avvisi vengono generati quando un dispositivo (oggetto) viola un comportamento.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| alertTargetArn               | Stringa                                                                      | ARN del target di notifica a cui vengono inviati gli avvisi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Nome                      | Tipo                                                 | Descrizione                                                                                                                                                                                                                                                               |
|---------------------------|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn                   | Stringa<br>Lunghezza max: 2048, min.: 20             | ARN del ruolo che concede l'autorizzazione per l'invio degli avvisi al target di notifica.                                                                                                                                                                                |
| additionalMetricsToRetain | elenco<br>membro: BehaviorMetric                     | Un elenco di parametri i cui dati vengono conservati (archiviati). Per impostazione predefinita, i dati vengono conservati per qualsiasi parametro utilizzato nel <code>behaviors</code> del profilo ma vengono anche conservati per qualsiasi parametro specificato qui. |
| tags                      | elenco<br>member: Tag<br>Classe Java: java.util.List | Metadati utilizzabili per la gestione del profilo di sicurezza.                                                                                                                                                                                                           |
| Chiave                    | Stringa                                              | La chiave del tag.                                                                                                                                                                                                                                                        |
| Valore                    | Stringa                                              | Il valore del tag.                                                                                                                                                                                                                                                        |

Output:

```
{
 "securityProfileName": "string",
 "securityProfileArn": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome                | Tipo                                                                  | Descrizione                             |
|---------------------|-----------------------------------------------------------------------|-----------------------------------------|
| securityProfileName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome assegnato al profilo di sicurezza. |
| securityProfileArn  | Stringa                                                               | ARN del profilo di sicurezza.           |

Errori:

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceAlreadyExistsException`

La risorsa esiste già.

`ThrottlingException`

La velocità supera il limite.

#### InternalFailureException

Si è verificato un errore imprevisto.

## DeleteSecurityProfile

Elimina un profilo di sicurezza di Device Defender.

Riepilogo:

```
aws iot delete-security-profile \
--security-profile-name <value> \
[--expected-version <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "securityProfileName": "string",
 "expectedVersion": "long"
}
```

Campi di **cli-input-json**:

| Nome                | Tipo                                                                  | Descrizione                                                                                                                                                                                                                                                    |
|---------------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| securityProfileName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del profilo di sicurezza da eliminare.                                                                                                                                                                                                                    |
| expectedVersion     | Long                                                                  | Versione prevista del profilo di sicurezza. Viene generata una nuova versione ogni volta che il profilo di sicurezza viene aggiornato. Se specifichi un valore diverso dalla versione effettiva, viene generata un'eccezione <b>VersionConflictException</b> . |

Output:

Nessuna

Errori:

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### ThrottlingException

La velocità supera il limite.

#### InternalFailureException

Si è verificato un errore imprevisto.

### VersionConflictException

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

## DescribeSecurityProfile

Ottiene le informazioni su un profilo di sicurezza di Device Defender.

Riepilogo:

```
aws iot describe-security-profile \
--security-profile-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di cli-input-json:

```
{
 "securityProfileName": "string"
}
```

Campi di **cli-input-json**:

| Nome                | Tipo                                                                  | Descrizione                                                    |
|---------------------|-----------------------------------------------------------------------|----------------------------------------------------------------|
| securityProfileName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del profilo di sicurezza di cui ottenere le informazioni. |

Output:

```
{
 "securityProfileName": "string",
 "securityProfileArn": "string",
 "securityProfileDescription": "string",
 "behaviors": [
 {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 },
 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "statistic": "string"
 }
 }
 }
]
}
```

```

 }
],
 "alertTargets": {
 "string": {
 "alertTargetArn": "string",
 "roleArn": "string"
 }
 },
 "additionalMetricsToRetain": [
 "string"
],
 "version": "long",
 "creationDate": "timestamp",
 "lastModifiedDate": "timestamp"
}

```

Campi di output dell'interfaccia a riga di comando:

| Nome                       | Tipo                                                                          | Descrizione                                                                                                                                                                                |
|----------------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| securityProfileName        | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome del profilo di sicurezza.                                                                                                                                                             |
| securityProfileArn         | Stringa                                                                       | ARN del profilo di sicurezza.                                                                                                                                                              |
| securityProfileDescription | Stringa<br><br>Lunghezza max: 1000<br><br>Modello: [\p{Graph}]*               | Descrizione del profilo di sicurezza (associata al profilo di sicurezza al momento della creazione o dell'aggiornamento).                                                                  |
| behaviors                  | elenco<br><br>membro: Behavior                                                | Specifica i comportamenti che, quando violati da un dispositivo (oggetto), causano la generazione di un avviso.                                                                            |
| name                       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome assegnato al comportamento.                                                                                                                                                           |
| metric                     | Stringa                                                                       | Valore misurato dal comportamento.                                                                                                                                                         |
| criteria                   | BehaviorCriteria                                                              | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a metric.                                                                                         |
| comparisonOperator         | Stringa                                                                       | Operatore che mette in correlazione l'oggetto misurato (metric) e i criteri (contenenti un value o statisticalThreshold).<br><br>enumerazione: less-than   less-than-equals   greater-than |

| Nome                         | Tipo                                     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              |                                          | greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| value                        | MetricValue                              | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count                        | Long<br>Intervallo - min.: 0             | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cids                         | elenco<br>membro: Cidr                   | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports                        | elenco<br>membro: Port                   | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds              | integer                                  | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |
| consecutiveDatapointsToAlarm | integer<br>Intervallo – Max: 10, min.: 1 | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                      |

| Nome                         | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| consecutiveDatapointsToClear | integer<br><br>Intervallo – Max: 10, min.: 1                                 | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                 |
| statisticalThreshold         | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| statistic                    | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato (durationSeconds) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto (comparisonOperator) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento. In caso contrario, si verifica una violazione. |
| alertTargets                 | mappa                                                                        | Destinazione di invio degli avvisi. Gli avvisi vengono sempre inviati alla console.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| alertTargetArn               | Stringa                                                                      | ARN del target di notifica a cui vengono inviati gli avvisi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| roleArn                      | Stringa<br><br>Lunghezza max: 2048, min.: 20                                 | ARN del ruolo che concede l'autorizzazione per l'invio degli avvisi al target di notifica.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Nome                      | Tipo                             | Descrizione                                                                                                                                                                                                                                                  |
|---------------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| additionalMetricsToRetain | elenco<br>membro: BehaviorMetric | Un elenco di parametri i cui dati vengono conservati (archiviati). Per impostazione predefinita, i dati vengono conservati per qualsiasi parametro utilizzato nel behaviors del profilo ma vengono anche conservati per qualsiasi parametro specificato qui. |
| Versione                  | Long                             | Versione del profilo di sicurezza. Viene generata una nuova versione ogni volta che il profilo di sicurezza viene aggiornato.                                                                                                                                |
| creationDate              | timestamp                        | Ora della creazione del profilo di sicurezza.                                                                                                                                                                                                                |
| lastModifiedDate          | timestamp                        | Ora dell'ultima modifica del profilo di sicurezza.                                                                                                                                                                                                           |

Errori:

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceNotFoundException`

La risorsa specificata non esiste.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

## DetachSecurityProfile

Elimina l'associazione di un profilo di sicurezza di Device Defender da un gruppo di oggetti o dall'account.

Riepilogo:

```
aws iot detach-security-profile \
--security-profile-name <value> \
--security-profile-target-arn <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`:

```
{
 "securityProfileName": "string",
 "securityProfileTargetArn": "string"
```

}

Campi di **cli-input-json**:

| Nome                     | Tipo    | Descrizione                                                                                            |
|--------------------------|---------|--------------------------------------------------------------------------------------------------------|
| securityProfileName      | Stringa | Profilo di sicurezza scollegato.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ |
| securityProfileTargetArn | Stringa | ARN del gruppo di oggetti da cui viene scollegato il profilo di sicurezza.                             |

Output:

Nessuna

Errori:

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## ListActiveViolations

Elenca le violazioni attive per un determinato profilo di Device Defender.

Riepilogo:

```
aws iot list-active-violations \
[--thing-name <value>] \
[--security-profile-name <value>] \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "thingName": "string",
 "securityProfileName": "string",
 "nextToken": "string",
```

```

 "maxResults": "integer"
 }
}
```

**Campi di cli-input-json:**

| Nome                | Tipo                                                                  | Descrizione                                                                                   |
|---------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| thingName           | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto per il quale vengono elencate le violazioni attive.                         |
| securityProfileName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del profilo di sicurezza di Device Defender per il quale vengono elencate le violazioni. |
| nextToken           | Stringa                                                               | Token per il set di risultati successivo.                                                     |
| maxResults          | integer<br>Intervallo – Max: 250, min.: 1                             | Numero massimo di risultati da restituire per volta.                                          |

**Output:**

```
{
 "activeViolations": [
 {
 "violationId": "string",
 "thingName": "string",
 "securityProfileName": "string",
 "behavior": {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 },
 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "statistic": "string"
 }
 }
 },
 "lastViolationValue": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [

```

```

 "integer"
],
},
"lastViolationTime": "timestamp",
"violationStartTime": "timestamp"
],
"nextToken": "string"
}

```

Campi di output dell'interfaccia a riga di comando:

| Nome                | Tipo                                                                          | Descrizione                                                                                                                                                                                                                    |
|---------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| activeViolations    | elenco<br>membro: ActiveViolation                                             | Elenco di violazioni attive.                                                                                                                                                                                                   |
| violationId         | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 -]+   | ID della violazione attiva.                                                                                                                                                                                                    |
| thingName           | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto responsabile della violazione attiva.                                                                                                                                                                        |
| securityProfileName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Profilo di sicurezza il cui comportamento causa una violazione.                                                                                                                                                                |
| behavior            | Comportamento                                                                 | Il comportamento violato.                                                                                                                                                                                                      |
| name                | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome assegnato al comportamento.                                                                                                                                                                                               |
| metric              | Stringa                                                                       | Valore misurato dal comportamento.                                                                                                                                                                                             |
| criteria            | BehaviorCriteria                                                              | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a metric.                                                                                                                             |
| comparisonOperator  | Stringa                                                                       | Operatore che mette in correlazione l'oggetto misurato (metric) e i criteri (contenenti un value o statisticalThreshold).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set |

| Nome                         | Tipo                                     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              |                                          | not-in-cidr-set   in-port-set   not-in-port-set                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| value                        | MetricValue                              | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count                        | Long<br>Intervallo - min.: 0             | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cids                         | elenco<br>membro: Cidr                   | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports                        | elenco<br>membro: Port                   | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds              | integer                                  | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |
| consecutiveDatapointsToAlarm | integer<br>Intervallo – Max: 10, min.: 1 | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                      |

| Nome                         | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| consecutiveDatapointsToClear | integer<br><br>Intervallo – Max: 10, min.: 1                                 | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| statisticalThreshold         | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistic                    | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato ( <code>durationSeconds</code> ) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto ( <code>comparisonOperator</code> ) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario si verifica una violazione. |
| lastViolationValue           | MetricValue                                                                  | Valore del parametro (misurazione) che ha causato la violazione più recente.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| count                        | Long<br><br>Intervallo - min.: 0                                             | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| cids                         | elenco<br><br>membro: Cidr                                                   | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Nome               | Tipo                   | Descrizione                                                                                                                                       |
|--------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| ports              | elenco<br>membro: Port | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> . |
| lastViolationTime  | timestamp              | Ora in cui si è verificata la violazione più recente.                                                                                             |
| violationStartTime | timestamp              | Ora di inizio della violazione.                                                                                                                   |
| nextToken          | Stringa                | Token che è possibile usare per recuperare il set di risultati successivo oppure <code>null</code> se non ci sono risultati aggiuntivi.           |

Errori:

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceNotFoundException`

La risorsa specificata non esiste.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

## ListSecurityProfiles

Elenca i profili di sicurezza di Device Defender creati. Puoi usare i filtri per elencare solo i profili di sicurezza associati a un gruppo di oggetti oppure solo quelli associati all'account.

Riepilogo:

```
aws iot list-security-profiles \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`:

```
{
 "nextToken": "string",
 "maxResults": "integer"
}
```

Campi di **cli-input-json**:

| Nome       | Tipo    | Descrizione                                                                            |
|------------|---------|----------------------------------------------------------------------------------------|
| nextToken  | Stringa | Token per il set di risultati successivo.                                              |
| maxResults | integer | Numero massimo di risultati da restituire per volta.<br>Intervallo – Max: 250, min.: 1 |

Output:

```
{
 "securityProfileIdentifiers": [
 {
 "name": "string",
 "arn": "string"
 }
],
 "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome                       | Tipo                                                                       | Descrizione                                                                                                                             |
|----------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| securityProfileIdentifiers | elenco<br>membro: SecurityProfileIdentifier<br>Classe Java: java.util.List | Elenco di identificatori dei profili di sicurezza (nomi e ARN).                                                                         |
| name                       | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+      | Nome assegnato al profilo di sicurezza.                                                                                                 |
| arn                        | Stringa                                                                    | ARN del profilo di sicurezza.                                                                                                           |
| nextToken                  | Stringa                                                                    | Token che è possibile usare per recuperare il set di risultati successivo oppure <code>null</code> se non ci sono risultati aggiuntivi. |

Errori:

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

## ListSecurityProfilesForTarget

Elenca i profili di sicurezza di Device Defender collegati a un target (gruppo di oggetti).

Riepilogo:

```
aws iot list-security-profiles-for-target \
[--next-token <value>] \
[--max-results <value>] \
[--recursive | --no-recursive] \
--security-profile-target-arn <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "nextToken": "string",
 "maxResults": "integer",
 "recursive": "boolean",
 "securityProfileTargetArn": "string"
}
```

Campi di **cli-input-json**:

| Nome                     | Tipo     | Descrizione                                                                            |
|--------------------------|----------|----------------------------------------------------------------------------------------|
| nextToken                | Stringa  | Token per il set di risultati successivo.                                              |
| maxResults               | integer  | Numero massimo di risultati da restituire per volta.<br>Intervallo – Max: 250, min.: 1 |
| recursive                | booleano | Se è true, restituisce anche i gruppi figlio.                                          |
| securityProfileTargetArn | Stringa  | ARN del target (gruppo di oggetti) di cui ottenere i profili di sicurezza collegati.   |

Output:

```
{
 "securityProfileTargetMappings": [
 {
 "securityProfileIdentifier": {
 "name": "string",
 "arn": "string"
 },
 "target": {
 "arn": "string"
 }
 }
],
 "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome                          | Tipo                                                                             | Descrizione                                                                                                                |
|-------------------------------|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| securityProfileTargetMappings | elenco<br>membro:<br>SecurityProfileTargetMapping<br>Classe Java: java.util.List | Elenco di profili di sicurezza e dei target associati.                                                                     |
| securityProfileIdentifier     | SecurityProfileIdentifier                                                        | Informazioni che identificano il profilo di sicurezza.                                                                     |
| name                          | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_]+             | Nome assegnato al profilo di sicurezza.                                                                                    |
| arn                           | Stringa                                                                          | ARN del profilo di sicurezza.                                                                                              |
| target                        | SecurityProfileTarget                                                            | Informazioni sul target (gruppo di oggetti) associato al profilo di sicurezza.                                             |
| arn                           | Stringa                                                                          | ARN del profilo di sicurezza.                                                                                              |
| nextToken                     | Stringa                                                                          | Token che è possibile usare per recuperare il set di risultati successivo oppure null se non ci sono risultati aggiuntivi. |

Errori:

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ResourceNotFoundException**

La risorsa specificata non esiste.

## ListTargetsForSecurityProfile

Elenca i target (gruppi di oggetti) associati a un determinato profilo di sicurezza di Device Defender.

Riepilogo:

```
aws iot list-targets-for-security-profile \
--security-profile-name <value> \
[--next-token <value>] \
[--max-results <value>]
```

```
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "securityProfileName": "string",
 "nextToken": "string",
 "maxResults": "integer"
}
```

Campi di **cli-input-json**:

| Nome                | Tipo    | Descrizione                                                                                 |
|---------------------|---------|---------------------------------------------------------------------------------------------|
| securityProfileName | Stringa | Profilo di sicurezza.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ |
| nextToken           | Stringa | Token per il set di risultati successivo.                                                   |
| maxResults          | integer | Numero massimo di risultati da restituire per volta.<br><br>Intervallo – Max: 250, min.: 1  |

Output:

```
{
 "securityProfileTargets": [
 {
 "arn": "string"
 }
],
 "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome                   | Tipo                                                                           | Descrizione                                                                                                                             |
|------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| securityProfileTargets | elenco<br><br>membro: SecurityProfileTarget<br><br>Classe Java: java.util.List | Gruppi di oggetti a cui è collegato il profilo di sicurezza.                                                                            |
| arn                    | Stringa                                                                        | ARN del profilo di sicurezza.                                                                                                           |
| nextToken              | Stringa                                                                        | Token che è possibile usare per recuperare il set di risultati successivo oppure <code>null</code> se non ci sono risultati aggiuntivi. |

Errori:

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### ResourceNotFoundException

La risorsa specificata non esiste.

#### ThrottlingException

La velocità supera il limite.

#### InternalFailureException

Si è verificato un errore imprevisto.

## ListViolationEvents

Elenca le violazioni dei profili di sicurezza di Device Defender rilevate durante il periodo di tempo specificato. Puoi usare i filtri per limitare i risultati solo agli avvisi creati per un determinato profilo di sicurezza, comportamento o oggetto (dispositivo).

Riepilogo:

```
aws iot list-violation-events \
--start-time <value> \
--end-time <value> \
[--thing-name <value>] \
[--security-profile-name <value>] \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**:

```
{
 "startTime": "timestamp",
 "endTime": "timestamp",
 "thingName": "string",
 "securityProfileName": "string",
 "nextToken": "string",
 "maxResults": "integer"
}
```

Campi di **cli-input-json**:

| Nome      | Tipo                                                               | Descrizione                                                                 |
|-----------|--------------------------------------------------------------------|-----------------------------------------------------------------------------|
| startTime | timestamp                                                          | Ora di inizio degli avvisi da elencare.                                     |
| endTime   | timestamp                                                          | Ora di fine degli avvisi da elencare.                                       |
| thingName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-zA-Z0-9:_-]+ | Filtro che limita i risultati agli avvisi causati dall'oggetto specificato. |

| Nome                | Tipo                                                                  | Descrizione                                                                              |
|---------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| securityProfileName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+ | Filtro che limita i risultati agli avvisi generati dal profilo di sicurezza specificato. |
| nextToken           | Stringa                                                               | Token per il set di risultati successivo.                                                |
| maxResults          | integer<br>Intervallo – Max: 250, min.: 1                             | Numero massimo di risultati da restituire per volta.                                     |

Output:

```
{
 "violationEvents": [
 {
 "violationId": "string",
 "thingName": "string",
 "securityProfileName": "string",
 "behavior": {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 },
 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "statistic": "string"
 }
 }
 },
 "metricValue": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 },
 "violationEventType": "string",
 "violationEventTime": "timestamp"
 }
],
 "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome                | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                      |
|---------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| violationEvents     | elenco<br>membro: ViolationEvent                                             | Avvisi di violazione dei profili di sicurezza creati per l'account durante l'intervallo di tempo specificato, che possono essere filtrati in base a profilo di sicurezza, comportamento violato o oggetto (dispositivo) responsabile della violazione.                           |
| violationId         | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :-]+ | ID dell'evento di violazione.                                                                                                                                                                                                                                                    |
| thingName           | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :-]+ | Nome dell'oggetto responsabile dell'evento di violazione.                                                                                                                                                                                                                        |
| securityProfileName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :-]+ | Nome del profilo di sicurezza il cui comportamento è stato violato.                                                                                                                                                                                                              |
| behavior            | Comportamento                                                                | Il comportamento che è stato violato.                                                                                                                                                                                                                                            |
| name                | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :-]+ | Nome assegnato al comportamento.                                                                                                                                                                                                                                                 |
| metric              | Stringa                                                                      | Valore misurato dal comportamento.                                                                                                                                                                                                                                               |
| criteria            | BehaviorCriteria                                                             | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a metric.                                                                                                                                                                               |
| comparisonOperator  | Stringa                                                                      | Operatore che mette in correlazione l'oggetto misurato (metric) e i criteri (contenenti un value o statisticalThreshold).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set |

| Nome                         | Tipo                                     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| value                        | MetricValue                              | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count                        | Long<br>Intervallo - min.: 0             | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cids                         | elenco<br>membro: Cidr                   | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports                        | elenco<br>membro: Port                   | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds              | integer                                  | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |
| consecutiveDatapointsToAlarm | integer<br>Intervallo – Max: 10, min.: 1 | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                      |
| consecutiveDatapointsToClear | integer<br>Intervallo – Max: 10, min.: 1 | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                   |

| Nome                 | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| statisticalThreshold | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistic            | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato ( <code>durationSeconds</code> ) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto ( <code>comparisonOperator</code> ) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario si verifica una violazione. |
| metricValue          | MetricValue                                                                  | Valore del parametro (misurazione).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| count                | Long<br><br>Intervallo - min.: 0                                             | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| cids                 | elenco<br><br>membro: Cidr                                                   | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ports                | elenco<br><br>membro: Port                                                   | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| violationEventType   | Stringa                                                                      | Tipo di evento di violazione.<br><br>enumerazione: in-alarm   alarm-cleared   alarm-invalidated                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| violationEventTime   | timestamp                                                                    | Ora in cui si è verificato l'evento di violazione.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Nome      | Tipo    | Descrizione                                                                                                                             |
|-----------|---------|-----------------------------------------------------------------------------------------------------------------------------------------|
| nextToken | Stringa | Token che è possibile usare per recuperare il set di risultati successivo oppure <code>null</code> se non ci sono risultati aggiuntivi. |

Errori:

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

## UpdateSecurityProfile

Aggiorna un profilo di sicurezza di Device Defender.

Riepilogo:

```
aws iot update-security-profile \
--security-profile-name <value> \
[--security-profile-description <value>] \
[--behaviors <value>] \
[--alert-targets <value>] \
[--additional-metrics-to-retain <value>] \
[--delete-behaviors | --no-delete-behaviors] \
[--delete-alert-targets | --no-delete-alert-targets] \
[--delete-additional-metrics-to-retain | --no-delete-additional-metrics-to-retain] \
[--expected-version <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`:

```
{
 "securityProfileName": "string",
 "securityProfileDescription": "string",
 "behaviors": [
 {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 }
 }
 }
]
},
```

```

 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "statistic": "string"
 }
 }
],
"alertTargets": {
 "string": {
 "alertTargetArn": "string",
 "roleArn": "string"
 }
},
"additionalMetricsToRetain": [
 "string"
],
"deleteBehaviors": "boolean",
"deleteAlertTargets": "boolean",
"deleteAdditionalMetricsToRetain": "boolean",
"expectedVersion": "long"
}
}

```

Campi di **cli-input-json**:

| Nome                       | Tipo                                                                  | Descrizione                                                                                                     |
|----------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| securityProfileName        | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del profilo di sicurezza da aggiornare.                                                                    |
| securityProfileDescription | Stringa<br>Lunghezza max: 1000<br>Modello: [\p{Graph}]*               | Descrizione del profilo di sicurezza.                                                                           |
| behaviors                  | elenco<br>membro: Behavior                                            | Specifica i comportamenti che, quando violati da un dispositivo (oggetto), causano la generazione di un avviso. |
| name                       | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome assegnato al comportamento.                                                                                |
| metric                     | Stringa                                                               | Valore misurato dal comportamento.                                                                              |
| criteria                   | BehaviorCriteria                                                      | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a metric.              |
| comparisonOperator         | Stringa                                                               | Operatore che mette in correlazione l'oggetto misurato (metric) e i criteri                                     |

| Nome                         | Tipo                                     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              |                                          | (contenenti un <code>value</code> o <code>statisticalThreshold</code> ).<br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set                                                                                                                                                                                                                                                                                                                                                           |
| value                        | MetricValue                              | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count                        | Long<br>Intervallo - min.: 0             | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cidrs                        | elenco<br>membro: Cidr                   | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports                        | elenco<br>membro: Port                   | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds              | integer                                  | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |
| consecutiveDatapointsToAlarm | integer<br>Intervallo – Max: 10, min.: 1 | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                      |

| Nome                         | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| consecutiveDatapointsToClear | integer<br><br>Intervallo – Max: 10, min.: 1                                 | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                |
| statisticalThreshold         | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| statistic                    | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato (durationSeconds) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto (comparisonOperator) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario si verifica una violazione. |
| alertTargets                 | mappa                                                                        | Destinazione di invio degli avvisi. Gli avvisi vengono sempre inviati alla console.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| alertTargetArn               | Stringa                                                                      | ARN del target di notifica a cui vengono inviati gli avvisi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| roleArn                      | Stringa<br><br>Lunghezza max: 2048, min.: 20                                 | ARN del ruolo che concede l'autorizzazione per l'invio degli avvisi al target di notifica.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Nome                            | Tipo                             | Descrizione                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| additionalMetricsToRetain       | elenco<br>membro: BehaviorMetric | Un elenco di parametri i cui dati vengono conservati (archiviati). Per impostazione predefinita, i dati vengono conservati per qualsiasi parametro utilizzato nel behaviors del profilo ma vengono anche conservati per qualsiasi parametro specificato qui. |
| deleteBehaviors                 | booleano                         | Se true, elimina tutti i behaviors definiti per questo profilo di sicurezza. Se esistono behaviors definiti nell'invocazione corrente, si verifica un'eccezione.                                                                                             |
| deleteAlertTargets              | booleano                         | Se true, elimina tutti i alertTargets definiti per questo profilo di sicurezza. Se esistono alertTargets definiti nell'invocazione corrente, si verifica un'eccezione.                                                                                       |
| deleteAdditionalMetricsToRetain | booleano                         | Se true, elimina tutti i additionalMetricsToRetain definiti per questo profilo di sicurezza. Se esistono additionalMetricsToRetain definiti nell'invocazione corrente, si verifica un'eccezione.                                                             |
| expectedVersion                 | Long                             | Versione prevista del profilo di sicurezza. Viene generata una nuova versione ogni volta che il profilo di sicurezza viene aggiornato. Se specifichi un valore diverso dalla versione effettiva, viene generata un'eccezione VersionConflictException.       |

Output:

```
{
 "securityProfileName": "string",
 "securityProfileArn": "string",
 "securityProfileDescription": "string",
 "behaviors": [
 {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "unit": "string"
 }
 }
 }
]
}
```

```

 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
},
"durationSeconds": "integer",
"consecutiveDatapointsToAlarm": "integer",
"consecutiveDatapointsToClear": "integer",
"statisticalThreshold": {
 "statistic": "string"
}
}
],
"alertTargets": {
 "string": {
 "alertTargetArn": "string",
 "roleArn": "string"
 }
},
"additionalMetricsToRetain": [
 "string"
],
"version": "long",
"creationDate": "timestamp",
"lastModifiedDate": "timestamp"
}
}

```

Campi di output dell'interfaccia a riga di comando:

| Nome                       | Tipo                                                               | Descrizione                                                                                                     |
|----------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| securityProfileName        | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-zA-Z0-9:_-]+ | Nome del profilo di sicurezza aggiornato.                                                                       |
| securityProfileArn         | Stringa                                                            | ARN del profilo di sicurezza aggiornato.                                                                        |
| securityProfileDescription | Stringa<br>Lunghezza max: 1000<br>Modello: [\p{Graph}]*            | Descrizione del profilo di sicurezza.                                                                           |
| behaviors                  | elenco<br>membro: Behavior                                         | Specifica i comportamenti che, quando violati da un dispositivo (oggetto), causano la generazione di un avviso. |
| name                       | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-zA-Z0-9:_-]+ | Nome assegnato al comportamento.                                                                                |
| metric                     | Stringa                                                            | Valore misurato dal comportamento.                                                                              |

| Nome               | Tipo                             | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| criteria           | BehaviorCriteria                 | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| comparisonOperator | Stringa                          | Operatore che mette in correlazione l'oggetto misurato ( <code>metric</code> ) e i criteri (contenenti un <code>value</code> o <code>statisticalThreshold</code> ).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set                                                                                                                                                                                                                                                            |
| value              | MetricValue                      | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count              | Long<br><br>Intervallo - min.: 0 | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cidrs              | elenco<br><br>membro: Cidr       | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports              | elenco<br><br>membro: Port       | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds    | integer                          | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |

| Nome                         | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| consecutiveDatapointsToAlarm | integer<br><br>Intervallo – Max: 10, min.: 1                                 | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| consecutiveDatapointsToClear | integer<br><br>Intervallo – Max: 10, min.: 1                                 | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| statisticalThreshold         | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| statistic                    | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato ( <code>durationSeconds</code> ) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto ( <code>comparisonOperator</code> ) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento. In caso contrario, si verifica una violazione. |
| alertTargets                 | mappa                                                                        | Destinazione di invio degli avvisi. Gli avvisi vengono sempre inviati alla console.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| alertTargetArn               | Stringa                                                                      | ARN del target di notifica a cui vengono inviati gli avvisi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Nome                      | Tipo                                     | Descrizione                                                                                                                                                                                                                                                               |
|---------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn                   | Stringa<br>Lunghezza max: 2048, min.: 20 | ARN del ruolo che concede l'autorizzazione per l'invio degli avvisi al target di notifica.                                                                                                                                                                                |
| additionalMetricsToRetain | elenco<br>membro: BehaviorMetric         | Un elenco di parametri i cui dati vengono conservati (archiviati). Per impostazione predefinita, i dati vengono conservati per qualsiasi parametro utilizzato nei behaviors del profilo di sicurezza ma vengono anche conservati per qualsiasi parametro specificato qui. |
| Versione                  | Long                                     | Versione aggiornata del profilo di sicurezza.                                                                                                                                                                                                                             |
| creationDate              | timestamp                                | Ora della creazione del profilo di sicurezza.                                                                                                                                                                                                                             |
| lastModifiedDate          | timestamp                                | Ora dell'ultima modifica del profilo di sicurezza.                                                                                                                                                                                                                        |

Errori:

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**VersionConflictException**

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro `--version`.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## ValidateSecurityProfileBehaviors

Convalida la specifica dei comportamenti dei profili di sicurezza di Device Defender.

Riepilogo:

```
aws iot validate-security-profile-behaviors \
--behaviors <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`:

```
{
 "behaviors": [
 {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 },
 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "statistic": "string"
 }
 }
 }
]
}
```

**Campi di `cli-input-json`:**

| Nome               | Tipo                                                                          | Descrizione                                                                                                                                                                                                                                                                                                                |
|--------------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| behaviors          | elenco<br>membro: Behavior                                                    | Specifica i comportamenti che, quando violati da un dispositivo (oggetto), causano la generazione di un avviso.                                                                                                                                                                                                            |
| name               | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome assegnato al comportamento.                                                                                                                                                                                                                                                                                           |
| metric             | Stringa                                                                       | Valore misurato dal comportamento.                                                                                                                                                                                                                                                                                         |
| criteria           | BehaviorCriteria                                                              | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a <code>metric</code> .                                                                                                                                                                                                           |
| comparisonOperator | Stringa                                                                       | Operatore che mette in correlazione l'oggetto misurato ( <code>metric</code> ) e i criteri (contenenti un <code>value</code> o <code>statisticalThreshold</code> ).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set |

| Nome                         | Tipo                                     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| value                        | MetricValue                              | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count                        | Long<br>Intervallo - min.: 0             | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cidrs                        | elenco<br>membro: Cidr                   | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports                        | elenco<br>membro: Port                   | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds              | integer                                  | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |
| consecutiveDatapointsToAlarm | integer<br>Intervallo – Max: 10, min.: 1 | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                      |
| consecutiveDatapointsToClear | integer<br>Intervallo – Max: 10, min.: 1 | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                   |

| Nome                 | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| statisticalThreshold | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| statistic            | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato (durationSeconds) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto (comparisonOperator) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento. In caso contrario, si verifica una violazione. |

Output:

```
{
 "valid": "boolean",
 "validationErrors": [
 {
 "errorMessage": "string"
 }
]
}
```

Campi di output dell'interfaccia a riga di comando:

| Nome             | Tipo                                  | Descrizione                                         |
|------------------|---------------------------------------|-----------------------------------------------------|
| valid            | booleano                              | True se i comportamenti sono validi.                |
| validationErrors | elenco<br><br>membro: ValidationError | Elenco degli errori trovati nei comportamenti.      |
| errorMessage     | Stringa                               | Descrizione di un errore trovato nei comportamenti. |

| Nome | Tipo                | Descrizione |
|------|---------------------|-------------|
|      | Lunghezza max: 2048 |             |

Errori:

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## Integrazione dell'agente dei dispositivi con AWS IoT Greengrass

AWS IoT Device Defender può essere utilizzato in combinazione con AWS IoT Greengrass. L'integrazione dell'agente dei dispositivi segue il modello di distribuzione standard della funzione Lambda AWS IoT Greengrass, per permettere di aggiungere la sicurezza di AWS IoT Device Defender ai dispositivi core AWS IoT Greengrass. Per integrare un agente dei dispositivi, segui le fasi descritte in questa sezione.

Prerequisiti:

- Configurazione dell'ambiente AWS IoT Greengrass
- Configurare ed eseguire il tuo core AWS IoT Greengrass.
- Verifica di poter distribuire ed eseguire correttamente una funzione Lambda nel core AWS IoT Greengrass.

In generale, il processo descritto qui segue la sezione relativa a [creazione di una funzione Lambda e inserimento in un pacchetto](#) della guida per sviluppatori di AWS IoT Greengrass.

### Creazione di un pacchetto Lambda

1. Clonare il repository di esempi Python per AWS IoT Device Defender.

```
git clone https://github.com/aws-samples/aws-iot-device-defender-agent-sdk-python.git
```

2. Creare e attivare un ambiente virtuale (opzionale ma consigliato).

```
pip install virtualenv
virtualenv metrics_lambda_environment
source metrics_lambda_environment/bin/activate
```

3. Installare l'agente di esempio AWS IoT Device Defender nell'ambiente virtuale. Installare da PyPi.

```
pip install AWSIoTDeviceDefenderAgentSDK
```

4. Installare l'origine scaricata.

```
cd aws-iot-device-defender-agent-sdk-python
#This must be run from the same directory as setup.py
pip install .
```

5. Creare una directory vuota per assemblare la funzione Lambda. Questa è la tua directory Lambda.

```
mkdir metrics_lambda
cd metrics_lambda
```

6. Completare i passaggi 1-4 in [creazione di una funzione Lambda e inserimento in un pacchetto](#).
7. Decomprimere il Python SDK AWS IoT Greengrass nella directory Lambda.

```
unzip ../aws_greengrass_core_sdk/sdk/python_sdk_1_1_0.zip
cp -R ../aws_greengrass_core_sdk/examples/HelloWorld/greengrass_common .
cp -R ../aws_greengrass_core_sdk/examples/HelloWorld/greengrassdk .
cp -R ../aws_greengrass_core_sdk/examples/HelloWorld/greengrass_ipc_python_sdk .
```

8. Copiare il modulo AWSIoTDeviceDefenderAgentSDK al livello root della directory Lambda.

```
cp -R ../aws-iot-device-defender-agent-sdk-python/AWSIoTDeviceDefenderAgentSDK .
```

9. Copiare l'agente AWS IoT Greengrass al livello root della directory Lambda.

```
cp ../aws-iot-device-defender-agent-sdk-python/samples/greengrass/
greengrass_core_metrics_agent/greengrass_defender_agent.py .
```

10. Personalizza l'agente AWS IoT Greengrass per includere il nome del dispositivo core AWS IoT Greengrass e il tasso di esempio dei parametri desiderati:

- Sostituisci GREENGASS\_CORENAME con il nome della tua funzione core AWS IoT Greengrass.
- Impostare SAMPLE\_RATE\_SECONDS sull'intervallo desiderato per la segnalazione dei parametri. 5 minuti (300 secondi) è l'intervallo di segnalazione più breve supportato da AWS IoT Device Defender.

11. Copiare le dipendenze dall'ambiente virtuale (o dal sistema) nel livello root della directory Lambda.

```
cp -R ../metrics_lambda_environment/lib/python2.7/site-packages/psutil .
cp -R ../metrics_lambda_environment/lib/python2.7/site-packages/cbor .
```

12. Creare il file ZIP della funzione Lambda. È necessario eseguire questo comando al livello root della directory Lambda.

```
rm *.zip
zip -r greengrass_defender_metrics_lambda.zip *
```

## Configurazione e distribuzione della funzione Lambda AWS IoT Greengrass

1. [Caricare il file ZIP Lambda](#).
2. Selezionare il runtime Python 2.7 e immettere `greengrass_defender_agent.function_handler` nel campo Handler.
3. [Configurare la funzione Lambda di lunga durata come una funzione Lambda](#).
4. [Configurare una sottoscrizione dalla funzione Lambda al cloud AWS IoT](#). Per AWS IoT Device Defender, non è richiesto un abbonamento dal cloud AWS IoT alla funzione Lambda.
5. Creare una risorsa locale per permettere alla funzione Lambda di raccogliere i parametri dall'host core AWS IoT Greengrass:

- Segui le istruzioni in [Accedi alle risorse locali con le funzioni Lambda](#). Utilizzare i seguenti parametri:
  - Nome risorsa: `Core_Proc`
  - Tipo: `Volume`
  - Percorso di origine: `/proc`
  - Percorso di destinazione: `/host_proc`
  - Autorizzazione di accesso ai file per il proprietario del gruppo "Aggiungi automaticamente le autorizzazioni del gruppo OS del gruppo Linux che possiede la risorsa"
  - Associare la risorsa alla funzione Lambda dei parametri.
- 6. Distribuire la funzione Lambda per il tuo gruppo AWS IoT Greengrass.

Analisi dei parametri dei dispositivi di AWS IoT Device Defender tramite la console AWS IoT

1. Modificare temporaneamente l'argomento di pubblicazione nella funzione Lambda AWS IoT Greengrass in "metrics/test".
2. Distribuire la funzione Lambda.
3. Per visualizzare i parametri che AWS IoT Greengrass core sta trasmettendo, nella pagina di prova della console AWS IoT, aggiungere una sottoscrizione all'argomento temporaneo ("metrics/test").

## Best practice per la sicurezza degli agenti dei dispositivi

### Privilegio minimo

Al processo dell'agente devono venire concesse solo le autorizzazioni minime necessarie.

### Meccanismi di base

- L'agente deve essere eseguito come utente non root.
- L'agente deve essere eseguito come utente dedicato, nel proprio gruppo.
- A utenti e gruppi devono essere concesse le autorizzazioni di sola lettura sulle risorse necessarie per raccogliere e trasmettere i parametri.
- Esempio: autorizzazione di sola lettura in `/proc /sys` per l'agente di esempio.
- Per un esempio di configurazione di un processo per l'esecuzione con autorizzazioni ridotte, consulta le istruzioni di configurazione incluse con l'agente di esempio Python.

Sono disponibili diversi meccanismi Linux noti che possono aiutare a limitare/isolare ulteriormente il processo dell'agente:

### Meccanismi avanzati

- [CGroups](#)
- [SELinux](#)
- [Chroot](#)
- [Spazi dei nomi Linux](#)

### Resilienza operativa

Il processo di un agente deve essere resiliente alle eccezioni e agli errori operativi imprevisti e non deve arrestarsi in modo anomalo o chiudersi definitivamente. Il codice deve gestire nel modo

appropriato le eccezioni e, come precauzione, deve essere configurato per il riavvio automatico in caso di interruzione imprevista (ad esempio, a causa del riavvio del sistema o di eccezioni non intercettate).

#### Dipendenze minime

Un agente deve usare il minor numero possibile di dipendenze (ad esempio librerie di terze parti) nella sua implementazione. Se l'uso di una libreria è giustificato dalla complessità di un'attività (ad esempio, Transport Layer Security), usa solo dipendenze ben gestite e stabilisci un meccanismo per mantenerle aggiornate. Se le dipendenze aggiunte contengono funzionalità non usate dall'agente e attive per impostazione predefinita (ad esempio l'apertura di porte o i socket di dominio), disabilitale nel codice o attraverso i file di configurazione della libreria.

#### Isolamento dei processi

Il processo di un agente deve contenere solo le funzionalità necessarie per raccogliere e trasmettere i parametri dei dispositivi. Non deve usare altri processi di sistema come contenitore o implementare funzionalità per altri casi d'uso non previsti. Il processo dell'agente non deve inoltre creare canali di comunicazione in entrata, ad esempio socket di dominio e porte di servizio di rete, che potrebbero permettere a processi locali o remoti di interferire con il funzionamento e influire sull'integrità e sull'isolamento.

#### Segretezza

Il nome del processo di un agente non deve contenere parole chiave come sicurezza, monitoraggio o audit che ne indicano lo scopo e l'importanza per la sicurezza. È preferibile usare nomi in codice generici o nomi di processi casuali univoci per ogni dispositivo. Lo stesso principio deve essere seguito nell'assegnazione del nome della directory in cui si trovano i file binari dell'agente e di eventuali nomi e valori degli argomenti del processo.

#### Condivisione di informazioni minime

Qualsiasi elemento di un agente distribuito nei dispositivi non deve contenere informazioni sensibili, ad esempio credenziali con privilegi, codice di debug o codice non utilizzato oppure commenti in linea o file di documentazione che rivelino dettagli sull'elaborazione lato server dei parametri raccolti dall'agente o altri dettagli sui sistemi back-end.

#### Transport Layer Security

Per stabilire canali TLS sicuri per la trasmissione dei dati, un processo dell'agente deve applicare tutte le convalide lato client, ad esempio la convalida della catena di certificati e del nome di dominio, a livello di applicazione, se questa opzione non è abilitata per impostazione predefinita. Un agente deve inoltre usare un archivio di certificati root contenente autorità attendibili e che non contiene certificati appartenenti a emittenti di certificati compromessi.

#### Distribuzione sicura

Tutti i meccanismi di distribuzione dell'agente, ad esempio la sincronizzazione o il push di codice e i repository contenenti i dati binari, il codice sorgente e i file di configurazione (inclusi i certificati root attendibili), devono essere controllati per impedire l'inserimento di codice non autorizzato o la manomissione. Se il meccanismo di distribuzione si basa sulla comunicazione di rete, è necessario usare metodi di crittografia per proteggere l'integrità degli elementi di distribuzione in transito.

#### Approfondimenti

- [Sicurezza e identità per AWS IoT](#)
- [Informazioni sul modello di sicurezza di AWS IoT](#)
- [Redhat: presentazione di Python](#)
- [10 problemi di sicurezza comuni in Python e come evitarli](#)
- [Informazioni sui privilegi minimi e sulla loro utilità](#)
- [10 indicazioni sulla sicurezza integrata di OWASP](#)
- [Progetto IoT OWASP](#)

# Risoluzione dei problemi di AWS IoT Device Defender

## Generali

D: Sono previsti prerequisiti per l'uso di AWS IoT Device Defender?

R: se si desidera utilizzare parametri riportati sul dispositivo, è necessario distribuire un agente sul dispositivo o il gateway di dispositivi AWS IoT connessi. I dispositivi devono fornire un identificatore client coerente o un nome dell'oggetto.

## Audit

D: Ho abilitato un controllo e lo stato dell'audit è rimasto "In corso" per molto tempo. C'è qualcosa che non funziona? Quando posso aspettarmi i risultati?

R: Quando un controllo viene abilitato, la raccolta dei dati inizia immediatamente. Tuttavia, se il tuo account ha una grande quantità di dati da raccogliere (certificati, oggetti, policy e così via), i risultati del controllo potrebbero non essere disponibili per un po' di tempo dopo l'attivazione.

## Rilevamento

D: Come faccio a sapere le soglie da impostare in un comportamento del profilo di sicurezza AWS IoT Device Defender?

R: Inizia creando un comportamento del profilo di sicurezza con soglie basse e collegalo a un gruppo di oggetti che contiene un set di dispositivi rappresentativo. È possibile utilizzare AWS IoT Device Defender per visualizzare i parametri correnti e quindi modificare le soglie del comportamento del dispositivo per ottenere la corrispondenza al tuo caso d'uso.

D: Ho creato un comportamento, ma non attiva una violazione quando previsto. Come posso risolvere il problema?

R: Quando si definisce un comportamento, si specifica in cosa consista un comportamento normale da parte del dispositivo. Se, ad esempio, hai una telecamera di sicurezza che si connette solo a un server centrale sulla porta TCP 8888, non è previsto che vengano stabilite altre connessioni. Per ricevere un avviso se la telecamera stabilisce una connessione su un'altra porta, puoi definire un comportamento, ad esempio:

```
{
 "name": "Listening TCP Ports",
 "metric": "aws:listening-tcp-ports",
 "criteria": {
 "comparisonOperator": "in-port-set",
 "value": {
 "ports": [8888]
 }
 }
}
```

Se la fotocamera invia una connessione TCP sulla porta TCP 443, il comportamento del dispositivo viene violato e viene attivato un avviso.

D: Uno o più dei comportamenti hanno provocato una violazione. Come posso cancellare la violazione?

R: Gli allarmi si disattivano quando il dispositivo torna al comportamento previsto, secondo quanto definito nei profili di comportamento. I profili di comportamento vengono valutati al momento della ricezione dei dati dei parametri per il dispositivo.

D: Ho eliminato un comportamento che provocava una violazione, come posso interrompere gli avvisi?

R: L'eliminazione di un comportamento interrompe tutte le violazioni future e gli avvisi relativi a tale comportamento. Gli avvisi precedenti devono essere eliminati dal tuo meccanismo di notifica. Quando, tuttavia, un comportamento viene eliminato, la registrazione delle violazioni per tale comportamento viene conservata per lo stesso periodo di tempo applicato ad altre violazioni nell'account.

#### Parametri dei dispositivi

D: Sto inviando segnalazioni di parametri che so che violano i miei comportamenti, ma non vengono attivate violazioni. Qual è il problema?

R: Controlla le segnalazioni di parametri vengano accettate sottoscrivendo gli argomenti MQTT seguenti:

```
$aws/things/THING_NAME/defender/metrics/FORMAT/rejected
$aws/things/THING_NAME/defender/metrics/FORMAT/accepted
```

dove **THING\_NAME** è il nome dell'oggetto che segnala il parametro e **FORMAT** è "json" o "cbor", a seconda del formato della segnalazione di parametri inviata dall'oggetto.

Dopo aver eseguito la sottoscrizione, dovresti ricevere messaggi su questi argomenti per ogni segnalazione di parametri inviata. Un messaggio **rejected** indica che si è verificato un problema durante l'analisi della segnalazione di parametri. Nel payload del messaggio è incluso un messaggio di errore utile per correggere eventuali errori nella segnalazione di parametri. Un messaggio **accepted** indica che la segnalazione di parametri è stata analizzata correttamente.

D: Cosa succede se invio un parametro vuoto nella segnalazione?

R: Un elenco vuoto di porte o indirizzi IP è sempre considerato conforme al comportamento corrispondente. Se il comportamento corrispondente risultava violato, la violazione verrà cancellata.

D: Perché i miei report sui parametri del dispositivo contengono messaggi per i dispositivi che non sono nel registro AWS IoT?

Se disponi di uno o più profili di sicurezza associati a tutti gli oggetti o a tutti gli oggetti non registrati, AWS IoT Device Defender include i parametri degli oggetti non registrati. Se si desidera escludere i parametri dagli oggetti non registrati, è possibile allegare i profili a tutti i dispositivi registrati invece che a tutti i dispositivi.

D: Non riesco a visualizzare i messaggi provenienti da uno o più dispositivi non registrati anche se viene applicato un profilo di sicurezza a tutti i dispositivi non registrati o a tutti i dispositivi. Come posso risolvere il problema?

Verificare che si stia inviando un report di parametri ben formati utilizzando uno dei formati supportati. Per ulteriori informazioni, consulta [Specifica del documento di parametri dei dispositivi \(p. 576\)](#). Verificare che i dispositivi non registrati utilizzino un identificatore client coerente o un nome oggetto. I messaggi riportati dai dispositivi sono rifiutati se il nome dell'oggetto contiene caratteri di controllo oppure se il nome dell'oggetto è più lungo di 128 byte di caratteri di codifica UTF-8.

D: Cosa succede se un dispositivo non registrato viene aggiunto al registro o un dispositivo registrato diventa non registrato?

R: Se un dispositivo viene aggiunto o rimosso dal registro:

- L'API `ListMetricValues` restituisce i parametri pubblicati per il `thingName` specificato (nessuna modifica di comportamento).
- Puoi vedere due diverse violazioni per il dispositivo (una sotto il suo nome oggetto registrato, una sotto la propria identità non registrata), se continuerà a pubblicare i parametri per violazioni. Le violazioni attive per la vecchia identità non vengono più visualizzate dopo due giorni, ma sono disponibili nello storico delle violazioni per un massimo di 14 giorni.

D: Quale valore devo fornire nel campo ID della segnalazione dei parametri di un dispositivo?

R: Devi usare un valore univoco per ogni segnalazione di parametri, espresso come valore intero positivo. In genere è consigliabile usare un [timestamp di epoca \(Unix epoch\)](#).

D: È consigliabile creare una connessione MQTT dedicata per i parametri di AWS IoT Device Defender?

R: Non è necessaria una connessione MQTT separata.

D: Quale ID client devo usare per la connessione per la pubblicazione di parametri del dispositivo?

Per i dispositivi (oggetti) che si trovano nel registro AWS IoT, utilizzare il nome dell'oggetto registrato.

Per i dispositivi che non sono presenti nel registro AWS IoT, utilizzare un identificatore coerente durante la connessione a AWS IoT. Questa pratica consente di abbinare le violazioni al nome dell'oggetto.

D: È possibile pubblicare parametri per un dispositivo con un ID client diverso?

È possibile pubblicare i parametri per conto di un altro oggetto. A tale scopo, è possibile pubblicare i parametri per l'argomento AWS IoT Device Defender riservato per quel dispositivo. Ad esempio, **Thing-1** vorrebbe pubblicare i parametri per sé e anche per conto di **Thing-2**. **Thing-1** raccoglie i propri parametri e li pubblica sull'argomento MQTT:

```
$aws/things/Thing-1/defender/metrics/json
```

**Thing-1** quindi ottiene i parametri da **Thing-2** e pubblica tali parametri nell'argomento MQTT:

```
$aws/things/Thing-2/defender/metrics/json
```

D: Quanti profili di sicurezza e comportamenti possono essere presenti nell'account?

R: Consulta la sezione Detect [Restrizioni dei servizi \(p. 575\)](#) della guida per sviluppatori di AWS IoT Device Defender.

D: Cos'è un ruolo target prototipo per un target di avvisi?

R: Un ruolo che permette a AWS IoT Device Defender di pubblicare avvisi nel target (argomento SNS) richiede 2 elementi:

- Una relazione di trust che specifica `iot.amazonaws.com` come entità attendibile e
- Una policy collegata per la concessione dell'autorizzazione AWS IoT per pubblicare su un argomento SNS specifico. Ad esempio:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "sns:Publish",
 "Resource": "<sns-topic-arn>"
 }
]
}
```

# Messaggi di eventi

## Note

In questa sezione sono disponibili informazioni sui messaggi pubblicati da AWS IoT quando gli oggetti o i processi vengono aggiornati o modificati. Per informazioni sul servizio AWS IoT Events che consente di creare rilevatori per monitorare la presenza di guasti nei dispositivi o di variazioni del funzionamento e di attivare operazioni specifiche quando questi eventi si verificano, consulta la panoramica sul servizio [AWS IoT Events](#).

AWS IoT pubblica messaggi di evento quando si verificano determinati eventi. Ad esempio, vengono generati eventi dal registro quando vengono aggiunti, aggiornati o eliminati oggetti. Ogni evento comporta l'invio di un singolo messaggio di evento. I messaggi di evento vengono pubblicati tramite MQTT con un payload JSON. Il contenuto del payload dipende dal tipo di evento.

## Note

I messaggi di evento vengono sicuramente pubblicati una volta. È anche possibile che vengano pubblicati più di una volta. L'ordinamento dei messaggi di evento non è garantito.

Per ricevere messaggi di evento, il dispositivo deve usare una policy appropriata che gli permetta di connettersi al gateway dei dispositivi AWS IoT e di sottoscrivere argomenti di evento MQTT. Devi anche sottoscrivere i filtri di argomenti appropriati.

Di seguito viene mostrato un esempio della policy necessaria per la ricezione di eventi del ciclo di vita:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iot:Subscribe",
 "iot:Receive"
],
 "Resource": [
 "arn:aws:iot:region:account:/$aws/events/*"
]
 }
]
}
```

È possibile controllare quali tipi di evento devono essere pubblicati chiamando l'API [UpdateEventConfigurations](#) o usando il comando CLI update-event-configurations. Ad esempio:

```
aws iot update-event-configurations --event-configurations "{\"THING\":{\"Enabled\": true}}"
```

## Note

Tutte le virgolette doppie ("") sono precedute dal carattere di escape barra rovesciata (\).

È possibile ottenere la configurazione degli eventi corrente chiamando l'API [DescribeEventConfigurations](#) o mediante il comando CLI describe-event-configurations. Ad esempio:

```
aws iot describe-event-configurations
```

L'output del comando describe-event-configurations è simile al seguente:

```
{
 "lastModifiedDate": 1552671347.841,
 "eventConfigurations": {
```

```
"THING_TYPE": {
 "Enabled": false
},
"JOB_EXECUTION": {
 "Enabled": false
},
"THING_GROUP_HIERARCHY": {
 "Enabled": false
},
"CERTIFICATE": {
 "Enabled": false
},
"THING_TYPE_ASSOCIATION": {
 "Enabled": false
},
"THING_GROUP_MEMBERSHIP": {
 "Enabled": false
},
"CA_CERTIFICATE": {
 "Enabled": false
},
"THING": {
 "Enabled": true
},
"JOB": {
 "Enabled": false
},
"POLICY": {
 "Enabled": false
},
"THING_GROUP": {
 "Enabled": false
}
},
"creationDate": 1552671347.84
}
```

## Eventi del registro

Il registro pubblica messaggi di evento quando vengono creati, aggiornati o eliminati oggetti, tipi di oggetto e gruppi di oggetti. Attualmente il registro supporta i tipi di evento seguenti:

### Oggetto creato/aggiornato/eliminato

Il registro pubblica i messaggi di evento seguenti quando vengono creati, aggiornati o eliminati oggetti:

- \$aws/events/thing/<thingName>/created
- \$aws/events/thing/<thingName>/updated
- \$aws/events/thing/<thingName>/deleted

I messaggi contengono il payload di esempio seguente:

```
{
 "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"
}
```

I payload contengono gli attributi seguenti:  
eventType

Imposta su "THING\_EVENT".

eventId

ID evento univoco (stringa).

timestamp

Timestamp UNIX del momento in cui si è verificato l'evento.

operation

Operazione che ha attivato l'evento. I valori validi sono:

- CREATED
- UPDATED
- DELETED

accountId

ID dell'account AWS.

thingId

ID dell'oggetto creato, aggiornato o eliminato.

thingName

Nome dell'oggetto creato, aggiornato o eliminato.

versionNumber

Versione dell'oggetto creato, aggiornato o eliminato. Questo valore è impostato su 1 quando viene creato un oggetto. Il valore viene incrementato di 1 ogni volta che l'oggetto viene aggiornato.

thingTypeName

Tipo di oggetto associato all'oggetto, se ne esiste uno. In caso contrario, `null`.

attributes

Raccolta di coppie nome/valore associate all'oggetto.

Tipo di oggetto che è stato creato, dichiarato obsoleto/non più obsoleto o eliminato

Il registro pubblica i messaggi di evento seguenti quando vengono creati, aggiornati, dichiarati obsoleti/non più obsoleti o eliminati tipi di oggetto:

- \$aws/events/thingType/<thingTypeName>/created
- \$aws/events/thingType/<thingTypeName>/updated
- \$aws/events/thingType/<thingTypeName>/deleted

Il messaggio contiene il payload di esempio seguente:

```
{
 "eventType" : "THING_TYPE_EVENT",
 "eventId" : "8827376c-4b05-49a3-9b3b-733729df7ed5",
 "timestamp" : 1514764800000,
 "operation" : "CREATED",
 "accountId" : "12345678901234567890123456789012",
 "thingId" : "d1345678901234567890123456789012",
 "thingName" : "My Thing",
 "versionNumber" : 1,
 "thingTypeName" : "My Thing Type",
 "attributes" : {
 "attribute1": "value1",
 "attribute2": "value2",
 "attribute3": "value3"
 }
}
```

```
 "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"],
 "description" : "My thing type"
}
```

I payload contengono gli attributi seguenti:

eventType

Imposta su "THING\_TYPE\_EVENT".

eventId

ID evento univoco (stringa).

timestamp

Timestamp UNIX del momento in cui si è verificato l'evento.

operation

Operazione che ha attivato l'evento. I valori validi sono:

- CREATED
- UPDATED
- DELETED

accountId

ID dell'account AWS.

thingTypeId

ID del tipo di oggetto creato, dichiarato obsoleto o eliminato.

thingTypeName

Nome del tipo di oggetto creato, dichiarato obsoleto o eliminato.

isDeprecated

true se il tipo di oggetto è obsoleto. In caso contrario, false.

deprecationDate

Timestamp UNIX del momento in cui il tipo di oggetto è stato dichiarato obsoleto.

searchableAttributes

Raccolta di coppie nome/valore associate al tipo di oggetto che può essere usato per la ricerca.

description

Descrizione del tipo di oggetto.

Tipo di oggetto associato o dissociato rispetto a un oggetto

Il registro pubblica i messaggi di evento seguenti quando un tipo di oggetto viene associato o dissociato rispetto a un oggetto.

- \$aws/events/thingTypeAssociation/thing/<thingName>/<typeName>

I messaggi contengono il payload di esempio seguente:

```
{
```

```
 "eventId" : "87f8e095-531c-47b3-aab5-5171364d138d",
 "eventType" : "THING_TYPE_ASSOCIATION_EVENT",
 "operation" : "CREATED|DELETED",
 "thingId" : "b604f69c-aa9a-4d4a-829e-c480e958a0b5",
 "thingName": "myThing",
 "thingTypeName" : "MyThingType",
 "timestamp" : 1234567890123,
 }
```

I payload contengono gli attributi seguenti:  
eventId

ID evento univoco (stringa).

eventType

Imposta su "THING\_TYPE\_ASSOCIATION\_EVENT".

operation

Operazione che ha attivato l'evento. I valori validi sono:

- CREATED
- DELETED

thingId

L'ID dell'oggetto la cui associazione a un determinato tipo è stata modificata.

thingName

Il nome dell'oggetto la cui associazione a un determinato tipo è stata modificata.

thingTypeName

Il tipo di oggetto associato, o non più associato, con l'oggetto.

timestamp

Timestamp UNIX del momento in cui si è verificato l'evento.

Gruppo di oggetti creato/aggiornato/eliminato

Il registro pubblica i messaggi di evento seguenti quando viene creato, aggiornato o eliminato un gruppo di oggetti.

- \$aws/events/thingGroup/<groupName>/created
- \$aws/events/thingGroup/<groupName>/updated
- \$aws/events/thingGroup/<groupName>/deleted

I messaggi contengono il payload di esempio seguente:

```
{
 "eventType" : "THING_GROUP_EVENT",
 "eventId" : "87f8e095-531c-47b3-aab5-5171364d138d",
 "timestamp" : 1234567890123,
 "operation" : "CREATED|UPDATED|DELETED",
 "accountId" : "123456789012",
 "thingGroupId" : "8f82a106-6b1d-4331-8984-a84db5f6f8cb",
 "thingGroupName" : "MyRootThingGroup",
 "versionNumber" : 1,
 "parentGroupName" : null,
 "parentGroupId" : null,
 "description" : "My root thing group",
 "rootToParentThingGroups" : null,
 "attributes" : {
 "attribute1" : "value1",
```

```
 "attribute3" : "value3",
 "attribute2" : "value2"
 }
```

I payload contengono gli attributi seguenti:

**eventType**

Imposta su "THING\_GROUP\_EVENT".

**eventId**

ID evento univoco (stringa).

**timestamp**

Timestamp UNIX del momento in cui si è verificato l'evento.

**operation**

Operazione che ha attivato l'evento. I valori validi sono:

- CREATED
- UPDATED
- DELETED

**accountId**

ID dell'account AWS.

**thingGroupId**

ID del gruppo di oggetti creato, aggiornato o eliminato.

**thingGroupName**

Nome del gruppo di oggetti creato, aggiornato o eliminato.

**versionNumber**

Versione del gruppo di oggetti. Questo valore è impostato su 1 quando viene creato un gruppo di oggetti. Il valore viene incrementato di 1 ogni volta che il gruppo di oggetti viene aggiornato.

**parentGroupName**

Nome del gruppo di oggetti padre, se esistente.

**parentGroupId**

ID del gruppo di oggetti padre, se esistente.

**description**

Descrizione del gruppo di oggetti.

**rootToParentThingGroups**

Matrice di informazioni sul gruppo di oggetti padre. È presente una voce per ogni gruppo di oggetti padre, iniziando dal padre del gruppo di oggetti corrente e continuando fino a raggiungere il gruppo di oggetti root. Ogni voce contiene il nome del gruppo di oggetti e l'ARN del gruppo di oggetti.

**attributes**

Raccolta di coppie nome/valore associate al gruppo di oggetti.

Oggetto aggiunto o rimosso in un gruppo di oggetti

Il registro pubblica i messaggi di evento seguenti quando un oggetto viene aggiunto o rimosso in un gruppo di oggetti.

- \$aws/events/thingGroupMembership/thingGroup/<thingGroupName>/thing/<thingName>/added
- \$aws/events/thingGroupMembership/thingGroup/<thingGroupName>/thing/<thingName>/removed

I messaggi contengono il payload di esempio seguente:

```
{
 "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"
}
```

I payload contengono gli attributi seguenti:

eventType

Imposta su "THING\_GROUP\_MEMBERSHIP\_EVENT".

eventId

ID evento.

timestamp

Timestamp UNIX del momento in cui si è verificato l'evento.

operation

ADDED quando un oggetto viene aggiunto a un gruppo di oggetti. REMOVED quando un oggetto viene rimosso da un gruppo di oggetti.

accountId

ID dell'account AWS.

groupArn

ARN del gruppo di oggetti.

groupId

ID del gruppo.

thingArn

ARN dell'oggetto aggiunto o rimosso nel gruppo di oggetti.

thingId

ID dell'oggetto aggiunto o rimosso nel gruppo di oggetti.

membershipId

ID che rappresenta la relazione tra l'oggetto e il gruppo di oggetti. Questo valore viene generato quando aggiungi un oggetto a un gruppo di oggetti.

Gruppo di oggetti aggiunto o rimosso in un gruppo di oggetti

Il registro pubblica i messaggi di evento seguenti quando un gruppo di oggetti viene aggiunto o rimosso in un altro gruppo di oggetti.

- \$aws/events/thingGroupHierarchy/thingGroup/<*parentThingGroupName*>/childThingGroup/<*childThingGroupName*>/added
- \$aws/events/thingGroupHierarchy/thingGroup/<*parentThingGroupName*>/childThingGroup/<*childThingGroupName*>/removed

Il messaggio contiene il payload di esempio seguente:

```
{
 "eventType" : "THING_GROUP_HIERARCHY_EVENT",
 "eventId" : "264192c7-b573-46ef-ab7b-489fc47da41",
 "timestamp" : 1234567890123,
 "operation" : "ADDED|REMOVED",
 "accountId" : "123456789012",
 "thingGroupId" : "8f82a106-6b1d-4331-8984-a84db5f6f8cb",
 "thingGroupName" : "MyRootThingGroup",
 "childGroupId" : "06838589-373f-4312-b1f2-53f2192291c4",
 "childGroupName" : "MyChildThingGroup"
}
```

I payload contengono gli attributi seguenti:

eventType

Imposta su "THING\_GROUP\_HIERARCHY\_EVENT".

eventId

ID evento.

timestamp

Timestamp UNIX del momento in cui si è verificato l'evento.

operation

ADDED quando un oggetto viene aggiunto a un gruppo di oggetti. REMOVED quando un oggetto viene rimosso da un gruppo di oggetti.

accountId

ID dell'account AWS.

thingGroupId

ID del gruppo di oggetti padre.

thingGroupName

Nome del gruppo di oggetti padre.

childGroupId

ID del gruppo di oggetti figlio.

childGroupName

Nome del gruppo di oggetti figlio.

## Eventi del servizio Jobs

Il servizio Jobs pubblica in argomenti riservati nel protocollo MQTT quando i processi sono in sospeso o vengono completati o annullati e quando un dispositivo segnala un esito positivo o negativo per l'esecuzione di un processo. I dispositivi o le applicazioni di gestione e monitoraggio permettono di tenere traccia dello stato dei processi sottoscrivendo questi argomenti. È necessario utilizzare l'API [UpdateEventConfigurations](#) per controllare quali tipi di eventi di processo si ricevono.

Poiché l'eliminazione e l'annullamento di un processo potrebbero richiedere alcuni minuti, vengono inviati due messaggi per indicare l'inizio e la fine di una richiesta. Ad esempio, quando si avvia una richiesta di annullamento, viene inviato un messaggio all'argomento `$aws/events/job/jobID/cancellation_in_progress`. Quando la richiesta di annullamento è completa, viene inviato un messaggio all'argomento `$aws/events/job/jobID/canceled`. Lo stesso processo si verifica per una richiesta di eliminazione di un processo. Le applicazioni di gestione e monitoraggio permettono di tenere traccia dello stato dei processi sottoscrivendo questi argomenti.

Per ulteriori informazioni sulla pubblicazione e sulla sottoscrizione di argomenti MQTT, consulta [Broker di messaggi per AWS IoT \(p. 239\)](#).

#### Processo completato/annullato/eliminato

Il servizio AWS IoT Jobs pubblica un messaggio su un argomento MQTT quando un processo viene completato, annullato, eliminato o è in corso l'annullamento o l'eliminazione:

- `$aws/events/job/jobID/completed`
- `$aws/events/job/jobID/canceled`
- `$aws/events/job/jobID/deleted`
- `$aws/events/job/jobID/cancellation_in_progress`
- `$aws/events/job/jobID/deletion_in_progress`

Il messaggio `completed` contiene il payload di esempio seguente:

```
{
 "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
 }
}
```

Il messaggio `canceled` contiene il payload di esempio seguente:

```
{
 "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
}
```

Il messaggio `deleted` contiene il payload di esempio seguente:

```
{
 "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"
}
```

Il messaggio `cancellation_in_progress` contiene il payload di esempio seguente:

```
{
 "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"
}
```

Il messaggio `deletion_in_progress` contiene il payload di esempio seguente:

```
{
 "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"
}
```

```
"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"
}
```

### Stato terminale dell'esecuzione del processo

Il servizio AWS IoT Jobs pubblica un messaggio quando un dispositivo aggiorna l'esecuzione di un processo allo stato terminale:

- \$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

Il messaggio contiene il payload di esempio seguente:

```
{
 "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"
 }
}
```

## Eventi del ciclo di vita

AWS IoT pubblica eventi del ciclo di vita negli argomenti MQTT descritti nelle sezioni seguenti. Questi messaggi ti permettono di ricevere notifiche sugli eventi del ciclo di vita dal broker di messaggi.

### Note

È possibile che i messaggi del ciclo di vita non vengano inviati in ordine. Potresti anche ricevere messaggi duplicati.

## Eventi di connessione/disconnessione

AWS IoT pubblica un messaggio negli argomenti MQTT seguenti quando un client si connette o disconnette:

- \$aws/events/presence/connected/*clientId*: client connesso al broker di messaggi.
- \$aws/events/presence/disconnected/*clientId*: client disconnesso dal broker di messaggi.

Di seguito è riportato un elenco di elementi JSON contenuti nei messaggi di connessione/disconnessione pubblicati nell'argomento \$aws/events/presence/connected/*clientId*.

#### clientId

ID del client che si connette o si disconnette.

#### Note

Gli ID client che contengono # o + non ricevono eventi del ciclo di vita.

#### clientInitiatedDisconnect

Presente solo nei messaggi di disconnessione. True se il client ha avviato la disconnessione. In caso contrario, false.

#### eventType

Tipo di evento. I valori validi sono connected e disconnected.

#### principalIdentifier

Credenziale usata per l'autenticazione. Per i certificati di autenticazione reciproca TLS, si tratta dell'ID certificato. Per altre connessioni, si tratta delle credenziali IAM.

#### sessionIdentifier

Identificatore univoco globale in AWS IoT esistente per tutta la durata della sessione.

#### timestamp

Approssimazione del momento in cui si è verificato l'evento, espressa in millisecondi rispetto all'epoca (Unix epoch). La precisione del timestamp è di +/- 2 minuti.

#### versionNumber

Numero di versione per l'evento del ciclo di vita. Consiste nell'aumentare in maniera monotona un valore intero lungo per ogni connessione dell'ID client. Il numero di versione può essere utilizzato da un sottoscrittore per dedurre l'ordine degli eventi del ciclo di vita.

#### Note

I messaggi di connessione e disconnessione per una connessione client hanno lo stesso numero di versione.

Il numero di versione potrebbe ignorare valori e non è garantito che aumenti di 1 in modo costante per ogni evento.

Se un client non è connesso per circa un'ora, il numero di versione viene reimpostato su 0. Per le sessioni permanenti, il numero di versione viene reimpostato su 0 dopo che un client è stato disconnesso per un periodo più lungo del time-to-live (TTL) configurato per la sessione persistente.

## Gestione delle disconnessioni client

Secondo le best practice, occorre sempre avere uno stato di attesa implementato per gli eventi del ciclo di vita, inclusi i messaggi Last Will and Testament (LWT). Quando si riceve un messaggio di disconnessione, il codice deve attendere un periodo di tempo e verificare che un dispositivo è ancora offline prima di effettuare operazioni. A questo scopo, è possibile utilizzare [Code di ritardo Amazon SQS](#). Quando un client riceve un LWT o un evento del ciclo di vita, è possibile accodare un messaggio, ad esempio per 5 secondi. Quando il messaggio diventa disponibile e viene elaborato (da Lambda o da un altro servizio), è possibile controllare innanzitutto se il dispositivo è ancora realmente offline prima di effettuare ulteriori operazioni.

## Eventi di sottoscrizione/annullamento della sottoscrizione

AWS IoT pubblica un messaggio nell'argomento MQTT seguente quando un client sottoscrive un argomento MQTT o ne annulla la sottoscrizione:

```
$aws/events/subscriptions/subscribed/clientId
```

oppure

```
$aws/events/subscriptions/unsubscribed/clientId
```

Dove **clientId** è l'ID client MQTT che si connette al broker di messaggi AWS IoT.

Il messaggio pubblicato in questo argomento ha la struttura seguente:

```
{
 "clientId": "186b5",
 "timestamp": 1460065214626,
 "eventType": "subscribed" | "unsubscribed",
 "sessionIdentifier": "00000000-0000-0000-0000-000000000000",
 "principalIdentifier": "000000000000/ABCDEFGHIJKLMNPQRSTUVWXYZ:some-user/
ABCDEFGHIJKLMNPQRSTUVWXYZ:some-user"
 "topics" : ["foo/bar", "device/data", "dog/cat"]
}
```

Di seguito è riportato un elenco di elementi JSON contenuti nei messaggi di cui è stata eseguita o annullata la sottoscrizione pubblicati negli argomenti `$aws/events/subscriptions/subscribed/clientId` e `$aws/events/subscriptions/unsubscribed/clientId`.

**clientId**

ID del client che esegue la sottoscrizione o l'annullamento della sottoscrizione.

**Note**

Gli ID client che contengono # o + non ricevono eventi del ciclo di vita.

**eventType**

Tipo di evento. I valori validi sono `subscribed` e `unsubscribed`.

**principalIdentifier**

Credenziale usata per l'autenticazione. Per i certificati di autenticazione reciproca TLS, si tratta dell'ID certificato. Per altre connessioni, si tratta delle credenziali IAM.

**sessionIdentifier**

Identificatore univoco globale in AWS IoT esistente per tutta la durata della sessione.

**timestamp**

Approssimazione del momento in cui si è verificato l'evento, espressa in millisecondi rispetto all'epoca (Unix epoch). La precisione del timestamp è di +/- 2 minuti.

**topics**

Matrice degli argomenti MQTT sottoscritti dal client.

#### Note

È possibile che i messaggi del ciclo di vita non vengano inviati in ordine. Potresti anche ricevere messaggi duplicati.

# SDK AWS IoT

## Indice

- [SDK AWS Mobile per Android \(p. 641\)](#)
- [SDK Arduino Yún \(p. 641\)](#)
- [SDK di dispositivo AWS IoT per Embedded C \(p. 641\)](#)
- [SDK di dispositivo AWS IoT per C++ \(p. 642\)](#)
- [SDK AWS Mobile per iOS \(p. 642\)](#)
- [SDK di dispositivo AWS IoT per Java \(p. 642\)](#)
- [SDK di dispositivo AWS IoT per JavaScript \(p. 642\)](#)
- [SDK di dispositivo AWS IoT per Python \(p. 643\)](#)

Gli SDK (Software Development Kit) di dispositivo AWS IoT ti aiutano a connettere rapidamente e in tutta semplicità i dispositivi ad AWS IoT. Gli SDK di dispositivo AWS IoT includono librerie open source, guide per sviluppatori con esempi e guide alla portabilità, con cui puoi creare soluzioni o prodotti IoT innovativi sulle piattaforme hardware che preferisci.

## SDK AWS Mobile per Android

L'SDK AWS per Android contiene una libreria, esempi e documentazione per aiutare gli sviluppatori a creare applicazioni per dispositivi mobili connesse usando AWS. Questo SDK include anche il supporto per la chiamata delle API AWS IoT. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [SDK AWS Mobile per Android su GitHub](#)
- [File Readme dell'SDK AWS Mobile per Android](#)
- [Esempi relativi all'SDK AWS Mobile per Android](#)

## SDK Arduino Yún

L'SDK AWS IoT Arduino Yún permette agli sviluppatori di connettere le schede compatibili con Arduino Yún ad AWS IoT. Connnettendo un dispositivo ad AWS IoT, gli utenti possono lavorare in modo sicuro con il broker di messaggi, le regole e le copie shadow forniti da AWS IoT, oltre che con altri servizi AWS come AWS Lambda, Kinesis e Amazon S3. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [SDK Arduino Yún su GitHub](#)
- [File Readme dell'SDK Arduino Yún](#)

## SDK di dispositivo AWS IoT per Embedded C

L'SDK di dispositivo AWS IoT per Embedded C è una raccolta di file di origine C che è possibile utilizzare nelle applicazioni integrate per la connessione sicura alla piattaforma AWS IoT. Questo SDK include client di trasporto, implementazioni TLS ed esempi d'uso. Supporta inoltre caratteristiche specifiche di AWS IoT, ad esempio un'API per accedere al servizio Device Shadow. Viene distribuito come codice sorgente ed è

pensato per essere integrato nel firmware del cliente con il codice dell'applicazione, altre librerie e sistemi RTOS. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [SDK di dispositivo AWS IoT per Embedded C su GitHub](#)
- [File Readme dell'SDK di dispositivo AWS IoT per Embedded C](#)
- [Guida alla portabilità per l'SDK di dispositivo AWS IoT per Embedded C](#)

## SDK di dispositivo AWS IoT per C++

L'SDK di dispositivo AWS IoT per C++ permette agli sviluppatori di creare applicazioni connesse utilizzando AWS e le API AWS IoT. In particolare, questo SDK è stato progettato per i dispositivi che non hanno vincoli di risorse e che richiedono caratteristiche avanzate come l'accodamento dei messaggi, il supporto per il multithreading e le più recenti caratteristiche di linguaggio. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [SDK di dispositivo AWS IoT per C++ su GitHub](#)
- [File Readme dell'SDK di dispositivo AWS IoT per C++](#)

## SDK AWS Mobile per iOS

L'SDK AWS per iOS è un Software Development Kit open source distribuito con una licenza Apache Open Source. L'SDK per iOS fornisce una libreria, esempi di codice e documentazione che aiutano gli sviluppatori a creare applicazioni per dispositivi mobili connesse usando AWS. Questo SDK include anche il supporto per la chiamata dell'API AWS IoT.

- [SDK AWS per iOS su GitHub](#)
- [File Readme dell'SDK AWS per iOS](#)
- [Esempi relativi all'SDK AWS per iOS](#)

## SDK di dispositivo AWS IoT per Java

L'SDK di dispositivo AWS IoT per Java permette agli sviluppatori Java di accedere alla piattaforma AWS IoT tramite il protocollo MQTT o MQTT over WebSocket. L'SDK è sviluppato con il supporto delle copie shadow. È possibile accedere alle copie shadow tramite i metodi HTTP, tra cui GET, UPDATE e DELETE. L'SDK supporta anche un modello di accesso semplificato alle copie shadow, che permette agli sviluppatori di scambiare i dati con le copie shadow semplicemente usando i metodi getter e setter, senza dover serializzare o deserializzare documenti JSON. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [SDK di dispositivo AWS IoT per Java su GitHub](#)
- [File Readme dell'SDK di dispositivo AWS IoT per Java](#)

## SDK di dispositivo AWS IoT per JavaScript

Il pacchetto aws-iot-device-sdk.js permette agli sviluppatori di scrivere applicazioni JavaScript che accedono ad AWS IoT utilizzando il protocollo MQTT o MQTT over WebSocket. Questo SDK può essere usato nelle applicazioni di tipo browser e negli ambienti Node.js. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [SDK di dispositivo AWS IoT per JavaScript su GitHub](#)

- [File Readme dell'SDK di dispositivo AWS IoT per JavaScript](#)

## SDK di dispositivo AWS IoT per Python

L'SDK di dispositivo AWS IoT per Python permette agli sviluppatori di scrivere script Python per usare i dispositivi per l'accesso alla piattaforma AWS IoT tramite il protocollo MQTT o MQTT over WebSocket. Connnettendo i propri dispositivi ad AWS IoT, gli utenti possono lavorare in modo sicuro con il broker di messaggi, le regole e le copie shadow forniti da AWS IoT, oltre che con altri servizi AWS come AWS Lambda, Kinesis, Amazon S3 e altri.

- [SDK di dispositivo AWS IoT per Python su GitHub](#)
- [File Readme dell'SDK di dispositivo AWS IoT per Python](#)

# Monitoraggio AWS IoT

Il monitoraggio è importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS IoT e delle soluzioni AWS. Devi raccogliere i dati sul monitoraggio da tutte le parti della soluzione AWS per permettere un debug più facile di eventuali guasti in più punti. Prima di iniziare il monitoraggio di AWS IoT, è opportuno creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Quali risorse verranno monitorate?
- Con quale frequenza eseguirai il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno usati?
- Chi eseguirà le attività di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

La fase successiva consiste nello stabilire una baseline per le prestazioni normali di AWS IoT nell'ambiente, misurando le prestazioni in diversi momenti e con condizioni di carico differenti. Quando monitori AWS IoT, archivia i dati di monitoraggio storici per poterli confrontare con i dati sulle prestazioni correnti e per poter identificare i normali modelli di prestazioni e le anomalie e ideare metodi per risolvere i problemi.

Se, ad esempio, usi Amazon EC2, puoi monitorare utilizzo della CPU, I/O su disco e utilizzo della rete per le istanze. Quando le prestazioni non rientrano nella baseline stabilita, può essere necessario riconfigurare o ottimizzare l'istanza per ridurre l'utilizzo della CPU, migliorare l'I/O su disco o ridurre il traffico di rete.

Per stabilire una baseline, devi monitorare almeno gli elementi seguenti:

- PublishIn.Success
- PublishOut.Success
- Subscribe.Success
- Ping.Success
- Connect.Success
- GetThingShadow.Accepted
- UpdateThingShadow.Accepted
- DeleteThingShadow.Accepted
- RulesExecuted

## Argomenti

- [Strumenti di monitoraggio \(p. 644\)](#)
- [Monitoraggio con Amazon CloudWatch \(p. 646\)](#)
- [Monitoraggio con CloudWatch Logs \(p. 655\)](#)
- [Registrazione delle chiamate API AWS IoT con AWS CloudTrail \(p. 676\)](#)

## Strumenti di monitoraggio

AWS offre strumenti che puoi utilizzare per monitorare AWS IoT. Alcuni di questi strumenti possono essere configurati per il monitoraggio automatico delle applicazioni. Alcuni degli strumenti richiedono l'intervento manuale. Si consiglia di automatizzare il più possibile le attività di monitoraggio.

## Strumenti di monitoraggio automatici

Per controllare AWS IoT e segnalare l'eventuale presenza di problemi, puoi usare gli strumenti di monitoraggio automatici seguenti:

- Allarmi Amazon CloudWatch – Controllano un singolo parametro per un periodo di tempo specificato ed eseguono una o più operazioni in base alla relazione tra il valore del parametro e una determinata soglia per più periodi di tempo. L'operazione corrisponde all'invio di una notifica a un argomento Amazon Simple Notification Service (Amazon SNS) o a una policy Amazon EC2 Auto Scaling. Gli allarmi CloudWatch non richiamano operazioni semplicemente perché si trovano in un determinato stato. Lo stato deve essere cambiato e restare costante per un numero specificato di periodi. Per ulteriori informazioni, consulta [Monitoraggio con Amazon CloudWatch \(p. 646\)](#).
- Amazon CloudWatch Logs – Monitorare, archiviare e accedere ai file di log da AWS CloudTrail o altre origini. Per ulteriori informazioni, consulta [Monitoraggio dei file di log](#) nella Guida per l'utente di Amazon CloudWatch.
- Amazon CloudWatch Events – Abbina gli eventi e li indirizza a una o più funzioni o flussi target per apportare modifiche, acquisire informazioni di stato ed effettuare azioni correttive. Per ulteriori informazioni, consulta [Cos'è Amazon CloudWatch Events?](#) nella Guida per l'utente di Amazon CloudWatch.
- Monitoraggio dei log AWS CloudTrail – È possibile condividere file di log tra gli account, monitorare i file di log CloudTrail in tempo reale inviandoli a CloudWatch Logs, scrivere applicazioni di elaborazione dei log in Java e verificare che i file di log non siano cambiati dopo la distribuzione da parte di CloudTrail. Per ulteriori informazioni, consulta [Gestione dei file di log con CloudTrail](#) nella AWS CloudTrail User Guide.

## Strumenti di monitoraggio manuali

Un'altra parte importante del monitoraggio di AWS IoT implica il monitoraggio manuale degli elementi non coperti dagli allarmi CloudWatch. AWS IoT, CloudWatch e altri pannelli di controllo della console del servizio AWS offrono una visualizzazione immediata dello stato dell'ambiente AWS. Ti consigliamo anche di controllare i file di log in AWS IoT.

- Il pannello di controllo di AWS IoT mostra le seguenti informazioni:
  - Certificati CA
  - Certificati
  - Policy
  - Regole
  - Oggetti
- La home page di CloudWatch mostra le seguenti informazioni:
  - Lo stato e gli allarmi attuali.
  - I grafici degli allarmi e delle risorse.
  - Lo stato dei servizi.

È possibile usare CloudWatch per le seguenti operazioni:

- Creare [pannelli di controllo personalizzati](#) per monitorare i servizi di tuo interesse.
- Creare grafici dei dati dei parametri per la risoluzione di problemi e il rilevamento di tendenze.
- Ricercare e analizzare tutti i parametri delle risorse AWS.
- Creare e modificare gli allarmi per ricevere le notifiche dei problemi.

# Monitoraggio con Amazon CloudWatch

Puoi monitorare AWS IoT usando CloudWatch, che raccoglie i dati non elaborati da AWS IoT e li elabora trasformandoli in parametri leggibili quasi in tempo reale. Queste statistiche vengono registrate per un periodo di due settimane, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione Web. Per impostazione predefinita, i dati dei parametri di AWS IoT vengono inviati automaticamente a CloudWatch a intervalli di un minuto. Per ulteriori informazioni, consulta [Introduzione a Amazon CloudWatch](#), [Amazon CloudWatch Events](#) e [Amazon CloudWatch Logs](#) nella Guida per l'utente di Amazon CloudWatch.

## Argomenti

- [Parametri e dimensioni di AWS IoT \(p. 646\)](#)
- [Come si utilizzano i parametri di AWS IoT? \(p. 653\)](#)
- [Creazione di allarmi CloudWatch per il monitoraggio di AWS IoT \(p. 653\)](#)

## Parametri e dimensioni di AWS IoT

Quando si interagisce con AWS IoT, il servizio invia i parametri e le dimensioni seguenti a CloudWatch ogni minuto. Per visualizzare i parametri per AWS IoT, puoi utilizzare le procedure seguenti.

### Per visualizzare i parametri (console CloudWatch)

I parametri vengono raggruppati prima in base al namespace del servizio e successivamente in base alle diverse combinazioni di dimensioni all'interno di ogni namespace.

1. Aprire la console CloudWatch all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nel riquadro di navigazione, scegliere Metrics (Parametri).
3. Nel riquadro CloudWatch Metrics by Category (Parametri CloudWatch per categoria), nella categoria dei parametri per AWS IoT, scegliere una categoria di parametri, quindi nel riquadro superiore scorrere verso il basso per visualizzare l'elenco completo di parametri.

### Per visualizzare i parametri (CLI)

- Al prompt dei comandi, utilizza il comando seguente:

```
aws cloudwatch list-metrics --namespace "AWS/IoT"
```

CloudWatch mostra i seguenti parametri per AWS IoT:

## Parametri di AWS IoT

Lo spazio dei nomi `AWS/IoT` include i seguenti parametri. AWS IoT invia i seguenti parametri a CloudWatch una volta per ogni richiesta ricevuta.

### Parametri di AWS IoT

| Parametro                            | Descrizione                                                                                               |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------|
| RulesExecuted                        | Il numero di regole AWS IoT eseguite.                                                                     |
| NumLogEventsFailedToPublishThrottled | Il numero di eventi di log nel batch la cui pubblicazione non è riuscita a causa di errori di throttling. |

| Parametro                             | Descrizione                                                                                            |
|---------------------------------------|--------------------------------------------------------------------------------------------------------|
| NumLogBatchesFailedToPublishThrottled | Il batch singolo di eventi di log la cui pubblicazione non è riuscita a causa di errori di throttling. |

#### Parametri delle regole

| Parametro            | Descrizione                                                                                                                                                                                                                                               |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TopicMatch           | Il numero di messaggi in arrivo pubblicati su un argomento che la regola sta ascoltando. La dimensione RuleName contiene il nome della regola.                                                                                                            |
| ParseError           | Il numero di errori di analisi JSON che si sono verificati in messaggi pubblicati su un argomento che la regola sta ascoltando. La dimensione RuleName contiene il nome della regola.                                                                     |
| RuleNotFound         | La regola da attivare non è stata trovata. La dimensione RuleName contiene il nome della regola.                                                                                                                                                          |
| RuleMessageThrottled | Il numero di messaggi sottoposto a throttling dal motore di regole a causa di comportamento dannoso o perché il numero di messaggi supera il limite di throttling del motore di regole. La dimensione RuleName contiene il nome della regola da attivare. |

#### Parametri delle operazioni sulle regole

| Parametro | Descrizione                                                                                                                                                                                                                                                                                                   |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Riuscito  | Il numero di invocazioni di operazioni sulle regole riuscite. La dimensione RuleName contiene il nome della regola che specifica l'operazione. La dimensione ActionType contiene il tipo di azione che è stato invocato.                                                                                      |
| Errore    | Il numero di invocazioni di operazioni sulle regole non riuscite. La dimensione RuleName contiene il nome della regola che specifica l'operazione. La dimensione RuleName contiene il nome della regola che specifica l'operazione. La dimensione ActionType contiene il tipo di azione che è stato invocato. |

#### Parametri del broker di messaggi

| Parametro           | Descrizione                                                                                                                                                                                                                                    |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connect.AuthError   | Il numero di richieste di connessione che il broker di messaggi non ha potuto autorizzare. La dimensione Protocol contiene il protocollo utilizzato per inviare il messaggio CONNECT.                                                          |
| Connect.ClientError | Il numero di richieste di connessione respinte perché il messaggio MQTT non rispondeva ai requisiti definiti in <a href="#">Limiti di AWS IoT</a> . La dimensione Protocol contiene il protocollo utilizzato per inviare il messaggio CONNECT. |

| Parametro              | Descrizione                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connect.ServerError    | Il numero di richieste di connessione non riuscite a causa di un errore interno. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per inviare il messaggio CONNECT.                                                                                                                                                                                            |
| Connect.Success        | Il numero di connessioni con esito positivo al broker di messaggi. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per inviare il messaggio CONNECT.                                                                                                                                                                                                          |
| Connect.Throttle       | Il numero di richieste di connessione per cui è stato eseguito il throttling perché il client ha superato la velocità di richiesta di connessione consentita. Può essere la velocità di connessione a livello di account o il numero di connessioni dallo stesso ID client. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per inviare il messaggio CONNECT. |
| Ping.Success           | Il numero di messaggi ping ricevuti dal broker di messaggi. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per inviare il messaggio ping.                                                                                                                                                                                                                    |
| PublishIn.AuthError    | Il numero di richieste di pubblicazione che il broker di messaggi non ha potuto autorizzare. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per pubblicare il messaggio.                                                                                                                                                                                     |
| PublishIn.ClientError  | Il numero di richieste di pubblicazione respinte dal broker di messaggi perché il messaggio non rispondeva ai requisiti definiti in <a href="#">Limiti di AWS IoT</a> . La dimensione <code>Protocol</code> contiene il protocollo utilizzato per pubblicare il messaggio.                                                                                                          |
| PublishIn.ServerError  | Il numero di richieste di pubblicazione che il broker di messaggi non è riuscito a elaborare a causa di un errore interno. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per inviare il messaggio PUBLISH.                                                                                                                                                  |
| PublishIn.Success      | Il numero di richieste di pubblicazione correttamente elaborate dal broker di messaggi. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per inviare il messaggio PUBLISH.                                                                                                                                                                                     |
| PublishIn.Throttle     | Il numero di richieste di pubblicazione per cui è stato eseguito il throttling perché il client ha superato la velocità di messaggi in arrivo consentita. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per inviare il messaggio PUBLISH.                                                                                                                   |
| PublishOut.AuthError   | Il numero di richieste di pubblicazione effettuate dal broker di messaggi che AWS IoT non ha potuto autorizzare. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per inviare il messaggio PUBLISH.                                                                                                                                                            |
| PublishOut.ClientError | Il numero di richieste di pubblicazione effettuate dal broker di messaggi che sono state respinte perché il messaggio non rispondeva ai requisiti definiti in <a href="#">Limiti di AWS IoT</a> . La dimensione <code>Protocol</code> contiene il protocollo utilizzato per inviare il messaggio PUBLISH.                                                                           |

| Parametro               | Descrizione                                                                                                                                                                                                                                                                                                    |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PublishOut.Success      | Il numero di richieste di pubblicazione correttamente effettuate dal broker di messaggi. La dimensione <b>Protocol</b> contiene il protocollo utilizzato per inviare il messaggio <b>PUBLISH</b> .                                                                                                             |
| Subscribe.AuthError     | Il numero di richieste di sottoscrizione effettuate da un client, che non è stato possibile autorizzare. La dimensione <b>Protocol</b> contiene il protocollo utilizzato per inviare il messaggio <b>SUBSCRIBE</b> .                                                                                           |
| Subscribe.ClientError   | Il numero di richieste di sottoscrizione che sono state respinte perché il messaggio <b>SUBSCRIBE</b> non rispondeva ai requisiti definiti in <a href="#">Limiti di AWS IoT</a> . La dimensione <b>Protocol</b> contiene il protocollo utilizzato per inviare il messaggio <b>SUBSCRIBE</b> .                  |
| Subscribe.ServerError   | Il numero di richieste di sottoscrizione respinte a causa di un errore interno. La dimensione <b>Protocol</b> contiene il protocollo utilizzato per inviare il messaggio <b>SUBSCRIBE</b> .                                                                                                                    |
| Subscribe.Success       | Il numero di richieste di sottoscrizione correttamente elaborate dal broker di messaggi. La dimensione <b>Protocol</b> contiene il protocollo utilizzato per inviare il messaggio <b>SUBSCRIBE</b> .                                                                                                           |
| Subscribe.Throttle      | Il numero di richieste di sottoscrizione per cui è stato eseguito il throttling perché il client ha superato la velocità di richiesta di sottoscrizione consentita. La dimensione <b>Protocol</b> contiene il protocollo utilizzato per inviare il messaggio <b>SUBSCRIBE</b> .                                |
| Unsubscribe.ClientError | Il numero di richieste di annullamento sottoscrizione che sono state respinte perché il messaggio <b>UNSUBSCRIBE</b> non rispondeva ai requisiti definiti in <a href="#">Limiti di AWS IoT</a> . La dimensione <b>Protocol</b> contiene il protocollo utilizzato per inviare il messaggio <b>UNSUBSCRIBE</b> . |
| Unsubscribe.ServerError | Il numero di richieste di annullamento della sottoscrizione respinte a causa di un errore interno. La dimensione <b>Protocol</b> contiene il protocollo utilizzato per inviare il messaggio <b>UNSUBSCRIBE</b> .                                                                                               |
| Unsubscribe.Success     | Il numero di richieste di annullamento della sottoscrizione correttamente elaborate dal broker di messaggi. La dimensione <b>Protocol</b> contiene il protocollo utilizzato per inviare il messaggio <b>UNSUBSCRIBE</b> .                                                                                      |
| Unsubscribe.Throttle    | Il numero di richieste di annullamento della sottoscrizione respinte perché il client ha superato la velocità di richiesta di annullamento della sottoscrizione consentita. La dimensione <b>Protocol</b> contiene il protocollo utilizzato per inviare il messaggio <b>UNSUBSCRIBE</b> .                      |

## Note

I parametri del broker di messaggi sono mostrati nella console AWS IoT sotto Protocol Metrics (Parametri protocollo).

### Parametri per la copia shadow del dispositivo

| Parametro                  | Descrizione                                                                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DeleteThingShadow.Accepted | Il numero di richieste DeleteThingShadow elaborate correttamente. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per effettuare la richiesta. |
| GetThingShadow.Accepted    | Il numero di richieste GetThingShadow elaborate correttamente. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per effettuare la richiesta.    |
| UpdateThingShadow.Accepted | Il numero di richieste UpdateThingShadow elaborate correttamente. La dimensione <code>Protocol</code> contiene il protocollo utilizzato per effettuare la richiesta. |

## Note

I parametri per la copia shadow del dispositivo vengono visualizzati nella console AWS IoT in Protocol Metrics (Parametri protocollo).

### Parametri processi

| Parametro                        | Descrizione                                                                                                                                                           |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ServerError                      | Numero di errori server generati durante l'esecuzione del processo. La dimensione <code>JobId</code> contiene l'ID del processo.                                      |
| ClientError                      | Numero di errori client generati durante l'esecuzione del processo. La dimensione <code>JobId</code> contiene l'ID del processo.                                      |
| QueuedJobExecutionTotalCount     | Il numero totale di esecuzioni di processi il cui stato è <code>QUEUED</code> per il dato processo. La dimensione <code>JobId</code> contiene l'ID del processo.      |
| InProgressJobExecutionTotalCount | Il numero totale di esecuzioni di processi il cui stato è <code>IN_PROGRESS</code> per il dato processo. La dimensione <code>JobId</code> contiene l'ID del processo. |
| FailedJobExecutionTotalCount     | Il numero totale di esecuzioni di processi il cui stato è <code>FAILED</code> per il dato processo. La dimensione <code>JobId</code> contiene l'ID del processo.      |
| SucceededJobExecutionTotalCount  | Il numero totale di esecuzioni di processi il cui stato è <code>SUCCESS</code> per il dato processo. La dimensione <code>JobId</code> contiene l'ID del processo.     |
| CanceledJobExecutionTotalCount   | Il numero totale di esecuzioni di processi il cui stato è <code>CANCELED</code> per il dato processo. La dimensione <code>JobId</code> contiene l'ID del processo.    |

| Parametro                      | Descrizione                                                                                                                                                                                                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RejectedJobExecutionTotalCount | Il numero totale di esecuzioni di processi il cui stato è REJECTED per il dato processo. La dimensione JobId contiene l'ID del processo.                                                                                                                                                         |
| RemovedJobExecutionTotalCount  | Il numero totale di esecuzioni di processi il cui stato è REMOVED per il dato processo. La dimensione JobId contiene l'ID del processo.                                                                                                                                                          |
| QueuedJobExecutionCount        | Il numero di esecuzioni di processi il cui stato è cambiato in QUEUED entro un intervallo temporale stabilito da CloudWatch. Per ulteriori informazioni sui parametri CloudWatch, consulta <a href="#">Parametri di Amazon CloudWatch</a> . La dimensione JobId contiene l'ID del processo.      |
| InProgressJobExecutionCount    | Il numero di esecuzioni di processi il cui stato è cambiato in IN_PROGRESS entro un intervallo temporale stabilito da CloudWatch. Per ulteriori informazioni sui parametri CloudWatch, consulta <a href="#">Parametri di Amazon CloudWatch</a> . La dimensione JobId contiene l'ID del processo. |
| FailedJobExecutionCount        | Il numero di esecuzioni di processi il cui stato è cambiato in FAILED entro un intervallo temporale stabilito da CloudWatch. Per ulteriori informazioni sui parametri CloudWatch, consulta <a href="#">Parametri di Amazon CloudWatch</a> . La dimensione JobId contiene l'ID del processo.      |
| SucceededJobExecutionCount     | Il numero di esecuzioni di processi il cui stato è cambiato in SUCCESS entro un intervallo temporale stabilito da CloudWatch. Per ulteriori informazioni sui parametri CloudWatch, consulta <a href="#">Parametri di Amazon CloudWatch</a> . La dimensione JobId contiene l'ID del processo.     |
| CanceledJobExecutionCount      | Il numero di esecuzioni di processi il cui stato è cambiato in CANCELED entro un intervallo temporale stabilito da CloudWatch. Per ulteriori informazioni sui parametri CloudWatch, consulta <a href="#">Parametri di Amazon CloudWatch</a> . La dimensione JobId contiene l'ID del processo.    |
| RejectedJobExecutionCount      | Il numero di esecuzioni di processi il cui stato è cambiato in REJECTED entro un intervallo temporale stabilito da CloudWatch. Per ulteriori informazioni sui parametri CloudWatch, consulta <a href="#">Parametri di Amazon CloudWatch</a> . La dimensione JobId contiene l'ID del processo.    |
| RemovedJobExecutionCount       | Il numero di esecuzioni di processi il cui stato è cambiato in REMOVED entro un intervallo temporale stabilito da CloudWatch. Per ulteriori informazioni sui parametri CloudWatch, consulta <a href="#">Parametri di Amazon CloudWatch</a> . La dimensione JobId contiene l'ID del processo.     |

### Parametri di Device Defender Audit

| Parametro             | Descrizione                                                                                                                                                          |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NonCompliantResources | Il numero di risorse risultate non conformi a un controllo. Il sistema rileva il numero di risorse risultate non conformi per ogni controllo di ogni audit eseguito. |
| ResourcesEvaluated    | Il numero di risorse valutate per la conformità. Il sistema rileva il numero di risorse valutate per ogni controllo di ogni audit eseguito.                          |

### Parametri di Device Defender Detect

| Parametro             | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Violazioni            | Il numero di nuove violazioni di comportamenti per il profilo di sicurezza rilevate dall'ultima valutazione completata. Il sistema rileva il numero di nuove violazioni per l'account per un profilo di sicurezza specifico e per un comportamento specifico di un profilo di sicurezza specifico.                                                                                                                                                                                   |
| ViolationsCleared     | Il numero di violazioni di comportamenti per il profilo di sicurezza risolte dall'ultima valutazione completata. Il sistema rileva il numero di violazioni risolte per l'account per un profilo di sicurezza specifico e per un comportamento specifico di un profilo di sicurezza specifico.                                                                                                                                                                                        |
| ViolationsInvalidated | Il numero di violazioni di comportamenti per il profilo di sicurezza per cui le informazioni non sono più disponibili dall'ultima valutazione completata (perché il dispositivo ha interrotto la reportistica o perché, per qualsiasi motivo, non viene più effettuato il monitoraggio). Il sistema rileva il numero di violazioni non convalidate per l'intero account per un profilo di sicurezza specifico e per un comportamento specifico di un profilo di sicurezza specifico. |

## Dimensioni per i parametri

I parametri utilizzano lo spazio dei nomi e forniscono i parametri per le seguenti dimensioni:

| Dimensione | Descrizione                                                                              |
|------------|------------------------------------------------------------------------------------------|
| ActionType | Il <a href="#">tipo di operazione</a> specificato dalla regola attivata dalla richiesta. |
| Protocollo | Il protocollo usato per effettuare la richiesta. I valori validi sono: MQTT o HTTP       |
| RuleName   | Il nome della regola attivata dalla richiesta.                                           |

| Dimensione          | Descrizione                                                                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| JobId               | L'ID del processo di cui si sta monitorando l'avanzamento o l'esito positivo/negativo della connessione al messaggio.                                                               |
| CheckName           | Il nome del controllo Device Defender Audit i cui risultati vengono monitorati.                                                                                                     |
| ScheduledAuditName  | Il nome del Device Defender Audit i cui risultati di controllo vengono monitorati. Ha il valore "OnDemand" se i risultati riportati si riferiscono a un audit effettuato on demand. |
| SecurityProfileName | Il nome del profilo di sicurezza Device Defender Detect i cui comportamenti vengono monitorati.                                                                                     |
| BehaviorName        | Il nome del comportamento del profilo di sicurezza Device Defender Detect che viene monitorato.                                                                                     |

## Come si utilizzano i parametri di AWS IoT?

I parametri forniti da AWS IoT offrono informazioni che possono essere analizzate in diversi modi. I casi d'uso seguenti sono basati su uno scenario in cui sono presenti dieci oggetti che si connettono a Internet una volta al giorno. Ogni giorno:

- Dieci oggetti si connettono a AWS IoT circa nello stesso momento.
- Ogni oggetto sottoscrive un filtro di argomenti e attende un'ora prima della disconnessione. Durante questo periodo, gli oggetti comunicano tra loro e apprendono ulteriori informazioni sullo stato del mondo.
- Ogni oggetto pubblica percezioni basate sui dati appena rilevati usando `UpdateThingShadow`.
- Ogni oggetto si disconnette da AWS IoT.

Questi suggerimenti sono solo introduttivi e non costituiscono un elenco completo.

- [Come è possibile ricevere una notifica se gli oggetti non si connettono correttamente ogni giorno? \(p. 654\)](#)
- [Come è possibile ricevere una notifica se gli oggetti non pubblicano dati ogni giorno? \(p. 654\)](#)
- [Come è possibile ricevere una notifica se gli aggiornamenti alle copie shadow degli oggetti vengono rifiutati ogni giorno? \(p. 655\)](#)

## Creazione di allarmi CloudWatch per il monitoraggio di AWS IoT

Puoi creare un allarme CloudWatch che invia un messaggio Amazon SNS quando lo stato dell'allarme cambia. Un allarme controlla un singolo parametro per un periodo di tempo specificato ed esegue una o più operazioni in base alla relazione tra il valore del parametro e la soglia impostata in diversi periodi di tempo. L'operazione corrisponde all'invio di una notifica a un argomento Amazon SNS o a una policy Auto Scaling. Gli allarmi attivano le operazioni solo per le modifiche di stato prolungate. Gli allarmi di CloudWatch non attivano operazioni semplicemente perché si trovano in un determinato stato, ma è necessario che lo stato sia stato cambiato e che sia rimasto invariato per un numero specificato di periodi.

## Come è possibile ricevere una notifica se gli oggetti non si connettono correttamente ogni giorno?

1. Crea un argomento Amazon SNS, arn:aws:sns:us-east-1:123456789012:things-not-connecting-successfully.

Per ulteriori informazioni, consulta la pagina relativa alla [configurazione di Amazon Simple Notification Service](#).

2. Crea l'allarme.

```
Prompt>aws cloudwatch put-metric-alarm \
 --alarm-name ConnectSuccessAlarm \
 --alarm-description "Alarm when my Things don't connect successfully" \
 --namespace AWS/IoT \
 --metric-name Connect.Success \
 --dimensions Name=Protocol,Value=MQTT \
 --statistic Sum \
 --threshold 10 \
 --comparison-operator LessThanThreshold \
 --period 86400 \
 --unit Count \
 --evaluation-periods 1 \
 --alarm-actions arn:aws:sns:us-east-1:1234567890:things-not-connecting-successfully
```

3. Testa l'allarme.

```
Prompt>aws cloudwatch set-alarm-state --alarm-name ConnectSuccessAlarm --state-reason
"initializing" --state-value OK
```

```
Prompt>aws cloudwatch set-alarm-state --alarm-name ConnectSuccessAlarm --state-reason
"initializing" --state-value ALARM
```

## Come è possibile ricevere una notifica se gli oggetti non pubblicano dati ogni giorno?

1. Creare un argomento Amazon SNS, arn:aws:sns:us-east-1:123456789012:things-not-publishing-data.

Per ulteriori informazioni, consulta la pagina relativa alla [configurazione di Amazon Simple Notification Service](#).

2. Crea l'allarme.

```
Prompt>aws cloudwatch put-metric-alarm \
 --alarm-name PublishInSuccessAlarm \
 --alarm-description "Alarm when my Things don't publish their data" \
 --namespace AWS/IoT \
 --metric-name PublishIn.Success \
 --dimensions Name=Protocol,Value=MQTT \
 --statistic Sum \
 --threshold 10 \
 --comparison-operator LessThanThreshold \
 --period 86400 \
 --unit Count \
 --evaluation-periods 1 \
 --alarm-actions arn:aws:sns:us-east-1:1234567890:things-not-publishing-data
```

3. Testa l'allarme.

```
Prompt>aws cloudwatch set-alarm-state --alarm-name PublishInSuccessAlarm --state-reason "initializing" --state-value OK
```

```
Prompt>aws cloudwatch set-alarm-state --alarm-name PublishInSuccessAlarm --state-reason "initializing" --state-value ALARM
```

## Come è possibile ricevere una notifica se gli aggiornamenti shadow degli oggetti vengono rifiutati ogni giorno?

1. Crea un argomento Amazon SNS, arn:aws:sns:us-east-1:1234567890:things-shadow-updates-rejected.

Per ulteriori informazioni, consulta la pagina relativa alla [configurazione di Amazon Simple Notification Service](#).

2. Crea l'allarme.

```
Prompt>aws cloudwatch put-metric-alarm \
--alarm-name UpdateThingShadowSuccessAlarm \
--alarm-description "Alarm when my Things Shadow updates are getting rejected" \
--namespace AWS/IoT \
--metric-name UpdateThingShadow.Success \
--dimensions Name=Protocol,Value=MQTT \
--statistic Sum \
--threshold 10 \
--comparison-operator LessThanThreshold \
--period 86400 \
--unit Count \
--evaluation-periods 1 \
--alarm-actions arn:aws:sns:us-east-1:1234567890:things-shadow-updates-rejected
```

3. Testa l'allarme.

```
Prompt>aws cloudwatch set-alarm-state --alarm-name UpdateThingShadowSuccessAlarm --state-reason "initializing" --state-value OK
```

```
Prompt>aws cloudwatch set-alarm-state --alarm-name UpdateThingShadowSuccessAlarm --state-reason "initializing" --state-value ALARM
```

## Monitoraggio con CloudWatch Logs

AWS IoT invia eventi di stato per ogni messaggio che passa dai dispositivi attraverso il broker di messaggi e il motore di regole. Per visualizzare questi log, è necessario configurare AWS IoT sulla generazione dei log usati da CloudWatch.

Per ulteriori informazioni su CloudWatch Logs, consulta [CloudWatch Logs](#). Per informazioni sugli AWS IoT CloudWatch Logs supportati, consulta [Formato delle voci di log di CloudWatch \(p. 660\)](#).

Per abilitare il logging di AWS IoT, è necessario creare un ruolo IAM, registrarlo su AWS IoT e configurare il logging di AWS IoT.

#### Note

Prima di abilitare il logging di AWS IoT, assicurati di comprendere le autorizzazioni di accesso di CloudWatch Logs. Gli utenti che dispongono dell'accesso a CloudWatch Logs possono visualizzare le informazioni di debug dai dispositivi. Per ulteriori informazioni, consulta [Autenticazione e controllo degli accessi per Amazon CloudWatch Logs](#).

## Creazione di un ruolo di logging

Usa la [console IAM](#) per creare un ruolo di logging.

1. Nel riquadro di navigazione scegli Roles (Ruoli) e quindi Create new role (Crea nuovo ruolo).
2. Scegliere AWS Service Role (Ruolo servizio AWS), quindi come tipo di ruolo del servizio scegliere AWS IoT.
3. Scegli il ruolo AWSIoTLogging e quindi Next Step (Fase successiva).
4. Immettere un nome e una descrizione per il ruolo e quindi scegliere Create role (Crea ruolo).

## Policy del ruolo di logging

Nei documenti seguenti relativi alle policy sono contenute la policy del ruolo e la policy di trust che permettono a AWS IoT di inviare i log a CloudWatch per tuo conto.

#### Note

Questi documenti sono stati creati al momento della creazione del ruolo di logging.

Policy del ruolo:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "logs:CreateLogGroup",
 "logs:CreateLogStream",
 "logs:PutLogEvents",
 "logs:PutMetricFilter",
 "logs:PutRetentionPolicy"
],
 "Resource": [
 "*"
]
 }
]
}
```

Policy di trust:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "",
 "Effect": "Allow",
 "Principal": {
 "Service": "iot.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
```

```
 "Action": "sts:AssumeRole"
 }
}
```

## Livello di log

Il livello di log specifica i tipi di log generati.

### ERROR

Qualsiasi errore che provoca la mancata riuscita di un'operazione.

I log includono solo informazioni per il livello ERROR.

### WARN

Qualsiasi evento che può potenzialmente causare incoerenze nel sistema, ma potrebbe non provocare la mancata riuscita dell'operazione.

I log includono informazioni per i livelli ERROR e WARN.

### INFO

Informazioni generali sul flusso di oggetti.

I log includono informazioni per i livelli INFO, ERROR e WARN.

### DEBUG

Informazioni che possono essere utili quando si esegue il debug di un problema.

I log includono informazioni per i livelli DEBUG, INFO, ERROR e WARN.

### DISABLED

Tutte le attività di logging sino disabilitate.

## Configurazione del logging di AWS IoT

È possibile utilizzare la console AWS IoT, il comando dell'interfaccia a riga di comando [set-v2-log-options](#) o l'API [SetV2LoggingOptions](#) per attivare la registrazione. L'entità principale utilizzata per effettuare la chiamata API deve avere [Passaggio delle autorizzazioni di un ruolo \(p. 256\)](#) per il ruolo di logging. Il ruolo di logging è passato a [set-v2-logging-opzioni](#) o [SetV2LoggingOptions](#) come parametro `roleARN`.

È possibile configurare la registrazione in modo che sia globale o granulare. Il logging globale imposta un livello di logging per tutti i log, indipendentemente dalla risorsa che ha attivato i log. Il logging granulare permette di impostare un livello di logging per una risorsa o un set di risorse specifico. Attualmente sono supportati solo i gruppi di oggetti. È possibile utilizzare la console AWS IoT, l'interfaccia a riga di comando o l'API per attivare la registrazione globale. È necessario utilizzare l'interfaccia a riga di comando o l'API per attivare la registrazione granulare.

## Logging globale

Usa il comando `set-v2-logging-options` dell'interfaccia a riga di comando per impostare le opzioni di logging per l'account. `set-v2-logging-options` accetta tre argomenti:

`--role-arn`

ARN del ruolo di logging. Il ruolo di logging concede a AWS IoT l'autorizzazione per scrivere i log in CloudWatch Logs.

--default-log-level

Livello di log da usare. I valori validi sono: ERROR, WARN, INFO, DEBUG e DISABLED

--disable-all-logs | --no-disable-all-logs

Se impostato su true (--disable-all-logs) disabilita tutti i log. Il valore predefinito (parametro non utilizzato) è false.

Ad esempio:

```
aws iot set-v2-logging-options \
--role-arn arn:aws:iam::<your-aws-account-num>:role/<IoTLoggingRole> \
--default-log-level <INFO>
```

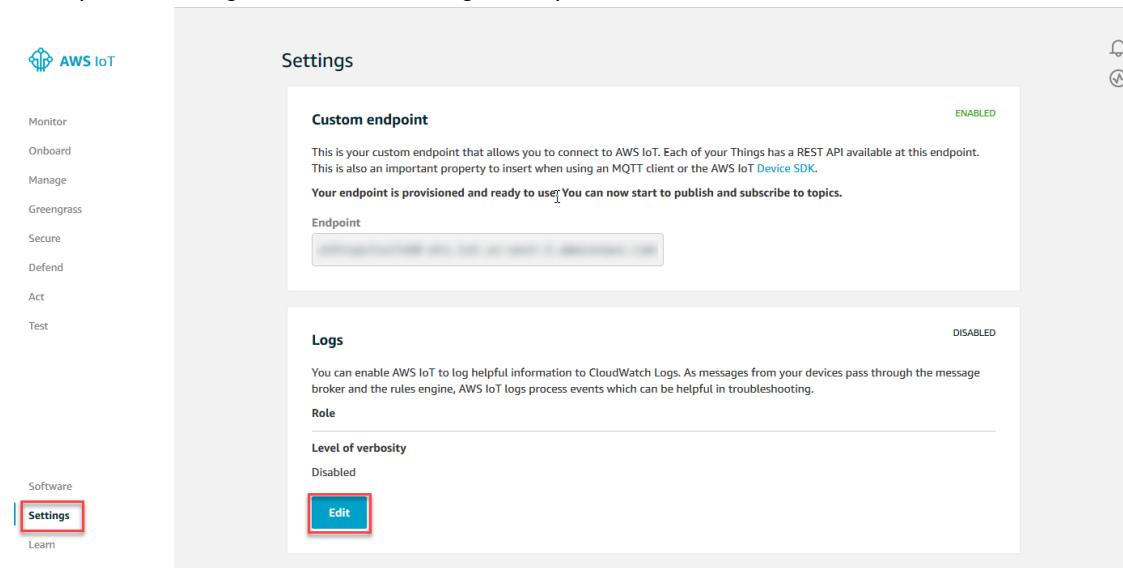
Usa il comando get-v2-logging-options dell'interfaccia a riga di comando per ottenere le opzioni di logging correnti.

#### Note

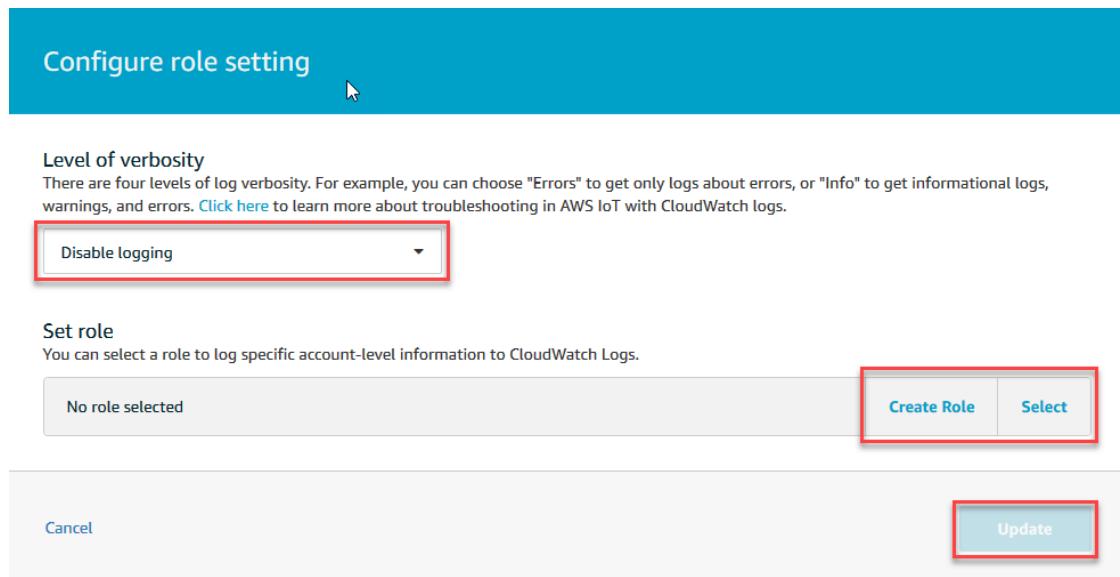
AWS IoT continua a supportare i comandi precedenti set-logging-options e get-logging-options per impostare e ottenere la registrazione globale sull'account. Va tenuto presente che, utilizzando questi comandi, i log risultanti contengono testo normale anziché payload JSON e la latenza di logging è generalmente più elevata. Non verranno apportati ulteriori miglioramenti all'implementazione dei comandi precedenti. Consigliamo di utilizzare versioni "V2" per configurare le opzioni di logging e, quando possibile, di modificare le applicazioni legacy che utilizzano le versioni precedenti.

Per configurare il monitoraggio globale tramite la console AWS IoT

1. Accedere alla console AWS IoT. Per ulteriori informazioni, consulta [Accesso alla console AWS IoT \(p. 5\)](#).
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.



3. Nella sezione Log della pagina Impostazioni scegliere Modifica. Nella sezione Log sono visualizzate le impostazioni per il ruolo e il livello di dettaglio.
4. Nella pagina Configura le impostazioni dei ruoli scegliere il livello di dettaglio che si desidera visualizzare nei log CloudWatch.



5. Scegliere Selezione per specificare un ruolo creato in precedenza oppure Crea ruolo per creare un ruolo da utilizzare per il logging.
6. Scegliere Update policy (Aggiorna policy) per salvare le modifiche.  
Esaminare i log CloudWatch per verificare se il livello delle informazioni raccolte è quello desiderato. In caso contrario, è sempre possibile modificare il livello di log in seguito.

## Logging granulare

Il logging granulare permette di specificare un livello di logging per un target. Un target è definito da un tipo di risorsa e un nome di risorsa. Al momento, AWS IoT supporta i gruppi di oggetti come target. Il logging granulare permette di impostare un livello di logging per un gruppo di oggetti specifico. Immaginiamo di avere un gruppo di oggetti denominato "Telefoni" contenente oggetti che rappresentano diversi tipi di telefoni. Creiamo quindi un altro gruppo di oggetti denominato "TelefoniCellulari" e lo impostiamo come figlio del gruppo "Telefoni". Il logging granulare permette di configurare un livello di logging per tutti gli oggetti nel gruppo "Telefoni" (e gli eventuali gruppi figlio) e un altro livello di logging per gli oggetti nel gruppo "TelefoniCellulari". In questo esempio, abbiamo assegnato due diversi livelli di logging agli oggetti nel gruppo "TelefoniCellulari" — uno che deriva dal livello di logging del gruppo di oggetti "Telefoni" e un altro che deriva dal gruppo di oggetti "TelefoniCellulari" — ma il livello di logging specificato per il gruppo di oggetti figlio ha la precedenza su quello specificato per il gruppo di oggetti padre.

Usa il comando `set-v2-logging-options` dell'interfaccia a riga di comando per abilitare il logging granulare e impostare il livello di logging predefinito. Il comando accetta gli argomenti facoltativi seguenti:

`--role-arn`

Ruolo IAM che permette a AWS IoT di scrivere in CloudWatch Logs. Se non è specificato, AWS IoT usa il ruolo di logging associato all'account. Il ruolo di logging viene associato all'account al momento della creazione. Per ulteriori informazioni, consulta [Creazione di un ruolo di logging \(p. 656\)](#).

`--default-log-level`

Livello di logging da usare se non ne viene specificato uno. I valori validi sono: `DEBUG`, `INFO`, `ERROR`, `WARN` e `DISABLED`.

`--disable-all-logs | --no-disable-all-logs`

Se impostato su `true` (`--disable-all-logs`), disabilita tutti i log. Il valore predefinito (parametro non utilizzato) è `false`.

Il comando `get-v2-logging-options` dell'interfaccia a riga di comando restituisce il ruolo di logging IAM configurato, il livello di logging predefinito e il valore `disableAllLogs`.

Usa il comando `set-v2-logging-level` dell'interfaccia a riga di comando per configurare il logging granulare per un target. Il comando accetta gli argomenti seguenti:

`--log-target`

Un oggetto JSON contenente il tipo di risorsa (campo `targetType`) e il nome (campo `targetName`) dell'entità per cui si configura il logging. AWS IoT attualmente supporta `THING_GROUP` come tipo di risorsa. È possibile configurare fino a 10 target di logging.

`--log-level`

Livello di logging usato durante la generazione di log per la risorsa specificata. I valori validi sono: `DEBUG`, `INFO`, `ERROR`, `WARN` e `DISABLED`

Usa il comando `list-v2-logging-levels` dell'interfaccia a riga di comando per ottenere un elenco dei livelli di logging granulare attualmente configurati. Chiama il comando `delete-v2-logging-level` dell'interfaccia a riga di comando per eliminare un livello di logging. Usa il comando `delete-v2-logging-level` per eliminare un livello di logging granulare.

## Formato delle voci di log di CloudWatch

Ogni componente di AWS IoT genera i propri log. Ogni voce di log ha un attributo `eventType` che indica l'operazione che ha causato la generazione del log. In questa sezione vengono descritti i log generati dai componenti di AWS IoT seguenti:

- [Broker di messaggi \(p. 661\)](#)
- [Servizio Device Shadow \(p. 665\)](#)
- [Motore di regole \(p. 667\)](#)
- [Jobs \(p. 671\)](#)

Tutti i log di CloudWatch Logs hanno gli attributi comuni seguenti:

`timestamp`

Timestamp UNIX relativo al momento in cui il client si è connesso al broker di messaggi AWS IoT.

`logLevel`

Livello di log usato. Per ulteriori informazioni, consulta [the section called “Livello di log” \(p. 657\)](#).

`traceId`

Identificatore generato in modo casuale che può essere usato per correlare tutti i log per una richiesta specifica.

`accountId`

ID dell'account AWS.

`status`

Stato della richiesta.

`eventType`

Tipo di evento per cui il log è stato generato. Il valore relativo al tipo di evento per ogni evento è elencato nelle sezioni seguenti.

## Log del broker di messaggi

Il broker di messaggi AWS IoT genera log per gli eventi seguenti:

### Connect Log

Il broker di messaggi AWS IoT genera un log **Connect** alla connessione di un client MQTT.

[more info \(1\)](#)

Ad esempio:

```
{
 "timestamp": "2017-08-10 15:37:23.476",
 "logLevel": "INFO",
 "traceId": "20b23f3f-d7f1-faeae-169f-82263394fbdb",
 "accountId": "123456789012",
 "status": "Success",
 "eventType": "Connect",
 "protocol": "MQTT",
 "clientId": "abf27092886e49a8a5c1922749736453",
 "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
 "sourceIp": "205.251.233.181",
 "sourcePort": 13490
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log **Connect** contengono gli attributi seguenti:

**eventType**

Connect per i log relativi alla connessione.

**protocol**

Protocollo usato per effettuare la richiesta. I valori validi sono **MQTT** e **HTTP**.

**clientId**

ID del client da cui proviene la richiesta.

**principalId**

ID dell'entità principale da cui proviene la richiesta.

**sourcelp**

Indirizzo IP da cui ha avuto origine la richiesta.

**sourcePort**

Porta da cui ha avuto origine la richiesta.

### Subscribe Log

Il broker di messaggi AWS IoT genera un log **Subscribe** quando un client MQTT sottoscrive un argomento.

[more info \(2\)](#)

Ad esempio:

```
{
 "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
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log **Subscribe** contengono gli attributi seguenti:

**eventType**

Subscribe per i log relativi alla sottoscrizione.

**protocol**

Protocollo usato per effettuare la richiesta. I valori validi sono **MQTT** e **HTTP**.

**topicName**

Nome dell'argomento sottoscritto.

**clientId**

ID del client da cui proviene la richiesta.

**principalId**

ID dell'entità principale da cui proviene la richiesta.

**sourceIp**

Indirizzo IP da cui ha avuto origine la richiesta.

**sourcePort**

Porta da cui ha avuto origine la richiesta.

### Publish-In Log

Quando il broker di messaggi AWS IoT riceve un messaggio MQTT, genera un log **Publish-In**.

[more info \(3\)](#)

Ad esempio:

```
{
 "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
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log **Publish-In** contengono gli attributi seguenti:

**eventType**

Publish-In quando il broker di messaggi riceve un messaggio.

**status**

Stato della richiesta.

**protocol**

Protocollo usato per effettuare la richiesta. I valori validi sono **MQTT** e **HTTP**.

**topicName**

Nome dell'argomento sottoscritto.

**clientId**

ID del client da cui proviene la richiesta.

**principalId**

ID dell'entità principale da cui proviene la richiesta.

**sourceIp**

Indirizzo IP da cui ha avuto origine la richiesta.

**sourcePort**

Porta da cui ha avuto origine la richiesta.

### Publish-Out Log

Quando il broker di messaggi pubblica un messaggio MQTT, genera un log **Publish-Out**.

[more info \(4\)](#)

Ad esempio:

```
{
 "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
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log **Publish-Out** contengono gli attributi seguenti:

**eventType**

Publish-Out quando il broker di messaggi pubblica un messaggio.

**status**

Stato della richiesta.

**protocol**

Protocollo usato per effettuare la richiesta. I valori validi sono **MQTT** e **HTTP**.

**topicName**

Nome dell'argomento sottoscritto.

**clientId**

ID del client da cui proviene la richiesta.

**principalId**

ID dell'entità principale da cui proviene la richiesta.

**sourceIp**

Indirizzo IP da cui ha avuto origine la richiesta.

**sourcePort**

Porta da cui ha avuto origine la richiesta.

### Disconnect Log

Il broker di messaggi AWS IoT genera un log **Disconnect** quando un client MQTT si disconnette.

[more info \(5\)](#)

Ad esempio:

```
{
 "timestamp": "2017-08-10 15:37:23.476",
 "logLevel": "INFO",
 "traceId": "20b23f3f-d7f1-faea-169f-82263394fbdb",
 "accountId": "123456789012",
 "status": "Success",
 "eventType": "Disconnect",
 "protocol": "MQTT",
 "clientId": "abf27092886e49a8a5c1922749736453",
 "principalId": "145179c40e2219e18a909d896a5340b74cf97a39641beec2fc3eeafc5a932167",
 "sourceIp": "205.251.233.181",
 "sourcePort": 13490
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log **Disconnect** contengono gli attributi seguenti:

**eventType**

**Disconnect** per i log relativi alla connessione.

**protocol**

Protocollo usato per effettuare la richiesta. I valori validi sono **MQTT** e **HTTP**.

**clientId**

ID del client da cui proviene la richiesta.

**principalId**

ID dell'entità principale da cui proviene la richiesta.

sourcelp

Indirizzo IP da cui ha avuto origine la richiesta.

sourcePort

Porta da cui ha avuto origine la richiesta.

## Log di Device Shadow

Il servizio Device Shadow AWS IoT genera log per gli eventi seguenti:

GetThingShadow Logs

Il servizio Device Shadow genera un log GetThingShadow quando viene ricevuta una richiesta GET per una copia shadow.

more info (6)

Ad esempio:

```
{
 "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"
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log GetThingShadow contengono gli attributi seguenti:

eventType

GetThingShadow per i log GetThingShadow.

protocol

Protocollo usato per effettuare la richiesta. I valori validi sono MQTT e HTTP.

deviceShadowName

Nome della copia shadow richiesta.

topicName

Nome dell'argomento in cui la richiesta è stata pubblicata.

UpdateThingShadow Logs

Il servizio Device Shadow genera un log UpdateThingShadow quando viene ricevuta una richiesta di aggiornamento di una copia shadow di un dispositivo.

more info (7)

Ad esempio:

```
{
 "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"
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log `UpdateThingShadow` contengono gli attributi seguenti:

**eventType**

UpdateThingShadow per i log di aggiornamento delle copie shadow.

**protocol**

Protocollo usato per effettuare la richiesta. I valori validi sono MQTT e HTTP.

**deviceShadowName**

Nome della copia shadow da aggiornare.

**topicName**

Nome dell'argomento in cui la richiesta è stata pubblicata.

### DeleteThingShadow Logs

Il servizio Device Shadow genera un log `DeleteThingShadow` quando viene ricevuta una richiesta di eliminazione di una copia shadow di un dispositivo.

[more info \(8\)](#)

Ad esempio:

```
{
 "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"
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log `DeleteThingShadow` contengono gli attributi seguenti:

**eventType**

DeleteThingShadow per i log DeleteThingShadow.

**protocol**

Protocollo usato per effettuare la richiesta. I valori validi sono MQTT e HTTP.

**deviceShadowName**

Nome della copia shadow da aggiornare.

#### topicName

Nome dell'argomento in cui la richiesta è stata pubblicata.

## Log del motore di regole

Il servizio del motore di regole di AWS IoT genera log per gli eventi seguenti:

### Rule Match Logs

Il motore di regole di AWS IoT genera un log `RuleMatch` quando il broker di messaggi riceve un messaggio che corrisponde a una regola.

[more info \(9\)](#)

Ad esempio:

```
{
 "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"
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log `RuleMatch` contengono gli attributi seguenti:

#### eventType

`RuleMatch` per i log `RuleMatch`.

#### clientId

ID del client da cui proviene la richiesta.

#### topicName

Nome dell'argomento sottoscritto.

#### ruleName

Nome della regola corrispondente.

#### principalId

ID dell'entità principale da cui proviene la richiesta.

### Function Execution Logs

Il motore di regole genera un log `FunctionExecution` quando una query SQL di una regola chiama una funzione esterna. Una funzione esterna viene richiamata quando l'operazione di una regola invia una richiesta HTTP a AWS IoT o a un altro servizio Web (ad esempio, richiamando `get_thing_shadow` o `machinelearning_predict`).

[more info \(10\)](#)

Un log `FunctionExecution` ha il seguente aspetto:

```
{
 "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"
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log **FunctionExecution** contengono gli attributi seguenti:

**eventType**

FunctionExecution per i log RuleMatch.

**clientId**

N/A per i log FunctionExecution.

**topicName**

Nome dell'argomento sottoscritto.

**ruleName**

Nome della regola corrispondente.

**resources**

Raccolta di risorse usate dalle operazioni della regola.

**principalId**

ID dell'entità principale da cui proviene la richiesta.

### Starting Execution Logs

Quando il motore di regole AWS IoT inizia ad attivare un'operazione di una regola, genera un log StartingExecution.

more info (11)

Ad esempio:

```
{
 "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"
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log `StartingExecution` contengono gli attributi seguenti:

`eventType`

StartingRuleExecution per i log StartingRuleExecution.

`clientId`

ID del client da cui proviene la richiesta.

`topicName`

Nome dell'argomento sottoscritto.

`ruleName`

Nome della regola corrispondente.

`ruleAction`

Il nome dell'operazione attivata.

`principalId`

ID dell'entità principale da cui proviene la richiesta.

### Rule Execution Logs

Quando il motore di regole AWS IoT attiva un'operazione di una regola, genera un log RuleExecution.

[more info \(12\)](#)

Ad esempio:

```
{
 "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"
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log RuleExecution contengono gli attributi seguenti:

`eventType`

RuleExecution per i log RuleExecution.

`clientId`

ID del client da cui proviene la richiesta.

`topicName`

Nome dell'argomento sottoscritto.

ruleName

Nome della regola corrispondente.

ruleAction

Il nome dell'operazione attivata.

resources

Raccolta di risorse usate dalle operazioni della regola.

principalId

ID dell'entità principale da cui proviene la richiesta.

### Rule Not Found Logs

Quando il motore di regole AWS IoT non è in grado di trovare una regola con un determinato nome, genera un log di errore RuleNotFound.

[more info \(13\)](#)

Ad esempio:

```
{
 "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"
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log RuleNotFound contengono gli attributi seguenti:

eventType

RuleNotFound per i log di regola non trovata.

clientId

ID del client da cui proviene la richiesta.

topicName

Il nome dell'argomento che è stato pubblicato.

ruleName

Il nome della regola che non è stato possibile trovare.

principalId

ID dell'entità principale da cui proviene la richiesta.

motivo

La stringa "RuleNotFound".

#### details

Una breve spiegazione dell'errore.

### Rule Message Throttled Logs

Quando un messaggio viene sottoposto a throttling, il motore di regole AWS IoT genera un log di errore **RuleMessageThrottled**.

[more info \(14\)](#)

Ad esempio:

```
{
 "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": "Message for Rule example_rule throttled"
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log **RuleMessageThrottled** contengono gli attributi seguenti:

#### eventType

**RuleMessageThrottled** per i log sottoposti al throttling del messaggio della regola.

#### clientId

ID del client da cui proviene la richiesta.

#### topicName

Il nome dell'argomento che è stato pubblicato.

#### ruleName

Nome della regola da attivare.

#### principalId

ID dell'entità principale da cui proviene la richiesta.

#### motivo

La stringa "RuleMessageThrottled".

#### details

Una breve spiegazione dell'errore.

## Log di Jobs

Il servizio AWS IoT Jobs genera log per gli eventi seguenti. I log vengono generati quando viene ricevuta una richiesta MQTT o HTTP dal dispositivo.

## Get Pending Job Execution Logs

Il servizio Jobs AWS IoT genera un log `GetJobExecution` quando riceve una richiesta di esecuzione di un processo.

more info (16)

Ad esempio:

```
{
 "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."
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log GetPendingJobExecution contengono gli attributi seguenti:

eventType

`GetPendingJobExecution` per i log di esecuzione dei processi in attesa.

## protocol

Protocollo usato per effettuare la richiesta. I valori validi sono MOTT e HTTP.

clientId

ID del client da cui proviene la richiesta.

topicName

Nome dell'argomento sottoscritto:

clientToken

Identificatore univoco con distinzione

### **richiesta**

Ulteriori informazioni dal servizio Jobe

10

## Job Execution Logs

Il servizio Jobs AWS IoT

re info (17)

Ad esemp

{

```
"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."
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log `GetJobExecution` contengono gli attributi seguenti:

`eventType`

`DescribeJobExecution` per i log `DescribeJobExecution`.

`protocol`

Protocollo usato per effettuare la richiesta. I valori validi sono `MQTT` e `HTTP`.

`clientId`

ID del client da cui proviene la richiesta.

`jobId`

Job ID per l'esecuzione del processo.

`topicName`

Argomento usato per effettuare la richiesta.

`clientToken`

Identificatore univoco con distinzione tra maiuscole e minuscole per assicurare l'idempotenza della richiesta. Per ulteriori informazioni, consulta [Come assicurare l'idempotenza](#).

`details`

Ulteriori informazioni dal servizio Jobs.

### Update Job Execution Logs

Il servizio Jobs AWS IoT genera un log `UpdateJobExecution` quando riceve una richiesta per aggiornare l'esecuzione di un processo.

[more info \(18\)](#)

Ad esempio:

```
{
 "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."
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log `UpdateJobExecution` contengono gli attributi seguenti:

eventType

UpdateJobExecution per i log UpdateJobExecution.

protocol

Protocollo usato per effettuare la richiesta. I valori validi sono MQTT e HTTP.

clientId

ID del client da cui proviene la richiesta.

jobId

Job ID per l'esecuzione del processo.

topicName

Argomento usato per effettuare la richiesta.

clientToken

Identificatore univoco con distinzione tra maiuscole e minuscole per assicurare l'idempotenza della richiesta. Per ulteriori informazioni, consulta [Come assicurare l'idempotenza](#).

versionNumber

Versione dell'esecuzione del processo.

details

Ulteriori informazioni dal servizio Jobs.

### Start Next Pending Job Execution Logs

Quando riceve una richiesta per avviare la successiva esecuzione in sospeso di un processo, il servizio Jobs AWS IoT genera un log StartNextPendingJobExecution.

[more info \(19\)](#)

Ad esempio:

```
{
 "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."
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log StartNextPendingJobExecution contengono gli attributi seguenti:

eventType

StartNextPendingJobExecution per i log di avvio della successiva esecuzione in sospeso di un processo.

protocol

Protocollo usato per effettuare la richiesta. I valori validi sono MQTT e HTTP.

clientId

ID del client da cui proviene la richiesta.

topicName

Argomento usato per effettuare la richiesta.

clientToken

Identificatore univoco con distinzione tra maiuscole e minuscole per assicurare l'idempotenza della richiesta. Per ulteriori informazioni, consulta [Come assicurare l'idempotenza](#).

details

Ulteriori informazioni dal servizio Jobs.

### Report Final Job Execution Count Logs

Il servizio AWS IoT Jobs genera un log `ReportFinalJobExecutionCount` quando un processo viene completato.

[more info \(20\)](#)

Ad esempio:

```
{
 "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"
}
```

Oltre agli attributi comuni a CloudWatch Logs, le voci del log `ReportFinalJobExecutionCount` contengono gli attributi seguenti:

eventType

`ReportFinalJobExecutionCount` per i log di report del numero finale di esecuzioni di processi.

jobId

Job ID per l'esecuzione del processo.

details

Ulteriori informazioni dal servizio Jobs.

## Visualizzazione dei log

Per visualizzare i log

1. Vai a <https://console.aws.amazon.com/cloudwatch/>. Nel riquadro di navigazione scegli Logs (Log).
2. Nella casella di testo Filtro immettere `AWSIoTLogsV2` e premere Invio.
3. Fai doppio clic sul gruppo di log `AWSIoTLogsV2`.

4. Scegli Search Log Group (Cerca gruppo di log). Verrà visualizzato un elenco completo dei log AWS IoT generati per l'account.
5. Scegli l'icona di espansione per esaminare un singolo flusso.

È possibile anche immettere una query nella casella di testo Filter events (Filtra eventi). Di seguito sono illustrate alcune query interessanti da provare:

- { \$.logLevel = "INFO" }  
Trova tutti i log con livello INFO.
- { \$.status = "Success" }  
Trova tutti i log con stato Success.
- { \$.status = "Success" && \$.eventType = "GetThingShadow" }  
Trova tutti i log con stato Success e un tipo di evento GetThingShadow.

Per ulteriori informazioni sulla creazione di espressioni di filtro, consulta la pagina relativa alle [query CloudWatch Logs](#).

## Registrazione delle chiamate API AWS IoT con AWS CloudTrail

AWS IoT è integrato con AWS CloudTrail, un servizio che offre un record di operazioni effettuate da un utente, un ruolo o un servizio AWS in AWS IoT. CloudTrail acquisisce tutte le chiamate API per AWS IoT come eventi, incluse le chiamate dalla console AWS IoT e dalle chiamate di codice alle API AWS IoT. Se crei un trail, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3 includendo eventi per AWS IoT. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da CloudTrail permettono di determinare la richiesta effettuata a AWS IoT, l'indirizzo IP da cui è stata effettuata la richiesta, l'autore della richiesta, il momento in cui è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni su CloudTrail, consulta [AWS CloudTrail User Guide](#).

## Informazioni di AWS IoT in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività in AWS IoT, questa viene registrata in un evento CloudTrail insieme ad altri eventi di servizio AWS in Event history (Cronologia eventi). È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta [Visualizzazione di eventi mediante la cronologia eventi di CloudTrail](#).

Per una registrazione continua degli eventi nell'account AWS, inclusi gli eventi per AWS IoT, crea un trail. Un trail consente a CloudTrail di fornire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando crei un trail nella console, il trail si applica a tutte le regioni AWS. Il trail registra gli eventi di tutte le regioni AWS nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Puoi configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati raccolti nei log CloudTrail. Per ulteriori informazioni, consulta:

- [Panoramica della creazione di un trail](#)
- [Servizi e integrazioni CloudTrail supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di log CloudTrail da più regioni](#) e [Ricezione di file di log CloudTrail da più account](#)

### Note

Le operazioni relative al piano dei dati AWS IoT (lato dispositivo) non vengono registrate da CloudTrail. Usa CloudWatch per monitorarle.

Le operazioni del piano di controllo AWS IoT vengono registrate da CloudTrail. Le chiamate alle sezioni CreateThing, ListThings e ListTopicRules, ad esempio, generano voci nei file di log di CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente IAM o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#). Le operazioni di AWS IoT sono documentate nelle [informazioni di riferimento sulle API di AWS IoT](#).

## Comprensione delle voci dei file di log di AWS IoT

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail contengono una o più voci di log. Un evento rappresenta una singola richiesta da qualsiasi sorgente e include informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. I file di log di CloudTrail non sono uno stack trace ordinato delle chiamate API pubbliche, pertanto queste non vengono visualizzate in un ordine specifico.

L'esempio seguente mostra una voce di log di CloudTrail che illustra l'operazione `AttachPolicy`.

```
{
 "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":""
}
```

# Risoluzione dei problemi di AWS IoT

Le informazioni seguenti possono risultare utili per risolvere i problemi comuni di AWS IoT.

## Attività

- [Diagnosi dei problemi di connettività \(p. 679\)](#)
- [Diagnosi dei problemi relativi alle regole \(p. 679\)](#)
- [Diagnosi dei problemi relativi a Shadows \(p. 680\)](#)
- [Diagnosi dei problemi relativi alle operazioni del flusso di input Salesforce IoT \(p. 682\)](#)
- [Limiti per AWS IoT \(p. 683\)](#)
- [Errori di AWS IoT \(p. 683\)](#)

## Diagnosi dei problemi di connettività

### Autenticazione

In che modo i dispositivi autenticano gli endpoint di AWS IoT?

Aggiungi il certificato CA di AWS IoT all'archivio di trust del client. Fai riferimento alla documentazione sull'[Autenticazione del server in AWS IoT core](#) e segui i collegamenti per scaricare il certificato CA appropriato.

In che modo è possibile convalidare un certificato configurato correttamente?

Usa il comando `s_client` OpenSSL per testare una connessione all'endpoint di AWS IoT:

```
openssl s_client -connect custom_endpoint.iot.us-east-1.amazonaws.com:8443 -
CAfile CA.pem -cert cert.pem -key privateKey.pem
```

### Autorizzazione

Ho ricevuto una risposta PUBNACK o SUBNACK dal broker. Cosa devo fare?

Assicurati che non ci siano policy collegate al certificato che stai usando per richiamare AWS IoT. Tutte le operazioni di pubblicazione/sottoscrizione vengono bloccate per impostazione predefinita.

## Diagnosi dei problemi relativi alle regole

CloudWatch Logs è lo strumento ideale per il debug dei problemi relativi alle regole. Per ulteriori informazioni sull'utilizzo di CloudWatch Logs con AWS IoT, consulta [Monitoraggio con CloudWatch Logs \(p. 655\)](#). Quando si abilita CloudWatch Logs per AWS IoT, puoi vedere quali regole vengono attivate e il loro esito. Puoi inoltre ottenere informazioni sulla corrispondenza delle condizioni delle clausole WHERE.

La maggior parte dei problemi comuni delle regole riguarda l'autorizzazione. I log mostrano se il ruolo non è autorizzato a eseguire un'operazione AssumeRole sulla risorsa. Di seguito è illustrato un esempio di log generato dal [logging granulare \(p. 659\)](#):

```
{
 "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",
 "ItemKeyValue": "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)"
}

```

Di seguito è illustrato un esempio di log generato dal [logging globale \(p. 657\)](#):

```

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: AKQJ987654321AKQJ987654321AKQJ987654321).
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.

```

Per ulteriori informazioni, consulta [the section called “Visualizzazione dei log” \(p. 675\)](#).

I servizi esterni sono controllati dall'utente finale. Prima dell'esecuzione delle regole, assicurati che i servizi esterni siano configurati con unità di capacità e throughput sufficienti.

## Diagnosi dei problemi relativi a Shadows

### Diagnosi di Shadows

| Problema                                                                                                                                        | Linee guida per la risoluzione dei problemi                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Un documento della copia shadow di un dispositivo viene rifiutato con un messaggio che indica che il documento JSON non è valido.               | Se non hai familiarità con JSON, modifica gli esempi forniti in questa guida per uso personale. Per ulteriori informazioni, consulta <a href="#">Sintassi dei documenti del servizio Device Shadow</a> .                                                             |
| Il codice JSON inviato è corretto, ma non viene archiviato, o viene archiviato solo in parte, nel documento della copia shadow del dispositivo. | Assicurati di rispettare le linee guida di formattazione per JSON. Solo i campi JSON nelle sezioni <code>desired</code> e <code>reported</code> vengono archiviati. I contenuti JSON (anche se formalmente corretti) al di fuori di queste sezioni vengono ignorati. |

| Problema                                                                                                                                                                                                              | Linee guida per la risoluzione dei problemi                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Si è verificato un errore che indica che la copia shadow del dispositivo supera le dimensioni permesse.                                                                                                               | La copia shadow di un dispositivo supporta solo fino a 8 KB di dati. Prova ad accorciare i nomi di campo all'interno del documento JSON o semplicemente crea più copie shadow creando più oggetti. Un dispositivo può avere un numero illimitato di oggetti/copie shadow associate a esso. L'unico requisito è che il nome di ogni oggetto deve essere univoco nell'account.                                                                     |
| Quando si riceve una copia shadow di un dispositivo, le sue dimensioni sono superiori a 8 KB. Come è possibile?                                                                                                       | Al momento della ricezione, il servizio AWS IoT aggiunge metadati alla copia shadow del dispositivo. Il servizio include questi dati nella risposta, che non vengono tuttavia conteggiati per il raggiungimento del limite di 8 KB. Solo i dati per gli stati <code>desired</code> e <code>reported</code> all'interno del documento sullo stato inviato alla copia shadow del dispositivo vengono conteggiati per il raggiungimento del limite. |
| La richiesta è stata rifiutata a causa di una versione errata. Cosa è necessario fare?                                                                                                                                | Esegui un'operazione GET per eseguire la sincronizzazione all'ultima versione del documento sullo stato. Quando usi MQTT, sottoscrivi l'argomento <code>./update/accepted</code> per ricevere la versione più recente del documento JSON e le notifiche sulle modifiche dello stato.                                                                                                                                                             |
| Il timestamp è disattivato per alcuni secondi.                                                                                                                                                                        | Il timestamp per i singoli campi e l'intero documento JSON viene aggiornato quando il documento viene ricevuto dal servizio AWS IoT o quando il documento sullo stato viene pubblicato nei messaggi <code>./update/accepted</code> e <code>./update/delta</code> . I messaggi possono essere ritardati nella rete e in questo caso il timestamp è disattivato per alcuni secondi.                                                                |
| Il dispositivo può pubblicare e sottoscrivere gli argomenti delle copie shadow corrispondenti, ma quando si tenta di aggiornare il documento della copia shadow tramite l'API REST HTTP, si riceve l'errore HTTP 403. | Assicurati di aver creato policy in IAM per le credenziali in uso per l'accesso a questi argomenti e per l'operazione corrispondente (UPDATE/GET/DELETE). Le policy IAM e le policy di certificato sono indipendenti.                                                                                                                                                                                                                            |
| Altri problemi.                                                                                                                                                                                                       | Il servizio Device Shadow registra gli errori in CloudWatch Logs. Per identificare i problemi relativi a dispositivi e configurazione, abilita CloudWatch Logs e visualizza i log relativi alle informazioni di debug.                                                                                                                                                                                                                           |

# Diagnosi dei problemi relativi alle operazioni del flusso di input Salesforce IoT

## Traccia di esecuzione

Come è possibile visualizzare la traccia di esecuzione di un'operazione di Salesforce?

Se CloudWatch Logs non è configurato, consulta la sezione [Monitoraggio con CloudWatch Logs \(p. 655\)](#). Una volta attivati i log, è possibile visualizzare la traccia di esecuzione dell'operazione di Salesforce.

## Esito dell'operazione

Come è possibile controllare che i messaggi siano stati inviati correttamente a un flusso di input Salesforce IoT?

Visualizza i log generati dall'esecuzione dell'operazione di Salesforce in CloudWatch Logs. Se viene visualizzato il messaggio "Action executed successfully", il motore di regole di AWS IoT ha ricevuto conferma da Salesforce IoT della riuscita della trasmissione del messaggio al flusso di input target.

Se si verificano problemi con la piattaforma Salesforce IoT, contatta il supporto di Salesforce IoT.

Cosa è possibile fare se i messaggi non sono stati inviati correttamente a un flusso di input Salesforce IoT?

Visualizza i log generati dall'esecuzione dell'operazione di Salesforce in CloudWatch Logs. A seconda della voce di log, puoi provare le operazioni seguenti:

**Failed to locate the host**

Controlla che il parametro `url` dell'operazione sia corretto e che il flusso di input Salesforce IoT esista.

**Received Internal Server Error from Salesforce**

Riprova. Se il problema persiste, contatta il supporto di Salesforce IoT.

**Received Bad Request Exception from Salesforce**

Controlla se sono presenti errori nel payload inviato.

**Received Unsupported Media Type Exception from Salesforce**

Al momento, Salesforce IoT non supporta un payload binario. Controlla che venga inviato un payload JSON.

**Received Unauthorized Exception from Salesforce**

Controlla che il parametro `token` dell'operazione sia corretto e che il token sia ancora valido.

**Received Not Found Exception from Salesforce**

Controlla che il parametro `url` dell'operazione sia corretto e che il flusso di input Salesforce IoT esista.

Se si verifica un errore non descritto in questa pagina, contatta AWS Support.

## Limiti per AWS IoT

I valori e le informazioni sui limiti di AWS IoT sono forniti nella sezione [Limiti per AWS IoT](#) di Riferimenti generali di Amazon Web Services.

## Errori di AWS IoT

Questa sezione elenca i codici di errore inviati da AWS IoT.

### Codici di errore del broker di messaggi

| Codice di errore | Descrizione dell'errore   |
|------------------|---------------------------|
| 400              | Richiesta non valida.     |
| 401              | Non autorizzato.          |
| 403              | Accesso negato.           |
| 503              | Servizio non disponibile. |

### Codici di errore relativi a identità e sicurezza

| Codice di errore | Descrizione dell'errore |
|------------------|-------------------------|
| 401              | Non autorizzato.        |

### Codici di errore relativi a Device Shadow

| Codice di errore | Descrizione dell'errore                |
|------------------|----------------------------------------|
| 400              | Richiesta non valida.                  |
| 401              | Non autorizzato.                       |
| 403              | Accesso negato.                        |
| 404              | Non trovato.                           |
| 409              | Conflitto.                             |
| 413              | Richiesta di dimensioni troppo grandi. |
| 422              | Impossibile elaborare la richiesta.    |
| 429              | Troppe richieste.                      |
| 500              | Errore interno.                        |
| 503              | Servizio non disponibile.              |

# Comandi IOT

Questo capitolo contiene le sezioni seguenti:

- [AcceptCertificateTransfer \(p. 688\)](#)
- [AddThingToBillingGroup \(p. 689\)](#)
- [AddThingToThingGroup \(p. 690\)](#)
- [AssociateTargetsWithJob \(p. 692\)](#)
- [AttachPolicy \(p. 693\)](#)
- [AttachPrincipalPolicy \(p. 694\)](#)
- [AttachSecurityProfile \(p. 696\)](#)
- [AttachThingPrincipal \(p. 697\)](#)
- [CancelAuditTask \(p. 698\)](#)
- [CancelCertificateTransfer \(p. 699\)](#)
- [CancelJob \(p. 700\)](#)
- [CancelJobExecution \(p. 702\)](#)
- [ClearDefaultAuthorizer \(p. 704\)](#)
- [CreateAuthorizer \(p. 705\)](#)
- [CreateBillingGroup \(p. 706\)](#)
- [CreateCertificateFromCsr \(p. 708\)](#)
- [CreateDynamicThingGroup \(p. 710\)](#)
- [CreateJob \(p. 713\)](#)
- [CreateKeysAndCertificate \(p. 719\)](#)
- [CreateOTAUpdate \(p. 720\)](#)
- [CreatePolicy \(p. 726\)](#)
- [CreatePolicyVersion \(p. 727\)](#)
- [CreateRoleAlias \(p. 729\)](#)
- [CreateScheduledAudit \(p. 731\)](#)
- [CreateSecurityProfile \(p. 733\)](#)
- [CreateStream \(p. 737\)](#)
- [CreateThing \(p. 740\)](#)
- [CreateThingGroup \(p. 742\)](#)
- [CreateThingType \(p. 745\)](#)
- [CreateTopicRule \(p. 747\)](#)
- [DeleteAccountAuditConfiguration \(p. 762\)](#)
- [DeleteAuthorizer \(p. 763\)](#)
- [DeleteBillingGroup \(p. 764\)](#)
- [DeleteCACertificate \(p. 765\)](#)

- [DeleteCertificate \(p. 766\)](#)
- [DeleteDynamicThingGroup \(p. 768\)](#)
- [DeleteJob \(p. 769\)](#)
- [DeleteJobExecution \(p. 770\)](#)
- [DeleteOTAUpdate \(p. 772\)](#)
- [DeletePolicy \(p. 774\)](#)
- [DeletePolicyVersion \(p. 775\)](#)
- [DeleteRegistrationCode \(p. 776\)](#)
- [DeleteRoleAlias \(p. 776\)](#)
- [DeleteScheduledAudit \(p. 777\)](#)
- [DeleteSecurityProfile \(p. 778\)](#)
- [DeleteStream \(p. 779\)](#)
- [DeleteThing \(p. 780\)](#)
- [DeleteThingGroup \(p. 781\)](#)
- [DeleteThingShadow \(p. 782\)](#)
- [DeleteThingType \(p. 784\)](#)
- [DeleteTopicRule \(p. 785\)](#)
- [DeleteV2LogLevel \(p. 786\)](#)
- [DeprecateThingType \(p. 786\)](#)
- [DescribeAccountAuditConfiguration \(p. 788\)](#)
- [DescribeAuditTask \(p. 789\)](#)
- [DescribeAuthorizer \(p. 792\)](#)
- [DescribeBillingGroup \(p. 794\)](#)
- [DescribeCACertificate \(p. 795\)](#)
- [DescribeCertificate \(p. 798\)](#)
- [DescribeDefaultAuthorizer \(p. 800\)](#)
- [DescribeEndpoint \(p. 802\)](#)
- [DescribeEventConfigurations \(p. 803\)](#)
- [DescribeIndex \(p. 804\)](#)
- [DescribeJob \(p. 806\)](#)
- [DescribeJobExecution \(p. 812\)](#)
- [DescribeJobExecution \(p. 815\)](#)
- [DescribeRoleAlias \(p. 818\)](#)
- [DescribeScheduledAudit \(p. 820\)](#)
- [DescribeSecurityProfile \(p. 822\)](#)
- [DescribeStream \(p. 826\)](#)
- [DescribeThing \(p. 828\)](#)
- [DescribeThingGroup \(p. 830\)](#)
- [DescribeThingRegistrationTask \(p. 833\)](#)
- [DescribeThingType \(p. 835\)](#)
- [DetachPolicy \(p. 837\)](#)

- [DetachPrincipalPolicy \(p. 838\)](#)
- [DetachSecurityProfile \(p. 839\)](#)
- [DetachThingPrincipal \(p. 840\)](#)
- [DisableTopicRule \(p. 842\)](#)
- [EnableTopicRule \(p. 842\)](#)
- [GetEffectivePolicies \(p. 843\)](#)
- [GetIndexingConfiguration \(p. 845\)](#)
- [GetJobDocument \(p. 847\)](#)
- [GetLoggingOptions \(p. 848\)](#)
- [GetOTAUpdate \(p. 848\)](#)
- [GetPendingJobExecutions \(p. 854\)](#)
- [GetPolicy \(p. 856\)](#)
- [GetPolicyVersion \(p. 858\)](#)
- [GetRegistrationCode \(p. 859\)](#)
- [GetStatistics \(p. 860\)](#)
- [GetThingShadow \(p. 862\)](#)
- [GetTopicRule \(p. 863\)](#)
- [GetV2LoggingOptions \(p. 878\)](#)
- [ListActiveViolations \(p. 879\)](#)
- [ListAttachedPolicies \(p. 884\)](#)
- [ListAuditFindings \(p. 886\)](#)
- [ListAuditTasks \(p. 891\)](#)
- [ListAuthorizers \(p. 894\)](#)
- [ListBillingGroups \(p. 895\)](#)
- [ListCACertificates \(p. 897\)](#)
- [ListCertificates \(p. 899\)](#)
- [ListCertificatesByCA \(p. 901\)](#)
- [ListIndices \(p. 903\)](#)
- [ListJobExecutionsForJob \(p. 904\)](#)
- [ListJobExecutionsForThing \(p. 906\)](#)
- [ListJobs \(p. 909\)](#)
- [ListOTAUpdates \(p. 912\)](#)
- [ListOutgoingCertificates \(p. 914\)](#)
- [ListPolicies \(p. 916\)](#)
- [ListPolicyPrincipals \(p. 917\)](#)
- [ListPolicyVersions \(p. 919\)](#)
- [ListPrincipalPolicies \(p. 920\)](#)
- [ListPrincipalThings \(p. 922\)](#)
- [ListRoleAliases \(p. 923\)](#)
- [ListScheduledAudits \(p. 925\)](#)
- [ListSecurityProfiles \(p. 927\)](#)

- [ListSecurityProfilesForTarget \(p. 928\)](#)
- [ListStreams \(p. 930\)](#)
- [ListTagsForResource \(p. 932\)](#)
- [ListTargetsForPolicy \(p. 933\)](#)
- [ListTargetsForSecurityProfile \(p. 934\)](#)
- [ListThingGroups \(p. 936\)](#)
- [ListThingGroupsForThing \(p. 938\)](#)
- [ListThingPrincipals \(p. 939\)](#)
- [ListThingRegistrationTaskReports \(p. 940\)](#)
- [ListThingRegistrationTasks \(p. 942\)](#)
- [ListThingTypes \(p. 943\)](#)
- [ListThings \(p. 946\)](#)
- [ListThingsInBillingGroup \(p. 948\)](#)
- [ListThingsInThingGroup \(p. 949\)](#)
- [ListTopicRules \(p. 951\)](#)
- [ListV2LoggingLevels \(p. 952\)](#)
- [ListViolationEvents \(p. 954\)](#)
- [Publish \(p. 959\)](#)
- [RegisterCACertificate \(p. 960\)](#)
- [RegisterCertificate \(p. 962\)](#)
- [RegisterThing \(p. 964\)](#)
- [RejectCertificateTransfer \(p. 965\)](#)
- [RemoveThingFromBillingGroup \(p. 966\)](#)
- [RemoveThingFromThingGroup \(p. 967\)](#)
- [ReplaceTopicRule \(p. 969\)](#)
- [SearchIndex \(p. 983\)](#)
- [SetDefaultAuthorizer \(p. 987\)](#)
- [SetDefaultPolicyVersion \(p. 988\)](#)
- [SetLoggingOptions \(p. 989\)](#)
- [SetV2LogLevel \(p. 990\)](#)
- [SetV2LoggingOptions \(p. 991\)](#)
- [StartNextPendingJobExecution \(p. 992\)](#)
- [StartOnDemandAuditTask \(p. 995\)](#)
- [StartThingRegistrationTask \(p. 997\)](#)
- [StopThingRegistrationTask \(p. 998\)](#)
- [TagResource \(p. 999\)](#)
- [TestAuthorization \(p. 1000\)](#)
- [TestInvokeAuthorizer \(p. 1004\)](#)
- [TransferCertificate \(p. 1006\)](#)
- [UntagResource \(p. 1007\)](#)
- [UpdateAccountAuditConfiguration \(p. 1008\)](#)

- [UpdateAuthorizer \(p. 1010\)](#)
- [UpdateBillingGroup \(p. 1012\)](#)
- [UpdateCACertificate \(p. 1014\)](#)
- [UpdateCertificate \(p. 1015\)](#)
- [UpdateDynamicThingGroup \(p. 1017\)](#)
- [UpdateEventConfigurations \(p. 1019\)](#)
- [UpdateIndexingConfiguration \(p. 1020\)](#)
- [UpdateJob \(p. 1022\)](#)
- [UpdateJobExecution \(p. 1026\)](#)
- [UpdateRoleAlias \(p. 1030\)](#)
- [UpdateScheduledAudit \(p. 1031\)](#)
- [UpdateSecurityProfile \(p. 1033\)](#)
- [UpdateStream \(p. 1041\)](#)
- [UpdateThing \(p. 1043\)](#)
- [UpdateThingGroup \(p. 1046\)](#)
- [UpdateThingGroupsForThing \(p. 1048\)](#)
- [UpdateThingShadow \(p. 1049\)](#)
- [ValidateSecurityProfileBehaviors \(p. 1050\)](#)

## AcceptCertificateTransfer

Accetta il trasferimento di un certificato in sospeso. Lo stato predefinito del certificato è INACTIVE.

Per verificare i trasferimenti di certificati in sospeso, chiama ListCertificates per enumerare i certificati.

Riepilogo

```
aws iot accept-certificate-transfer \
--certificate-id <value> \
[--set-as-active | --no-set-as-active] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "certificateId": "string",
 "setAsActive": "boolean"
}
```

Campi di `cli-input-json`

| Nome          | Tipo    | Descrizione                                                                                                           |
|---------------|---------|-----------------------------------------------------------------------------------------------------------------------|
| certificateId | Stringa | ID del certificato. L'ultima parte dell'ARN del certificato contiene l'ID certificato.<br>Lunghezza max: 64, min.: 64 |

| Nome        | Tipo                         | Descrizione                           |
|-------------|------------------------------|---------------------------------------|
|             | Modello: (0x)?[a-f A-F 0-9]+ |                                       |
| setAsActive | booleano                     | Specifica se il certificato è attivo. |

#### Output

Nessuna

#### Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**TransferAlreadyCompletedException**

Non puoi annullare il trasferimento del certificato perché è già stato completato.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## AddThingToBillingGroup

Aggiunge un oggetto a un gruppo di fatturazione.

#### Riepilogo

```
aws iot add-thing-to-billing-group \
[--billing-group-name <value>] \
[--billing-group-arn <value>] \
[--thing-name <value>] \
[--thing-arn <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "billingGroupName": "string",
```

```
 "billingGroupArn": "string",
 "thingName": "string",
 "thingArn": "string"
}
```

#### Campi di **cli-input-json**

| Nome             | Tipo    | Descrizione                                                                                                                 |
|------------------|---------|-----------------------------------------------------------------------------------------------------------------------------|
| billingGroupName | Stringa | Il nome del gruppo di fatturazione.<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+                           |
| billingGroupArn  | Stringa | L'ARN del gruppo di fatturazione.                                                                                           |
| thingName        | Stringa | Il nome dell'oggetto da aggiungere al gruppo di fatturazione.<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+ |
| thingArn         | Stringa | L'ARN dell'oggetto da aggiungere al gruppo di fatturazione.                                                                 |

#### Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ResourceNotFoundException**

La risorsa specificata non esiste.

## AddThingToThingGroup

Aggiunge un oggetto a un gruppo di oggetti.

Riepilogo

```
aws iot add-thing-to-thing-group \
[--thing-group-name <value>] \
[--thing-group-arn <value>] \
```

```
[--thing-name <value>] \
[--thing-arn <value>] \
[--override-dynamic-groups | --no-override-dynamic-groups] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "thingGroupName": "string",
 "thingGroupArn": "string",
 "thingName": "string",
 "thingArn": "string",
 "overrideDynamicGroups": "boolean"
}
```

#### Campi di cli-input-json

| Nome                  | Tipo                                                                  | Descrizione                                                                                                                                                                                                                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingGroupName        | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del gruppo cui stai aggiungendo un oggetto.                                                                                                                                                                                                                                                                                  |
| thingGroupArn         | Stringa                                                               | ARN del gruppo cui stai aggiungendo un oggetto.                                                                                                                                                                                                                                                                                   |
| thingName             | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto da aggiungere a un gruppo.                                                                                                                                                                                                                                                                                      |
| thingArn              | Stringa                                                               | ARN dell'oggetto da aggiungere a un gruppo.                                                                                                                                                                                                                                                                                       |
| overrideDynamicGroups | boolean                                                               | Sostituisce i gruppi di oggetti dinamici con gruppi di oggetti statici quando viene raggiunto il limite di 10 oggetti per gruppo. Se un oggetto appartiene a gruppi di 10 oggetti e uno o più gruppi sono gruppi di oggetti dinamici, l'aggiunta di un oggetto a un gruppo statico rimuove l'oggetto dall'ultimo gruppo dinamico. |

#### Output

Nessuna

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

#### ThrottlingException

La velocità supera il limite.

#### InternalFailureException

Si è verificato un errore imprevisto.

#### ResourceNotFoundException

La risorsa specificata non esiste.

## AssociateTargetsWithJob

Associa un gruppo a un processo continuo. Devono essere soddisfatti i criteri seguenti:

- Il processo deve essere stato creato con il campo targetSelection impostato su "CONTINUOUS".
- Lo stato del processo deve essere "IN\_PROGRESS".
- Il numero totale di target associati a un processo non deve essere superiore a 100.

#### Riepilogo

```
aws iot associate-targets-with-job \
 --targets <value> \
 --job-id <value> \
 [--comment <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "targets": [
 "string"
],
 "jobId": "string",
 "comment": "string"
}
```

#### Campi di cli-input-json

| Nome    | Tipo                                                             | Descrizione                                                                                             |
|---------|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| targets | elenco<br>Membro: TargetArn                                      | Elenco di ARN dei gruppi di oggetti che definiscono i target del processo.                              |
| jobId   | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a-zA-Z0-9_-]+ | Identificatore univoco assegnato al processo al momento della creazione.                                |
| comment | Stringa<br>Lunghezza max: 2028<br>Modello: [^\p{C}]+             | Stringa di commento facoltativa che descrive il motivo per cui il processo è stato associato ai target. |

## Output

```
{
 "jobArn": "string",
 "jobId": "string",
 "description": "string"
}
```

## Campi di output dell'interfaccia a riga di comando

| Nome        | Tipo                                                                       | Descrizione                                                              |
|-------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------|
| jobArn      | Stringa                                                                    | ARN che identifica il processo.                                          |
| jobId       | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+ | Identificatore univoco assegnato al processo al momento della creazione. |
| description | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+               | Breve descrizione di testo del processo.                                 |

## Errori

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ResourceNotFoundException

La risorsa specificata non esiste.

### LimitExceededException

È stato superato un limite.

### ThrottlingException

La velocità supera il limite.

### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

# AttachPolicy

Collega una policy al target specificato.

## Riepilogo

```
aws iot attach-policy \
 --policy-name <value> \
 --target <value> \
 [--cli-input-json <value>] \

```

```
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "policyName": "string",
 "target": "string"
}
```

Campi di **cli-input-json**

| Nome       | Tipo                                                                  | Descrizione                                              |
|------------|-----------------------------------------------------------------------|----------------------------------------------------------|
| policyName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+ | Nome della policy da collegare.                          |
| target     | Stringa                                                               | L' <a href="#">identità</a> a cui è collegata la policy. |

Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

**LimitExceededException**

È stato superato un limite.

## AttachPrincipalPolicy

Collega la policy indicata all'entità principale specificata (certificato o altra credenziale).

Nota: questa API è obsoleta. Usa invece AttachPolicy.

### Riepilogo

```
aws iot attach-principal-policy \
--policy-name <value> \
--principal <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di **cli-input-json**

```
{
 "policyName": "string",
 "principal": "string"
}
```

### Campi di **cli-input-json**

| Nome       | Tipo                                                                  | Descrizione                                                                                                                               |
|------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| policyName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+ | Nome della policy.                                                                                                                        |
| principal  | Stringa                                                               | Entità principale, che può essere l'ARN di un certificato (restituito dall'operazione CreateCertificate) o un'identità di Amazon Cognito. |

### Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

#### LimitExceededException

È stato superato un limite.

## AttachSecurityProfile

Associa un profilo di sicurezza di Device Defender a un gruppo di oggetti o all'account. Ogni gruppo di oggetti o account può avere fino a cinque profili di sicurezza associati.

#### Riepilogo

```
aws iot attach-security-profile \
--security-profile-name <value> \
--security-profile-target-arn <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "securityProfileName": "string",
 "securityProfileTargetArn": "string"
}
```

#### Campi di cli-input-json

| Nome                     | Tipo    | Descrizione                                                                                           |
|--------------------------|---------|-------------------------------------------------------------------------------------------------------|
| securityProfileName      | Stringa | Profilo di sicurezza collegato.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ |
| securityProfileTargetArn | Stringa | ARN del target (gruppo di oggetti) a cui è collegato il profilo di sicurezza.                         |

#### Output

Nessuna

Errori

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### ResourceNotFoundException

La risorsa specificata non esiste.

#### LimitExceededException

È stato superato un limite.

#### VersionConflictException

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## AttachThingPrincipal

Collega l'entità principale indicata all'oggetto specificato. Un principale può essere certificati X.509, utenti IAM, gruppi e ruoli, identità Amazon Cognito o identità federate.

Riepilogo

```
aws iot attach-thing-principal \
 --thing-name <value> \
 --principal <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "thingName": "string",
 "principal": "string"
}
```

Campi di **cli-input-json**

| Nome      | Tipo    | Descrizione                                                                              |
|-----------|---------|------------------------------------------------------------------------------------------|
| thingName | Stringa | Nome dell'oggetto.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ |
| principal | Stringa | Entità principale, ad esempio un certificato o un'altra credenziale.                     |

Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## CancelAuditTask

Annulla un audit in corso. L'audit può essere pianificato o on demand. Se l'audit non è in corso, viene generata un'eccezione "InvalidRequestException".

### Riepilogo

```
aws iot cancel-audit-task \
--task-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "taskId": "string"
}
```

### Campi di **cli-input-json**

| Nome   | Tipo                                                                       | Descrizione                                                                              |
|--------|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| taskId | Stringa<br><br>Lunghezza max: 40, min.: 1<br><br>Modello: [a-z A-Z 0-9 -]+ | ID dell'audit da annullare. È possibile annullare solo un audit con stato "IN_PROGRESS". |

### Output

Nessuna

### Errori

#### ResourceNotFoundException

La risorsa specificata non esiste.

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### ThrottlingException

La velocità supera il limite.

#### InternalFailureException

Si è verificato un errore imprevisto.

## CancelCertificateTransfer

Annulla un trasferimento in sospeso per il certificato specificato.

Nota Solo l'account di origine del trasferimento può usare questa operazione per annullare un trasferimento. Le destinazioni del trasferimento possono usare invece RejectCertificateTransfer. Dopo il trasferimento, AWS IoT restituisce il certificato all'account di origine con stato INACTIVE. Dopo che l'account di destinazione ha accettato il trasferimento, il trasferimento non può essere annullato.

Dopo l'annullamento di un trasferimento del certificato, lo stato del certificato cambia da PENDING\_TRANSFER a INACTIVE.

#### Riepilogo

```
aws iot cancel-certificate-transfer \
 --certificate-id <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "certificateId": "string"
}
```

#### Campi di **cli-input-json**

| Nome          | Tipo                                                                           | Descrizione                                                                            |
|---------------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| certificateId | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato. L'ultima parte dell'ARN del certificato contiene l'ID certificato. |

#### Output

Nessuna

Errori

#### ResourceNotFoundException

La risorsa specificata non esiste.

#### TransferAlreadyCompletedException

Non puoi annullare il trasferimento del certificato perché è già stato completato.

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### ThrottlingException

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## CancelJob

Annulla un processo.

### Riepilogo

```
aws iot cancel-job \
 --job-id <value> \
 [--reason-code <value>] \
 [--comment <value>] \
 [--force | --no-force] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "jobId": "string",
 "reasonCode": "string",
 "comment": "string",
 "force": "boolean"
}
```

### Campi di cli-input-json

| Nome       | Tipo                                                                | Descrizione                                                                                   |
|------------|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| jobId      | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+ | Identificatore univoco assegnato al processo al momento della creazione.                      |
| reasonCode | Stringa<br>Lunghezza max: 128<br>Modello: [\p{Upper} \p{Digit}_]+   | (Opzionale) Una stringa di codice motivo che spiega perché il processo è stato annullato.     |
| comment    | Stringa<br>Lunghezza max: 2028<br>Modello: [^\p{C}]+                | Stringa di commento facoltativa che descrive il motivo per cui il processo è stato annullato. |

| Nome  | Tipo     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| force | booleano | <p>(Opzionale) Se <code>true</code>, vengono annullate le esecuzioni dei processi con stato "IN_PROGRESS" e "QUEUED"; altrimenti vengono annullate solo le esecuzioni dei processi con stato "QUEUED". Il valore di default è <code>false</code>.</p> <p>L'annullamento di un processo "IN_PROGRESS" impedirà al dispositivo in cui è in esecuzione il processo di aggiornarne lo stato di esecuzione. Prestare attenzione e verificare che tutti i dispositivi in cui sono in esecuzione processi annullati siano in grado di effettuare il ripristino a uno stato valido.</p> |

#### Output

```
{
 "jobArn": "string",
 "jobId": "string",
 "description": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome        | Tipo                                                                        | Descrizione                                                              |
|-------------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------|
| jobArn      | Stringa                                                                     | ARN del processo.                                                        |
| jobId       | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Identificatore univoco assegnato al processo al momento della creazione. |
| description | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+                | Breve descrizione di testo del processo.                                 |

#### Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceNotFoundException`

La risorsa specificata non esiste.

#### ThrottlingException

La velocità supera il limite.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

## CancelJobExecution

Annulla l'esecuzione di un processo per un determinato oggetto.

### Riepilogo

```
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]
```

### Formato di cli-input-json

```
{
 "jobId": "string",
 "thingName": "string",
 "force": "boolean",
 "expectedVersion": "long",
 "statusDetails": {
 "string": "string"
 }
}
```

### Campi di cli-input-json

| Nome      | Tipo     | Descrizione                                                                                                                                                                                                                                       |
|-----------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId     | Stringa  | L'ID del processo da annullare.<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+                                                                                                                                               |
| thingName | Stringa  | Il nome dell'oggetto di cui verrà annullata l'esecuzione del processo.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+                                                                                                      |
| force     | booleano | (Opzionale) Se true, verrà annullata l'esecuzione del processo se lo stato è IN_PROGRESS o QUEUED; altrimenti l'esecuzione del processo verrà annullata solo se lo stato è QUEUED. Se si tenta di annullare l'esecuzione di un processo con stato |

| Nome            | Tipo  | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |       | <p>IN_PROGRESS e non si imposta force su true, verrà generata un'eccezione <code>InvalidStateTransitionException</code>. Il valore di default è false.</p> <p>L'annullamento dell'esecuzione di un processo "IN_PROGRESS" impedirà al dispositivo di aggiornarne lo stato di esecuzione. Prestare attenzione e verificare che il dispositivo sia in grado di effettuare il ripristino a uno stato valido.</p>                                                                                                                                                                                                               |
| expectedVersion | Long  | <p>(Opzionale) Versione corrente prevista dell'esecuzione del processo. Ogni volta che aggiorni l'esecuzione del processo, la versione viene incrementata. Se la versione dell'esecuzione del processo archiviata in Jobs non corrisponde, l'aggiornamento viene rifiutato con errore <code>VersionMismatch</code> e viene restituita una risposta <code>ErrorResponse</code> che contiene i dati sullo stato di esecuzione del processo corrente. Questo comportamento rende superfluo eseguire una richiesta <code>DescribeJobExecution</code> separata per ottenere i dati sullo stato dell'esecuzione del processo.</p> |
| statusDetails   | mappa | <p>Raccolta di coppie nome/valore che descrivono lo stato dell'esecuzione del processo. Se non è specificato, <code>statusDetails</code> resta invariato. È possibile specificare al massimo 10 coppie nome/valore.</p>                                                                                                                                                                                                                                                                                                                                                                                                     |

## Output

Nessuna

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`InvalidStateTransitionException`

Un aggiornamento ha tentato di modificare l'esecuzione del processo impostando uno stato non valido in base allo stato corrente dell'esecuzione del processo (ad esempio, un tentativo di modificare

una richiesta con stato SUCCESS impostando lo stato IN\_PROGRESS). In questo caso, il corpo del messaggio di errore contiene anche il campo executionState.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**VersionConflictException**

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

## ClearDefaultAuthorizer

Cancella l'autorizzazione predefinita.

Riepilogo

```
aws iot clear-default-authorizer \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di cli-input-json

```
{
}
```

Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

# CreateAuthorizer

Crea un'autorizzazione.

Riepilogo

```
aws iot create-authorizer \
--authorizer-name <value> \
--authorizer-function-arn <value> \
--token-key-name <value> \
--token-signing-public-keys <value> \
[--status <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "authorizerName": "string",
 "authorizerFunctionArn": "string",
 "tokenKeyName": "string",
 "tokenSigningPublicKeys": {
 "string": "string"
 },
 "status": "string"
}
```

Campi di **cli-input-json**

| Nome                   | Tipo    | Descrizione                                                                                                                                           |
|------------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| authorizerName         | Stringa | Nome dell'autorizzazione.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=,@-]+                                                                 |
| authorizerFunctionArn  | Stringa | ARN della funzione Lambda dell'autorizzazione.                                                                                                        |
| tokenKeyName           | Stringa | Nome della chiave del token usata per estrarre il token dalle intestazioni HTTP.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ |
| tokenSigningPublicKeys | mappa   | Chiavi pubbliche usate per verificare la firma digitale restituita dal servizio di autenticazione personalizzato.                                     |
| status                 | Stringa | Stato della richiesta di creazione dell'autorizzazione.<br><br>Enumerazione: ACTIVE   INACTIVE                                                        |

Output

```
{
 "authorizerName": "string",
 "authorizerArn": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo    | Descrizione                                                                   |
|----------------|---------|-------------------------------------------------------------------------------|
| authorizerName | Stringa | Nome dell'autorizzazione.<br>Lunghezza max: 128, min.: 1<br>Modello: [w=,@-]+ |
| authorizerArn  | Stringa | ARN dell'autorizzazione.                                                      |

Errori

**ResourceAlreadyExistsException**

La risorsa esiste già.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**LimitExceededException**

È stato superato un limite.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## CreateBillingGroup

Crea un gruppo di fatturazione.

Riepilogo

```
aws iot create-billing-group \
 --billing-group-name <value> \
 [--billing-group-properties <value>] \
 [--tags <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di cli-input-json

```
{
 "billingGroupName": "string",
 "billingGroupProperties": {
 "billingGroupDescription": "string"
 },
 "tags": [
 {
 "Key": "string",
 "Value": "string"
 }
]
}
```

#### Campi di **cli-input-json**

| Nome                    | Tipo                                                                  | Descrizione                                                       |
|-------------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------|
| billingGroupName        | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome da assegnare al gruppo di fatturazione.                      |
| billingGroupProperties  | BillingGroupProperties                                                | Le proprietà del gruppo di fatturazione.                          |
| billingGroupDescription | Stringa<br>Lunghezza max: 2028<br>Modello: [\p{Graph}]*               | La descrizione del gruppo di fatturazione.                        |
| tags                    | elenco<br>member: Tag<br>Classe Java: java.util.List                  | Metadati utilizzabili per la gestione del gruppo di fatturazione. |
| Chiave                  | Stringa                                                               | La chiave del tag.                                                |
| Valore                  | Stringa                                                               | Il valore del tag.                                                |

#### Output

```
{
 "billingGroupName": "string",
 "billingGroupArn": "string",
 "billingGroupId": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome             | Tipo                                                                  | Descrizione                                  |
|------------------|-----------------------------------------------------------------------|----------------------------------------------|
| billingGroupName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Il nome assegnato al gruppo di fatturazione. |

| Nome            | Tipo    | Descrizione                                                                                      |
|-----------------|---------|--------------------------------------------------------------------------------------------------|
| billingGroupArn | Stringa | L'ARN del gruppo di fatturazione.                                                                |
| billingGroupId  | Stringa | L'ID del gruppo di fatturazione.<br><br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 -]+ |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ResourceAlreadyExistsException`

La risorsa esiste già.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

## CreateCertificateFromCsr

Crea un certificato X.509 usando la richiesta di firma del certificato specificata.

Nota: la richiesta di firma del certificato deve includere una chiave pubblica che sia una chiave RSA con lunghezza di almeno 2048 bit o una chiave ECC da curva NIST P-256 o NIST P-384.

Nota: il riutilizzo della stessa richiesta di firma del certificato restituisce un certificato distinto.

Puoi creare più certificati in un batch creando una directory, copiando più file CSR nella directory e quindi specificando la directory nella riga di comando. I comandi seguenti mostrano come creare un batch di certificati a partire da un batch di richieste di firma del certificato.

Presupponendo che un set di richieste di firma del certificato si trovi all'interno della directory my-csr-directory:

Su Linux e OS X il comando è il seguente:

```
$ ls my-csr-directory/ | xargs -I aws iot create-certificate-from-csr --certificate-signing-request file://my-csr-directory/
```

Questo comando elenca tutte le richieste di firma del certificato in my-csr-directory e invia in modalità pipeline ogni nome di file CSR al comando aws iot create-certificate-from-csr dell'interfaccia a riga di comando AWS per creare un certificato per la richiesta di firma del certificato corrispondente.

La parte aws iot create-certificate-from-csr del comando può essere eseguita anche in parallelo per accelerare il processo di creazione del certificato:

```
$ ls my-csr-directory/ | xargs -P 10 -I aws iot create-certificate-from-csr --certificate-signing-request file://my-csr-directory/
```

In Windows PowerShell il comando per creare certificati per tutte le richieste di firma del certificato in my-csr-directory è il seguente:

```
> ls -Name my-csr-directory | % aws iot create-certificate-from-csr --certificate-signing-request file://my-csr-directory/$_
```

In un prompt de comandi di Windows il comando per creare certificati per tutte le richieste di firma del certificato in my-csr-directory è il seguente:

```
> forfiles /p my-csr-directory /c "cmd /c aws iot create-certificate-from-csr --certificate-signing-request file://@path"
```

#### Riepilogo

```
aws iot create-certificate-from-csr \
--certificate-signing-request <value> \
[--set-as-active | --no-set-as-active] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "certificateSigningRequest": "string",
 "setAsActive": "boolean"
}
```

#### Campi di **cli-input-json**

| Nome                      | Tipo     | Descrizione                                              |
|---------------------------|----------|----------------------------------------------------------|
| certificateSigningRequest | Stringa  | Richiesta di firma del certificato.<br>Lunghezza min.: 1 |
| setAsActive               | booleano | Specifica se il certificato è attivo.                    |

#### Output

```
{
 "certificateArn": "string",
 "certificateId": "string",
 "certificatePem": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo    | Descrizione                                                                                                                                                             |
|----------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| certificateArn | Stringa | ARN (Amazon Resource Name) del certificato. Puoi usare l'ARN come entità principale per le operazioni delle policy.                                                     |
| certificateId  | Stringa | ID del certificato. Le operazioni di gestione dei certificati accettano solo un parametro certificateId.<br>Lunghezza max: 64, min.: 64<br>Modello: (0x)?[a-f A-F 0-9]+ |
| certificatePem | Stringa | Dati del certificato, in formato PEM.                                                                                                                                   |

| Nome | Tipo                          | Descrizione |
|------|-------------------------------|-------------|
|      | Lunghezza max: 65536, min.: 1 |             |

#### Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## CreateDynamicThingGroup

Crea un gruppo di oggetti dinamico.

#### Riepilogo

```
aws iot create-dynamic-thing-group \
--thing-group-name <value> \
[--thing-group-properties <value>] \
[--index-name <value>] \
--query-string <value> \
[--query-version <value>] \
[--tags <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "thingGroupName": "string",
 "thingGroupProperties": {
 "thingGroupDescription": "string",
 "attributePayload": {
 "attributes": {
 "string": "string"
 },
 "merge": "boolean"
 }
 },
 "indexName": "string",
 "queryString": "string",
 "queryVersion": "string",
 "tags": [
 {
 "Key": "string",
 "Value": "string"
 }
]
}
```

```
]
}
```

### Campi di **cli-input-json**

| Nome                  | Tipo                                                                  | Descrizione                                                                                                                                                                                                                                                                                                                                |
|-----------------------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingGroupName        | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Il nome del gruppo di oggetti dinamico da creare.                                                                                                                                                                                                                                                                                          |
| thingGroupProperties  | ThingGroupProperties                                                  | Le proprietà del gruppo di oggetti dinamico.                                                                                                                                                                                                                                                                                               |
| thingGroupDescription | Stringa<br>Lunghezza max: 2028<br>Modello: [\p{Graph}]*               | Descrizione del gruppo di oggetti.                                                                                                                                                                                                                                                                                                         |
| attributePayload      | AttributePayload                                                      | Attributi del gruppo di oggetti in formato JSON.                                                                                                                                                                                                                                                                                           |
| attributes            | mappa                                                                 | Stringa JSON contenente fino a tre coppie chiave/valore in formato JSON. Ad esempio:<br><br><code>\"attributes\":<br/>{\\"string1\\":<br/>\"string2\\\"}</code>                                                                                                                                                                            |
| merge                 | booleano                                                              | Specifica se l'elenco di attributi fornito in AttributePayload deve essere unito agli attributi archiviati nel registro, anziché sovrascrivere questi ultimi.<br><br>Per rimuovere un attributo, chiama UpdateThing con un valore di attributo vuoto.<br><br><b>Note</b><br><br>L'attributo merge è valido solo quando chiavi UpdateThing. |
| indexName             | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Il nome d'indice del gruppo di oggetti dinamico.<br><br><b>Note</b><br><br>Attualmente è supportato un indice: "AWS_Things".                                                                                                                                                                                                               |
| queryString           | Stringa                                                               | La stringa di query per la ricerca del gruppo di oggetti dinamico.                                                                                                                                                                                                                                                                         |

| Nome         | Tipo                                                 | Descrizione                                                                                                                                                                                                                                          |
|--------------|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | Lunghezza min.: 1                                    | Consulta la sezione <a href="#">Sintassi di query</a> per informazioni sulla sintassi delle stringhe di query.                                                                                                                                       |
| queryVersion | Stringa                                              | <p>La versione di query del gruppo di oggetti dinamico.</p> <p><b>Note</b></p> <p>Attualmente è supportata una versione di query: "2017-09-30". Se non viene specificata, la versione di query è impostata in modo predefinito su questo valore.</p> |
| tags         | elenco<br>member: Tag<br>Classe Java: java.util.List | Metadati utilizzabili per la gestione del gruppo di oggetti dinamico.                                                                                                                                                                                |
| Chiave       | Stringa                                              | La chiave del tag.                                                                                                                                                                                                                                   |
| Valore       | Stringa                                              | Il valore del tag.                                                                                                                                                                                                                                   |

#### Output

```
{
 "thingGroupName": "string",
 "thingGroupArn": "string",
 "thingGroupId": "string",
 "indexName": "string",
 "queryString": "string",
 "queryVersion": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo                                                                  | Descrizione                             |
|----------------|-----------------------------------------------------------------------|-----------------------------------------|
| thingGroupName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Il nome del gruppo di oggetti dinamico. |
| thingGroupArn  | Stringa                                                               | L'ARN del gruppo di oggetti dinamico.   |
| thingGroupId   | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :-]+  | L'ID del gruppo di oggetti dinamico.    |

| Nome         | Tipo                                                                  | Descrizione                                                        |
|--------------|-----------------------------------------------------------------------|--------------------------------------------------------------------|
| indexName    | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+ | Il nome d'indice del gruppo di oggetti dinamico.                   |
| queryString  | Stringa<br>Lunghezza min.: 1                                          | La stringa di query per la ricerca del gruppo di oggetti dinamico. |
| queryVersion | Stringa                                                               | La versione di query del gruppo di oggetti dinamico.               |

#### Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceAlreadyExistsException**

La risorsa esiste già.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

**InvalidQueryException**

La query non è valida.

**LimitExceededException**

È stato superato un limite.

## CreateJob

Crea un processo.

#### Riepilogo

```
aws iot create-job \
--job-id <value> \
--targets <value> \
[--document-source <value>] \
[--document <value>] \
[--description <value>] \
[--presigned-url-config <value>] \
[--target-selection <value>] \
[--job-executions-rollout-config <value>] \
[--abort-config <value>]
```

```
[--timeout-config <value>] \
[--tags <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "jobId": "string",
 "targets": [
 "string"
],
 "documentSource": "string",
 "document": "string",
 "description": "string",
 "presignedUrlConfig": {
 "roleArn": "string",
 "expiresInSec": "long"
 },
 "targetSelection": "string",
 "jobExecutionsRolloutConfig": {
 "maximumPerMinute": "integer",
 "exponentialRate": {
 "baseRatePerMinute": "integer",
 "incrementFactor": "double",
 "rateIncreaseCriteria": {
 "numberOfNotifiedThings": "integer",
 "numberOfSucceededThings": "integer"
 }
 }
 },
 "abortConfig": {
 "criteriaList": [
 {
 "failureType": "string",
 "action": "string",
 "thresholdPercentage": "double",
 "minNumberOfExecutedThings": "integer"
 }
]
 },
 "timeoutConfig": {
 "inProgressTimeoutInMinutes": "long"
 },
 "tags": [
 {
 "Key": "string",
 "Value": "string"
 }
]
}
```

#### Campi di cli-input-json

| Nome  | Tipo                                                                        | Descrizione                                                                                                                                                                      |
|-------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Identificatore del processo, che deve essere univoco per l'account AWS. È consigliabile usare un UUID. I caratteri alfanumerici, "-" e "_" sono i caratteri validi da usare qui. |

| Nome               | Tipo                                                 | Descrizione                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| targets            | elenco<br>Membro: TargetArn                          | Elenco di oggetti e gruppi di oggetti cui deve essere inviato il processo.                                                                                                                                                                                                                                                                                                                                |
| documentSource     | Stringa<br>Lunghezza max: 1350, min.: 1              | Collegamento S3 al documento del processo.                                                                                                                                                                                                                                                                                                                                                                |
| document           | Stringa<br>Lunghezza max: 32768                      | Documento del processo.<br><br><b>Note</b><br><br>Se il documento si trova in un bucket S3, devi utilizzare un collegamento segnaposto quando specifichi il documento. Il collegamento segnaposto ha il formato seguente:<br><code>\$ aws:iot:s3-presigned-url:https://s3.amazonaws.com/bucket/key</code><br>dove bucket è il nome del bucket e key è l'oggetto nel bucket a cui rimanda il collegamento. |
| description        | Stringa<br>Lunghezza max: 2028<br>Modello: [^\p{C}]+ | Breve descrizione di testo del processo.                                                                                                                                                                                                                                                                                                                                                                  |
| presignedUrlConfig | PresignedUrlConfig                                   | Informazioni di configurazione per URL S3 prefirmati.                                                                                                                                                                                                                                                                                                                                                     |
| roleArn            | Stringa<br>Lunghezza max: 2048, min.: 20             | L'ARN di un ruolo IAM che concede l'autorizzazione per scaricare file dal bucket S3 in cui vengono archiviati i dati e gli aggiornamenti del processo. Il ruolo deve anche concedere l'autorizzazione per IoT per il download dei file.                                                                                                                                                                   |

| Nome                       | Tipo                                      | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| expiresInSec               | Long<br>Intervallo – Max: 3600, min.: 60  | Periodo di validità (in secondi) degli URL prefirmati. I valori validi sono compresi tra 60 e 3600 e il valore predefinito è 3600 secondi. Gli URL prefirmati vengono generati quando il servizio Jobs riceve una richiesta MQTT per il documento del processo.                                                                                                                                                                                                                                                                                                       |
| targetSelection            | Stringa                                   | Specifica se l'esecuzione del processo continuerà (CONTINUOUS) o se il processo verrà completato dopo che tutti gli oggetti specificati come target avranno completato il processo (SNAPSHOT). Se è continuo, il processo può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un processo verrà eseguito in un oggetto quando l'oggetto viene aggiunto a un gruppo target, anche dopo che il processo è stato completato da tutti gli oggetti originariamente nel gruppo.<br><br>Enumerazione: CONTINUOUS   SNAPSHOT |
| jobExecutionsRolloutConfig | JobExecutionsRolloutConfig                | Permette di creare un'implementazione per fasi del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| maximumPerMinute           | intero<br>Intervallo - min.: 1            | Numero massimo di oggetti che riceveranno una notifica di un processo in sospeso, ogni minuto. Questo parametro permette di creare un'implementazione per fasi.                                                                                                                                                                                                                                                                                                                                                                                                       |
| exponentialRate            | ExponentialRolloutRate                    | La velocità di aumento di un rollout di processo. Questo parametro consente di definire una velocità esponenziale per un rollout di processo.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| baseRatePerMinute          | intero<br>Intervallo – Max: 1000, min.: 1 | Il numero minimo di oggetti che riceveranno una notifica di un processo in sospeso, ogni minuto all'inizio del rollout di processo. Questo parametro consente di definire la velocità iniziale di un rollout.                                                                                                                                                                                                                                                                                                                                                         |

| Nome                      | Tipo                                                               | Descrizione                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rateIncreaseCriteria      | RateIncreaseCriteria                                               | I criteri per avviare l'aumento della velocità di rollout per un processo.<br><br>AWS IoT supporta fino a una cifra dopo il decimale (ad esempio, 1,5 ma non 1,55).                                                                                                                                                                                                                      |
| numberOfNotifiedThings    | intero<br>Intervallo - min.: 1                                     | La soglia per il numero di oggetti notificati che avvierà l'aumento della velocità di rollout.                                                                                                                                                                                                                                                                                           |
| numberOfSucceededThings   | intero<br>Intervallo - min.: 1                                     | La soglia per il numero di oggetti completati che avvierà l'aumento della velocità di rollout.                                                                                                                                                                                                                                                                                           |
| abortConfig               | AbortConfig                                                        | Consente di creare criteri per interrompere un processo.                                                                                                                                                                                                                                                                                                                                 |
| criteriaList              | elenco<br>member: AbortCriteria<br><br>Classe Java: java.util.List | L'elenco dei criteri di eliminazione per definire regole per interrompere il processo.                                                                                                                                                                                                                                                                                                   |
| failureType               | Stringa                                                            | Il tipo di errore di esecuzione di processo per definire una regola di avvio dell'interruzione di un processo.<br><br>enum: FAILED   REJECTED   TIMED_OUT   ALL                                                                                                                                                                                                                          |
| action                    | Stringa                                                            | Il tipo di operazione di eliminazione per avviare l'interruzione di un processo.<br><br>enum: CANCEL                                                                                                                                                                                                                                                                                     |
| minNumberOfExecutedThings | intero<br>Intervallo - min.: 1                                     | Il numero minimo di oggetti eseguiti prima della valutazione della regola di interruzione.                                                                                                                                                                                                                                                                                               |
| timeoutConfig             | TimeoutConfig                                                      | Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione del processo. Il timer viene avviato quando imposti lo stato di esecuzione del processo su IN_PROGRESS. Se lo stato di esecuzione del processo non è impostato su un altro stato terminale prima della scadenza del tempo a disposizione, verrà automaticamente impostato su TIMED_OUT. |

| Nome                       | Tipo                                                 | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| inProgressTimeoutInMinutes | Long                                                 | Specifica l'intervallo di tempo, in minuti, a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. L'intervallo di timeout può essere compreso fra 1 minuto e 7 giorni (da 1 a 10080 minuti). Il timer in corso non può essere aggiornato e verrà applicato a tutte le esecuzioni del processo. Se l'esecuzione del processo resta nello stato IN_PROGRESS per un periodo di tempo superiore a quello consentito dall'intervallo, l'esecuzione del processo non andrà a buon fine e verrà impostato lo stato TIMED_OUT terminale. |
| tags                       | elenco<br>member: Tag<br>Classe Java: java.util.List | Metadati utilizzabili per la gestione del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Chiave                     | Stringa                                              | La chiave del tag.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Valore                     | Stringa                                              | Il valore del tag.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

#### Output

```
{
 "jobArn": "string",
 "jobId": "string",
 "description": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome        | Tipo                                                                        | Descrizione                                   |
|-------------|-----------------------------------------------------------------------------|-----------------------------------------------|
| jobArn      | Stringa                                                                     | ARN del processo.                             |
| jobId       | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Identificatore univoco assegnato al processo. |
| description | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+                | Descrizione del processo.                     |

## Errori

## InvalidRequestException

I contenuti della richiesta non sono validi.

ResourceNotFoundException

La risorsa specificata non esiste.

`ResourceAlreadyExistsException`

La risorsa esiste già.

## LimitExceededException

È stato superato un limite.

## ThrottlingException

La velocità supera il limite.

## ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

## CreateKeysAndCertificate

Crea una coppia di chiavi RSA a 2048 bit e rilascia una certificazione X.509 usando la chiave pubblica emessa.

Nota Poiché questa è l'unica volta in cui AWS IoT emette la chiave privata per il certificato, è importante conservare la in una posizione sicura.

Riepilogo

```
aws iot create-keys-and-certificate \
[--set-as-active | --no-set-as-active] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "setAsActive": "boolean"
}
```

#### Campi di `cli-input-json`

| Nome        | Tipo     | Descrizione                           |
|-------------|----------|---------------------------------------|
| setAsActive | booleano | Specifica se il certificato è attivo. |

## Output

```

 "PrivateKey": "string"
 }
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo    | Descrizione                                                 |
|----------------|---------|-------------------------------------------------------------|
| certificateArn | Stringa | ARN del certificato.                                        |
| certificateId  | Stringa | Lunghezza max: 64, min.: 64<br>Modello: (0x)?[a-f A-F 0-9]+ |
| certificatePem | Stringa | Lunghezza max: 65536, min.: 1                               |
| keyPair        | KeyPair | Coppia di chiavi generata.                                  |
| PublicKey      | Stringa | Chiave pubblica.                                            |
| PrivateKey     | Stringa | Chiave privata.                                             |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

##### InternalFailureException

Si è verificato un errore imprevisto.

## CreateOTAUpdate

Crea un elemento AWS IoT OTAUpdate in un gruppo target di oggetti o gruppi.

#### Riepilogo

```

aws iot create-ota-update \
--ota-update-id <value> \
[--description <value>] \
--targets <value> \
```

```
[--target-selection <value>] \
[--aws-job-executions-rollout-config <value>] \
--files <value> \
--role-arn <value> \
[--additional-parameters <value>] \
[--tags <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di cli-input-json

```
{
 "otaUpdateId": "string",
 "description": "string",
 "targets": [
 "string"
],
 "targetSelection": "string",
 "awsJobExecutionsRolloutConfig": {
 "maximumPerMinute": "integer"
 },
 "files": [
 {
 "fileName": "string",
 "fileVersion": "string",
 "fileLocation": {
 "stream": {
 "streamId": "string",
 "fileId": "integer"
 },
 "s3Location": {
 "bucket": "string",
 "key": "string",
 "version": "string"
 }
 },
 "codeSigning": {
 "awsSignerJobId": "string",
 "startSigningJobParameter": {
 "signingProfileParameter": {
 "certificateArn": "string",
 "platform": "string",
 "certificatePathOnDevice": "string"
 },
 "signingProfileName": "string",
 "destination": {
 "s3Destination": {
 "bucket": "string",
 "prefix": "string"
 }
 }
 },
 "customCodeSigning": {
 "signature": {
 "inlineDocument": "blob"
 },
 "certificateChain": {
 "certificateName": "string",
 "inlineDocument": "string"
 },
 "hashAlgorithm": "string",
 "signatureAlgorithm": "string"
 }
 },
 "attributes": {
```

```

 "string": "string"
 }
},
"roleArn": "string",
"additionalParameters": {
 "string": "string"
},
"tags": [
 {
 "Key": "string",
 "Value": "string"
 }
]
}
```

#### Campi di **cli-input-json**

| Nome            | Tipo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Descrizione                                               |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| otaUpdateId     | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 _]+                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | ID dell'aggiornamento OTA da creare.                      |
| description     | Stringa<br>Lunghezza max: 2028<br>Modello: [^\p{C}]+                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Descrizione dell'aggiornamento OTA.                       |
| targets         | elenco<br>Membro: Target                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Dispositivi target per la ricezione di aggiornamenti OTA. |
| targetSelection | Stringa<br><br>Specifica se l'esecuzione dell'aggiornamento continuerà (CONTINUOUS) o se l'aggiornamento verrà completato dopo che tutti gli oggetti specificati come target avranno completato l'aggiornamento (SNAPSHOT). Se è continuo, l'aggiornamento può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un aggiornamento verrà eseguito in un oggetto quando l'oggetto viene aggiunto a un gruppo target, anche dopo che l'aggiornamento è stato completato da tutti gli oggetti originariamente nel gruppo.<br>Valori validi: CONTINUOUS   SNAPSHOT.<br><br>Enumerazione: CONTINUOUS   SNAPSHOT |                                                           |

| Nome                          | Tipo                                                                        | Descrizione                                                                       |
|-------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| awsJobExecutionsRolloutConfig | AwsJobExecutionsRolloutConfig                                               | Configurazione per l'implementazione degli aggiornamenti OTA.                     |
| maximumPerMinute              | intero<br><br>Intervallo – Max: 1000, min.: 1                               | Numero massimo di esecuzioni del processo di aggiornamento OTA avviate al minuto. |
| files                         | elenco<br><br>Membro: OTAUpdateFile                                         | File da distribuire in streaming dall'aggiornamento OTA.                          |
| fileName                      | Stringa                                                                     | Nome del file.                                                                    |
| fileVersion                   | Stringa                                                                     | Versione del file.                                                                |
| fileLocation                  | FileLocation                                                                | Percorso del firmware aggiornato.                                                 |
| stream                        | Flusso                                                                      | Flusso contenente l'aggiornamento OTA.                                            |
| streamId                      | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+ | ID flusso.                                                                        |
| fileId                        | intero<br><br>Intervallo – Max: 255, min.: 0                                | ID di un file associato a un flusso.                                              |
| s3Location                    | S3Location                                                                  | Percorso del firmware aggiornato in S3.                                           |
| bucket                        | Stringa<br><br>Lunghezza min.: 1                                            | Bucket S3.                                                                        |
| key                           | Stringa<br><br>Lunghezza min.: 1                                            | La chiave S3.                                                                     |
| versione                      | Stringa                                                                     | Versione del bucket S3                                                            |
| codeSigning                   | CodeSigning                                                                 | Metodo di firma del codice del file.                                              |
| awsSignerJobId                | Stringa                                                                     | ID dell'elemento AWSSignerJob che è stato creato per firmare il file.             |
| startSigningJobParameter      | StartSigningJobParameter                                                    | Describe il processo di firma del codice.                                         |
| signingProfileParameter       | SigningProfileParameter                                                     | Describe il profilo di firma del codice.                                          |
| certificateArn                | Stringa                                                                     | ARN del certificato.                                                              |

| Nome                    | Tipo                                                 | Descrizione                                                                                    |
|-------------------------|------------------------------------------------------|------------------------------------------------------------------------------------------------|
| platform                | Stringa                                              | Piattaforma hardware del tuo dispositivo.                                                      |
| certificatePathOnDevice | Stringa                                              | Percorso del certificato di firma del codice sul tuo dispositivo.                              |
| signingProfileName      | Stringa                                              | Nome del profilo di firma del codice.                                                          |
| destinazione            | Destinazione                                         | Percorso in cui scrivere il file firmato del codice.                                           |
| s3Destination           | S3Destination                                        | Describe il percorso del firmware aggiornato in S3.                                            |
| bucket                  | Stringa<br>Lunghezza min.: 1                         | Bucket S3 che contiene il firmware aggiornato.                                                 |
| prefisso                | Stringa                                              | Prefisso S3.                                                                                   |
| customCodeSigning       | CustomCodeSigning                                    | Metodo personalizzato per la firma del codice di un file.                                      |
| signature               | CodeSigningSignature                                 | Firma per il file.                                                                             |
| inlineDocument          | blob                                                 | Rappresentazione binaria codificata in base64 della firma del codice.                          |
| certificateChain        | CodeSigningCertificateChain                          | Catena di certificati.                                                                         |
| certificateName         | Stringa                                              | Nome del certificato.                                                                          |
| inlineDocument          | Stringa                                              | Rappresentazione binaria codificata in base64 della catena di certificati di firma del codice. |
| hashAlgorithm           | Stringa                                              | Algoritmo hash usato per firmare il codice del file.                                           |
| signatureAlgorithm      | Stringa                                              | Algoritmo di firma usato per firmare il codice del file.                                       |
| attributes              | mappa                                                | Elenco di coppie nome/attributo.                                                               |
| roleArn                 | Stringa<br>Lunghezza max: 2048, min.: 20             | Ruolo IAM che permette l'accesso al servizio AWS IoT Jobs.                                     |
| additionalParameters    | Mappa                                                | Elenco di parametri aggiuntivi per l'aggiornamento OTA che sono coppie nome/valore.            |
| tags                    | elenco<br>member: Tag<br>Classe Java: java.util.List | Metadati utilizzabili per la gestione degli aggiornamenti.                                     |

| Nome   | Tipo    | Descrizione        |
|--------|---------|--------------------|
| Chiave | Stringa | La chiave del tag. |
| Valore | Stringa | Il valore del tag. |

#### Output

```
{
 "otaUpdateId": "string",
 "awsIotJobId": "string",
 "otaUpdateArn": "string",
 "awsIotJobArn": "string",
 "otaUpdateStatus": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome            | Tipo    | Descrizione                                                                                                                          |
|-----------------|---------|--------------------------------------------------------------------------------------------------------------------------------------|
| otaUpdateId     | Stringa | ID aggiornamento OTA.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 _–]+                                           |
| awslotJobId     | Stringa | Job ID AWS IoT associato all'aggiornamento OTA.                                                                                      |
| otaUpdateArn    | Stringa | ARN dell'aggiornamento OTA.                                                                                                          |
| awslotJobArn    | Stringa | ARN del processo AWS IoT associato all'aggiornamento OTA.                                                                            |
| otaUpdateStatus | Stringa | Stato dell'aggiornamento OTA.<br><br>Enumerazione:<br>CREATE_PENDING  <br>CREATE_IN_PROGRESS  <br>CREATE_COMPLETE  <br>CREATE_FAILED |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### LimitExceededException

È stato superato un limite.

##### ResourceNotFoundException

La risorsa specificata non esiste.

##### ResourceAlreadyExistsException

La risorsa esiste già.

#### ThrottlingException

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### InternalFailureException

Si è verificato un errore imprevisto.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

## CreatePolicy

Crea una policy AWS IoT.

La policy creata è la versione predefinita per la policy. Questa operazione crea una versione della policy con un identificatore di versione 1 e imposta 1 come versione predefinita della policy.

#### Riepilogo

```
aws iot create-policy \
--policy-name <value> \
--policy-document <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "policyName": "string",
 "policyDocument": "string"
}
```

#### Campi di cli-input-json

| Nome           | Tipo    | Descrizione                                                                                                                                               |
|----------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| policyName     | Stringa | Nome della policy.<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+                                                                          |
| policyDocument | Stringa | Il documento JSON che descrive la policy. policyDocument deve avere una lunghezza minima pari a 1 e una lunghezza massima pari a 2048, esclusi gli spazi. |

#### Output

```
{
 "policyName": "string",
 "policyArn": "string",
```

```

 "policyDocument": "string",
 "policyVersionId": "string"
}

```

Campi di output dell'interfaccia a riga di comando

| Nome            | Tipo                                                          | Descrizione                            |
|-----------------|---------------------------------------------------------------|----------------------------------------|
| policyName      | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [w+=,.@-]+ | Nome della policy.                     |
| policyArn       | Stringa                                                       | ARN della policy.                      |
| policyDocument  | Stringa                                                       | Documento JSON che descrive la policy. |
| policyVersionId | Stringa<br>Modello: [0-9]+                                    | ID versione della policy.              |

Errori

`ResourceAlreadyExistsException`

La risorsa esiste già.

`MalformedPolicyException`

La documentazione della policy non è valida.

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

`InternalFailureException`

Si è verificato un errore imprevisto.

## CreatePolicyVersion

Crea una nuova versione della policy AWS IoT specificata. Per aggiornare una policy, crea una nuova versione della policy. Una policy gestita può avere fino a cinque versioni. Se la policy ha cinque versioni, devi usare `DeletePolicyVersion` per eliminare una versione esistente prima di creare una nuova.

Puoi impostare la nuova versione come versione predefinita della policy (operazione facoltativa). La versione predefinita è la versione operativa, ovvero la versione valida per i certificati cui è collegata la policy.

## Riepilogo

```
aws iot create-policy-version \
--policy-name <value> \
--policy-document <value> \
[--set-as-default | --no-set-as-default] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "policyName": "string",
 "policyDocument": "string",
 "setAsDefault": "boolean"
}
```

## Campi di cli-input-json

| Nome           | Tipo                                                                  | Descrizione                                                                                                                                                                                                                              |
|----------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| policyName     | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+ | Nome della policy.                                                                                                                                                                                                                       |
| policyDocument | Stringa                                                               | Documento JSON che descrive la policy. Lunghezza minima pari a 1. Lunghezza massima pari a 2048, esclusi gli spazi.                                                                                                                      |
| setAsDefault   | booleano                                                              | Specifica se la versione della policy è impostata come predefinita. Quando questo parametro è true, la nuova versione della policy diventa la versione operativa, ovvero la versione valida per i certificati cui è collegata la policy. |

## Output

```
{
 "policyArn": "string",
 "policyDocument": "string",
 "policyVersionId": "string",
 "isDefaultVersion": "boolean"
}
```

## Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo    | Descrizione                            |
|----------------|---------|----------------------------------------|
| policyArn      | Stringa | ARN della policy.                      |
| policyDocument | Stringa | Documento JSON che descrive la policy. |

| Nome             | Tipo                       | Descrizione                                                 |
|------------------|----------------------------|-------------------------------------------------------------|
| policyVersionId  | Stringa<br>Modello: [0-9]+ | ID versione della policy.                                   |
| isDefaultVersion | booleano                   | Specifica se la versione della policy è quella predefinita. |

#### Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**MalformedPolicyException**

La documentazione della policy non è valida.

**VersionsLimitExceededException**

Il numero di versioni della policy supera il limite.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## CreateRoleAlias

Crea un alias del ruolo.

#### Riepilogo

```
aws iot create-role-alias \
--role-alias <value> \
--role-arn <value> \
[--credential-duration-seconds <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "roleAlias": "string",
 "roleArn": "string",
 "credentialDurationSeconds": "integer"
}
```

### Campi di **cli-input-json**

| Nome                      | Tipo                                                        | Descrizione                                                                                                                  |
|---------------------------|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| roleAlias                 | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [w=,@-]+ | Alias del ruolo che punta a un ARN di ruolo. In questo modo, puoi modificare il ruolo senza dover aggiornare il dispositivo. |
| roleArn                   | Stringa<br>Lunghezza max: 2048, min.: 20                    | ARN del ruolo.                                                                                                               |
| credentialDurationSeconds | intero<br>Intervallo – Max: 3600, min.: 900                 | Periodo di validità (in secondi) delle credenziali.                                                                          |

### Output

```
{
 "roleAlias": "string",
 "roleAliasArn": "string"
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome         | Tipo                                                        | Descrizione               |
|--------------|-------------------------------------------------------------|---------------------------|
| roleAlias    | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [w=,@-]+ | Alias del ruolo.          |
| roleAliasArn | Stringa                                                     | ARN dell'alias del ruolo. |

### Errori

#### `ResourceAlreadyExistsException`

La risorsa esiste già.

#### `InvalidRequestException`

I contenuti della richiesta non sono validi.

#### `LimitExceededException`

È stato superato un limite.

#### `ThrottlingException`

La velocità supera il limite.

#### `UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## CreateScheduledAudit

Crea un audit pianificato che viene eseguito con un intervallo di tempo specificato.

### Riepilogo

```
aws iot create-scheduled-audit \
 --frequency <value> \
 [--day-of-month <value>] \
 [--day-of-week <value>] \
 --target-check-names <value> \
 [--tags <value>] \
 --scheduled-audit-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "frequency": "string",
 "dayOfMonth": "string",
 "dayOfWeek": "string",
 "targetCheckNames": [
 "string"
],
 "tags": [
 {
 "Key": "string",
 "Value": "string"
 }
],
 "scheduledAuditName": "string"
}
```

### Campi di cli-input-json

| Nome       | Tipo                                                       | Descrizione                                                                                                                                                                                                                        |
|------------|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| frequenza  | Stringa                                                    | Frequenza di esecuzione dell'audit. I valori possibili sono "DAILY", "WEEKLY", "BIWEEKLY" o "MONTHLY". L'ora di inizio effettiva di ogni audit è determinata dal sistema.<br><br>enumerazione: DAILY   WEEKLY   BIWEEKLY   MONTHLY |
| dayOfMonth | Stringa<br><br>modello: ^([1-9] [12][0-9] 3[01])\$ ^LAST\$ | Giorno del mese in cui viene eseguito l'audit pianificato. Il valore può essere compreso tra "1" e "31" oppure può essere "LAST". Questo campo è obbligatorio se il parametro "frequency" è impostato su                           |

| Nome               | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                 |
|--------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    |                                                                              | "MONTHLY". Se vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese.                                                                                                                                                                                    |
| dayOfWeek          | Stringa                                                                      | Giorno della settimana in cui viene eseguito l'audit pianificato. I valori possibili sono "SUN", "MON", "TUE", "WED", "THU", "FRI" o "SAT". Questo campo è obbligatorio se il parametro "frequency" è impostato su "WEEKLY" o "BIWEEKLY".<br><br>enumerazione: SUN   MON   TUE   WED   THU   FRI   SAT                      |
| targetCheckNames   | elenco<br><br>membro: AuditCheckName                                         | Controlli eseguiti durante l'audit pianificato. I controlli devono essere abilitati per l'account. Usa <a href="#">DescribeAccountAuditConfiguration</a> per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati, o <a href="#">UpdateAccountAuditConfiguration</a> per selezionare i controlli abilitati. |
| tags               | elenco<br><br>member: Tag<br><br>Classe Java: java.util.List                 | Metadati utilizzabili per la gestione dell'audit pianificato.                                                                                                                                                                                                                                                               |
| Chiave             | Stringa                                                                      | La chiave del tag.                                                                                                                                                                                                                                                                                                          |
| Valore             | Stringa                                                                      | Il valore del tag.                                                                                                                                                                                                                                                                                                          |
| scheduledAuditName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Nome da assegnare all'audit pianificato. Massimo 128 caratteri.                                                                                                                                                                                                                                                             |

## Output

```
{
 "scheduledAuditArn": "string"
}
```

## Campi di output dell'interfaccia a riga di comando

| Nome              | Tipo    | Descrizione                 |
|-------------------|---------|-----------------------------|
| scheduledAuditArn | Stringa | ARN dell'audit pianificato. |

## Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

**LimitExceededException**

È stato superato un limite.

## CreateSecurityProfile

Crea un profilo di sicurezza di Device Defender.

### Riepilogo

```
aws iot create-security-profile \
--security-profile-name <value> \
[--security-profile-description <value>] \
[--behaviors <value>] \
[--alert-targets <value>] \
[--additional-metrics-to-retain <value>] \
[--tags <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "securityProfileName": "string",
 "securityProfileDescription": "string",
 "behaviors": [
 {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 },
 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "statistic": "string"
 }
 }
 }
],
 "alertTargets": {
 "string": {
 "string": "string"
 }
 }
}
```

```

 "alertTargetArn": "string",
 "roleArn": "string"
 }
},
"additionalMetricsToRetain": [
 "string"
],
"tags": [
 {
 "Key": "string",
 "Value": "string"
 }
]
}

```

### Campi di **cli-input-json**

| Nome                       | Tipo                                                                          | Descrizione                                                                                                                                                                                                                                                                      |
|----------------------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| securityProfileName        | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome da assegnare al profilo di sicurezza.                                                                                                                                                                                                                                       |
| securityProfileDescription | Stringa<br><br>Lunghezza max: 1000<br><br>Modello: [\p{Graph}]*               | Descrizione del profilo di sicurezza.                                                                                                                                                                                                                                            |
| behaviors                  | elenco<br><br>membro: Behavior                                                | Specifica i comportamenti che, quando violati da un dispositivo (oggetto), causano la generazione di un avviso.                                                                                                                                                                  |
| name                       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome assegnato al comportamento.                                                                                                                                                                                                                                                 |
| metric                     | Stringa                                                                       | Valore misurato dal comportamento.                                                                                                                                                                                                                                               |
| criteria                   | BehaviorCriteria                                                              | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a metric.                                                                                                                                                                               |
| comparisonOperator         | Stringa                                                                       | Operatore che mette in correlazione l'oggetto misurato (metric) e i criteri (contenenti un value o statisticalThreshold).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set |

| Nome                         | Tipo                                    | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| value                        | MetricValue                             | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count                        | Long<br>Intervallo - min.: 0            | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cidrs                        | elenco<br>membro: Cidr                  | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports                        | elenco<br>membro: Port                  | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds              | intero                                  | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |
| consecutiveDatapointsToAlarm | intero<br>Intervallo – Max: 10, min.: 1 | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                      |
| consecutiveDatapointsToClear | intero<br>Intervallo – Max: 10, min.: 1 | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                   |

| Nome                      | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| statisticalThreshold      | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistic                 | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato ( <code>durationSeconds</code> ) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto ( <code>comparisonOperator</code> ) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario si verifica una violazione. |
| alertTargets              | mappa                                                                        | Specifica le destinazioni di invio degli avvisi. Gli avvisi vengono sempre inviati alla console. Gli avvisi vengono generati quando un dispositivo (oggetto) viola un comportamento.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| alertTargetArn            | Stringa                                                                      | ARN del target di notifica a cui vengono inviati gli avvisi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| roleArn                   | Stringa<br><br>Lunghezza max: 2048, min.: 20                                 | ARN del ruolo che concede l'autorizzazione per l'invio degli avvisi al target di notifica.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| additionalMetricsToRetain | elenco<br><br>membro: BehaviorMetric                                         | Un elenco di parametri i cui dati vengono conservati (archiviati). Per impostazione predefinita, i dati vengono conservati per qualsiasi parametro utilizzato nel <code>behaviors</code> del profilo ma vengono anche conservati per qualsiasi parametro specificato qui.                                                                                                                                                                                                                                                                                                                                                                                                        |

| Nome   | Tipo                                                 | Descrizione                                                     |
|--------|------------------------------------------------------|-----------------------------------------------------------------|
| tags   | elenco<br>member: Tag<br>Classe Java: java.util.List | Metadati utilizzabili per la gestione del profilo di sicurezza. |
| Chiave | Stringa                                              | La chiave del tag.                                              |
| Valore | Stringa                                              | Il valore del tag.                                              |

#### Output

```
{
 "securityProfileName": "string",
 "securityProfileArn": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome                | Tipo                                                                          | Descrizione                             |
|---------------------|-------------------------------------------------------------------------------|-----------------------------------------|
| securityProfileName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome assegnato al profilo di sicurezza. |
| securityProfileArn  | Stringa                                                                       | ARN del profilo di sicurezza.           |

#### Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceAlreadyExistsException**

La risorsa esiste già.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## CreateStream

Crea un flusso per la distribuzione di uno o più file di grandi dimensioni in blocchi su MQTT. Un flusso trasporta byte di dati in blocchi o blocchi in pacchetti come messaggi MQTT da un'origine come S3. A un flusso possono essere associati uno o più file. La dimensione totale di un file associato al flusso non può superare 2 MB. Il flusso verrà creato con la versione 0. Se viene creato un flusso con lo stesso streamID come flusso esistente che è stato eliminato negli ultimi 90 giorni, verrà recuperato il vecchio flusso incrementando la versione di 1.

## Riepilogo

```
aws iot create-stream \
--stream-id <value> \
[--description <value>] \
--files <value> \
--role-arn <value> \
[--tags <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "streamId": "string",
 "description": "string",
 "files": [
 {
 "fileId": "integer",
 "s3Location": {
 "bucket": "string",
 "key": "string",
 "version": "string"
 }
 }
],
 "roleArn": "string",
 "tags": [
 {
 "Key": "string",
 "Value": "string"
 }
]
}
```

## Campi di cli-input-json

| Nome        | Tipo                                                                        | Descrizione                        |
|-------------|-----------------------------------------------------------------------------|------------------------------------|
| streamId    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+ | ID flusso.                         |
| description | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+                | Descrizione del flusso.            |
| files       | elenco<br><br>Membro: StreamFile                                            | File di cui eseguire lo streaming. |
| fileId      | intero<br><br>Intervallo – Max: 255, min.: 0                                | ID file.                           |
| s3Location  | S3Location                                                                  | Posizione del file in S3.          |
| bucket      | Stringa                                                                     | Bucket S3.                         |

| Nome     | Tipo                                                 | Descrizione                                                                                                               |
|----------|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
|          | Lunghezza min.: 1                                    |                                                                                                                           |
| key      | Stringa                                              | La chiave S3.                                                                                                             |
|          | Lunghezza min.: 1                                    |                                                                                                                           |
| versione | Stringa                                              | Versione del bucket S3                                                                                                    |
| roleArn  | Stringa                                              | Ruolo IAM che l'entità principale del servizio IoT può assumere per accedere ai file S3.<br>Lunghezza max: 2048, min.: 20 |
| tags     | elenco<br>member: Tag<br>Classe Java: java.util.List | Metadati utilizzabili per la gestione dei flussi.                                                                         |
| Chiave   | Stringa                                              | La chiave del tag.                                                                                                        |
| Valore   | Stringa                                              | Il valore del tag.                                                                                                        |

#### Output

```
{
 "streamId": "string",
 "streamArn": "string",
 "description": "string",
 "streamVersion": "integer"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome          | Tipo                                                                | Descrizione             |
|---------------|---------------------------------------------------------------------|-------------------------|
| streamId      | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 _]+ | ID flusso.              |
| streamArn     | Stringa                                                             | ARN del flusso.         |
| description   | Stringa<br>Lunghezza max: 2028<br>Modello: [^\p{C}]+                | Descrizione del flusso. |
| streamVersion | intero<br>Intervallo – Max: 65535, min.: 0                          | Versione del flusso.    |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

**LimitExceededException**

È stato superato un limite.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ResourceAlreadyExistsException**

La risorsa esiste già.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## CreateThing

Crea un record dell'oggetto nel registro. La chiamata ha esito positivo se viene effettuata più volte utilizzando lo stesso nome di oggetto e configurazione. Se la chiamata viene effettuata con lo stesso nome di oggetto, ma configurazione diversa, viene generata l'eccezione `ResourceAlreadyExistsException`.

### Note

Si tratta di un'operazione del piano di controllo. Vedi [Authorization](#) (Autorizzazione) per informazioni relativa all'autorizzazione di operazioni del piano di controllo.

### Riepilogo

```
aws iot create-thing \
 --thing-name <value> \
 [--thing-type-name <value>] \
 [--attribute-payload <value>] \
 [--billing-group-name <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

### Formato di `cli-input-json`

```
{
 "thingName": "string",
 "thingTypeName": "string",
 "attributePayload": {
 "attributes": {
 "string": "string"
 },
 "merge": "boolean"
 },
 "billingGroupName": "string"
}
```

### Campi di `cli-input-json`

| Nome             | Tipo                                                                          | Descrizione                                                                                                                                                                                                                                                                                                                         |
|------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingName        | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto da creare.                                                                                                                                                                                                                                                                                                        |
| thingTypeName    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del tipo di oggetto associato al nuovo oggetto.                                                                                                                                                                                                                                                                                |
| attributePayload | AttributePayload                                                              | Payload dell'attributo, costituito da un massimo di tre coppie nome/valore in un documento JSON. Ad esempio:<br><br><code>\ "attributes\":<br/>{\ \"string1\":<br/>\"string2\"}</code>                                                                                                                                              |
| attributes       | mappa                                                                         | Stringa JSON contenente fino a tre coppie chiave/valore in formato JSON. Ad esempio:<br><br><code>\ "attributes\":<br/>{\ \"string1\":<br/>\"string2\"}</code>                                                                                                                                                                      |
| merge            | booleano                                                                      | Specifica se l'elenco di attributi fornito in AttributePayload deve essere unito agli attributi archiviati nel registro, anziché sovrascrivere questi ultimi.<br><br>Per rimuovere un attributo, chiama UpdateThing con un valore di attributo vuoto.<br><br>Note<br><br>L'attributo merge è valido solo quando chiami UpdateThing. |
| billingGroupName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Il nome del gruppo di fatturazione a cui sarà aggiunto l'oggetto.                                                                                                                                                                                                                                                                   |

### Output

```
{
 "thingName": "string",
 "thingArn": "string",
```

```
 "thingId": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome      | Tipo    | Descrizione                                                                           |
|-----------|---------|---------------------------------------------------------------------------------------|
| thingName | Stringa | Nome del nuovo oggetto.<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ |
| thingArn  | Stringa | ARN del nuovo oggetto.                                                                |
| thingId   | Stringa | ID oggetto.                                                                           |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ThrottlingException`

La velocità supera il limite.

##### `UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

##### `ResourceAlreadyExistsException`

La risorsa esiste già.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

## CreateThingGroup

Crea un gruppo di oggetti.

#### Note

Si tratta di un'operazione del piano di controllo. Vedi [Authorization](#) (Autorizzazione) per informazioni relativa all'autorizzazione di operazioni del piano di controllo.

#### Riepilogo

```
aws iot create-thing-group \
--thing-group-name <value> \
[--parent-group-name <value>] \
[--thing-group-properties <value>] \
[--tags <value>] \
[--cli-input-json <value>]
```

[--generate-cli-skeleton]

#### Formato di cli-input-json

```
{
 "thingGroupName": "string",
 "parentGroupName": "string",
 "thingGroupProperties": {
 "thingGroupDescription": "string",
 "attributePayload": {
 "attributes": {
 "string": "string"
 },
 "merge": "boolean"
 }
 },
 "tags": [
 {
 "Key": "string",
 "Value": "string"
 }
]
}
```

#### Campi di cli-input-json

| Nome                  | Tipo                                                                  | Descrizione                                                                                                                                                        |
|-----------------------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingGroupName        | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del gruppo di oggetti da creare.                                                                                                                              |
| parentGroupName       | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del gruppo di oggetti padre.                                                                                                                                  |
| thingGroupProperties  | ThingGroupProperties                                                  | Proprietà del gruppo di oggetti.                                                                                                                                   |
| thingGroupDescription | Stringa<br>Lunghezza max: 2028<br>Modello: [\p{Graph}]*               | Descrizione del gruppo di oggetti.                                                                                                                                 |
| attributePayload      | AttributePayload                                                      | Attributi del gruppo di oggetti in formato JSON.                                                                                                                   |
| attributes            | mappa                                                                 | Stringa JSON contenente fino a tre coppie chiave/valore in formato JSON. Ad esempio:<br><br><code>\\"attributes\\":<br/>{\\"string1\\":<br/>\\"string2\\\"}</code> |
| merge                 | booleano                                                              | Specifica se l'elenco di attributi fornito in AttributePayload deve essere unito agli attributi                                                                    |

| Nome   | Tipo                                                                             | Descrizione                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                                                                                  | <p>archiviati nel registro, anziché sovrascrivere questi ultimi.</p> <p>Per rimuovere un attributo, chiama <code>UpdateThing</code> con un valore di attributo vuoto.</p> <p><b>Note</b></p> <p>L'attributo <code>merge</code> è valido solo quando chiavi <code>UpdateThing</code>.</p> |
| tags   | <p>elenco</p> <p>member: Tag</p> <p>Classe Java: <code>java.util.List</code></p> | Metadati utilizzabili per la gestione del gruppo di oggetti.                                                                                                                                                                                                                             |
| Chiave | Stringa                                                                          | La chiave del tag.                                                                                                                                                                                                                                                                       |
| Valore | Stringa                                                                          | Il valore del tag.                                                                                                                                                                                                                                                                       |

#### Output

```
{
 "thingGroupName": "string",
 "thingGroupArn": "string",
 "thingGroupId": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo                                                                                 | Descrizione                 |
|----------------|--------------------------------------------------------------------------------------|-----------------------------|
| thingGroupName | <p>Stringa</p> <p>Lunghezza max: 128, min.: 1</p> <p>Modello: [a-z A-Z 0-9 :_-]+</p> | Nome del gruppo di oggetti. |
| thingGroupArn  | Stringa                                                                              | ARN del gruppo di oggetti.  |
| thingGroupId   | <p>Stringa</p> <p>Lunghezza max: 128, min.: 1</p> <p>Modello: [a-z A-Z 0-9 :-]+</p>  | ID gruppo di oggetti.       |

#### Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceAlreadyExistsException`

La risorsa esiste già.

#### ThrottlingException

La velocità supera il limite.

#### InternalFailureException

Si è verificato un errore imprevisto.

## CreateThingType

Crea un nuovo tipo di oggetto.

### Riepilogo

```
aws iot create-thing-type \
 --thing-type-name <value> \
 [--thing-type-properties <value>] \
 [--tags <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "thingTypeName": "string",
 "thingTypeProperties": {
 "thingTypeDescription": "string",
 "searchableAttributes": [
 "string"
]
 },
 "tags": [
 {
 "Key": "string",
 "Value": "string"
 }
]
}
```

### Campi di **cli-input-json**

| Nome                 | Tipo                                                                          | Descrizione                                                                                                                                                                                                       |
|----------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingTypeName        | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome del tipo di oggetto.                                                                                                                                                                                         |
| thingTypeProperties  | ThingTypeProperties                                                           | Elemento ThingTypeProperties per il tipo di oggetto da creare. Contiene informazioni sul nuovo tipo di oggetto, tra cui una descrizione e un elenco di nomi di attributi dell'oggetto che possono essere cercati. |
| thingTypeDescription | Stringa                                                                       | Descrizione del tipo di oggetto.                                                                                                                                                                                  |

| Nome                 | Tipo                                                           | Descrizione                                                       |
|----------------------|----------------------------------------------------------------|-------------------------------------------------------------------|
|                      | Lunghezza max: 2028<br>Modello: [\p{Graph}]*                   |                                                                   |
| searchableAttributes | elenco<br>Membro: AttributeName<br>Classe Java: java.util.List | Elenco di nomi di attributi dell'oggetto che è possibile cercare. |
| tags                 | elenco<br>member: Tag<br>Classe Java: java.util.List           | Metadati utilizzabili per la gestione del tipo di oggetti.        |
| Chiave               | Stringa                                                        | La chiave del tag.                                                |
| Valore               | Stringa                                                        | Il valore del tag.                                                |

#### Output

```
{
 "thingTypeName": "string",
 "thingTypeArn": "string",
 "thingTypeId": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome          | Tipo                                                                  | Descrizione                                     |
|---------------|-----------------------------------------------------------------------|-------------------------------------------------|
| thingTypeName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del tipo di oggetto.                       |
| thingTypeArn  | Stringa                                                               | ARN (Amazon Resource Name) del tipo di oggetto. |
| thingTypeId   | Stringa                                                               | ID tipo di oggetto.                             |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

#### ResourceAlreadyExistsException

La risorsa esiste già.

## CreateTopicRule

Crea una regola. La creazione di regole è un'operazione a livello di amministratore. Qualsiasi utente che ha l'autorizzazione necessaria per creare regole potrà accedere ai dati elaborati dalla regola.

### Riepilogo

```
aws iot create-topic-rule \
--rule-name <value> \
--topic-rule-payload <value> \
[--tags <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "ruleName": "string",
 "topicRulePayload": {
 "sql": "string",
 "description": "string",
 "actions": [
 {
 "dynamoDB": {
 "tableName": "string",
 "roleArn": "string",
 "operation": "string",
 "hashKeyField": "string",
 "hashKeyValue": "string",
 "hashKeyType": "string",
 "rangeKeyField": "string",
 "rangeKeyValue": "string",
 "rangeKeyType": "string",
 "payloadField": "string"
 },
 "dynamoDBv2": {
 "roleArn": "string",
 "putItem": {
 "tableName": "string"
 }
 },
 "lambda": {
 "functionArn": "string"
 },
 "sns": {
 "targetArn": "string",
 "roleArn": "string",
 "messageFormat": "string"
 },
 "sqs": {
 "roleArn": "string",
 "queueUrl": "string",
 "useBase64": "boolean"
 }
 }
]
 }
}
```

```
},
"kinesis": {
 "roleArn": "string",
 "streamName": "string",
 "partitionKey": "string"
},
"republish": {
 "roleArn": "string",
 "topic": "string"
},
"s3": {
 "roleArn": "string",
 "bucketName": "string",
 "key": "string",
 "cannedAcl": "string"
},
"firehose": {
 "roleArn": "string",
 "deliveryStreamName": "string",
 "separator": "string"
},
"cloudwatchMetric": {
 "roleArn": "string",
 "metricNamespace": "string",
 "metricName": "string",
 "metricValue": "string",
 "metricUnit": "string",
 "metricTimestamp": "string"
},
"cloudwatchAlarm": {
 "roleArn": "string",
 "alarmName": "string",
 "stateReason": "string",
 "stateValue": "string"
},
"elasticsearch": {
 "roleArn": "string",
 "endpoint": "string",
 "index": "string",
 "type": "string",
 "id": "string"
},
"salesforce": {
 "token": "string",
 "url": "string"
},
"iotAnalytics": {
 "channelArn": "string",
 "channelName": "string",
 "roleArn": "string"
},
"iotEvents": {
 "inputName": "string",
 "messageId": "string",
 "roleArn": "string"
},
"stepFunctions": {
 "executionNamePrefix": "string",
 "stateMachineName": "string",
 "roleArn": "string"
}
},
],
"ruleDisabled": "boolean",
"awsIotSqlVersion": "string",
"errorAction": {
```

```
"dynamoDB": {
 "tableName": "string",
 "roleArn": "string",
 "operation": "string",
 "hashKeyField": "string",
 "hashKeyValue": "string",
 "hashKeyType": "string",
 "rangeKeyField": "string",
 "rangeKeyValue": "string",
 "rangeKeyType": "string",
 "payloadField": "string"
},
"dynamoDBv2": {
 "roleArn": "string",
 "putItem": {
 "tableName": "string"
 }
},
"lambda": {
 "functionArn": "string"
},
"sns": {
 "targetArn": "string",
 "roleArn": "string",
 "messageFormat": "string"
},
"sqs": {
 "roleArn": "string",
 "queueUrl": "string",
 "useBase64": "boolean"
},
"kinesis": {
 "roleArn": "string",
 "streamName": "string",
 "partitionKey": "string"
},
"republish": {
 "roleArn": "string",
 "topic": "string"
},
"s3": {
 "roleArn": "string",
 "bucketName": "string",
 "key": "string",
 "cannedAcl": "string"
},
"firehose": {
 "roleArn": "string",
 "deliveryStreamName": "string",
 "separator": "string"
},
"cloudwatchMetric": {
 "roleArn": "string",
 "metricNamespace": "string",
 "metricName": "string",
 "metricValue": "string",
 "metricUnit": "string",
 "metricTimestamp": "string"
},
"cloudwatchAlarm": {
 "roleArn": "string",
 "alarmName": "string",
 "stateReason": "string",
 "stateValue": "string"
},
"elasticsearch": {
```

```

 "roleArn": "string",
 "endpoint": "string",
 "index": "string",
 "type": "string",
 "id": "string"
},
"salesforce": {
 "token": "string",
 "url": "string"
},
"iotAnalytics": {
 "channelArn": "string",
 "channelName": "string",
 "roleArn": "string"
},
"iotEvents": {
 "inputName": "string",
 "messageId": "string",
 "roleArn": "string"
},
"stepFunctions": {
 "executionNamePrefix": "string",
 "stateMachineName": "string",
 "roleArn": "string"
}
},
"tags": "string"
}

```

### Campi di **cli-input-json**

| Nome             | Tipo                                                                           | Descrizione                                                                                                                                                                                          |
|------------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ruleName         | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: ^[a-z A-Z 0-9 _]+\$ | Nome della regola.                                                                                                                                                                                   |
| topicRulePayload | TopicRulePayload                                                               | Payload della regola.                                                                                                                                                                                |
| sql              | Stringa                                                                        | Istruzione SQL usata per eseguire query sull'argomento. Per ulteriori informazioni, consulta le <a href="#">informazioni di riferimento su SQL per AWS IoT</a> nella Guida per sviluppatori AWS IoT. |
| description      | Stringa                                                                        | Descrizione della regola.                                                                                                                                                                            |
| actions          | elenco<br><br>Membro: Action                                                   | Operazioni associate alla regola.                                                                                                                                                                    |
| dynamoDB         | DynamoDBAction                                                                 | Scrive in una tabella DynamoDB.                                                                                                                                                                      |
| tableName        | Stringa                                                                        | Nome della tabella DynamoDB.                                                                                                                                                                         |
| roleArn          | Stringa                                                                        | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                       |

| Nome          | Tipo             | Descrizione                                                                                                                                                                                                               |
|---------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| operation     | Stringa          | Tipo di operazione da eseguire. Segue il modello di sostituzione, per cui può essere \$ <b>operation</b> , ma la sostituzione deve restituire uno dei risultati seguenti: <b>INSERT</b> , <b>UPDATE</b> o <b>DELETE</b> . |
| hashKeyField  | Stringa          | Nome della chiave hash.                                                                                                                                                                                                   |
| hashKeyValue  | Stringa          | Valore della chiave hash.                                                                                                                                                                                                 |
| hashKeyType   | Stringa          | Tipo di chiave hash. I valori validi sono "STRING" e "NUMBER"<br><br>Enumerazione: STRING   NUMBER                                                                                                                        |
| rangeKeyField | Stringa          | Nome della chiave di intervallo.                                                                                                                                                                                          |
| rangeKeyValue | Stringa          | Valore della chiave di intervallo.                                                                                                                                                                                        |
| rangeKeyType  | Stringa          | Tipo di chiave di intervallo. I valori validi sono "STRING" e "NUMBER"<br><br>Enumerazione: STRING   NUMBER                                                                                                               |
| payloadField  | Stringa          | Payload dell'operazione. Questo nome può essere personalizzato.                                                                                                                                                           |
| dynamoDBv2    | DynamoDBv2Action | Scrive in una tabella DynamoDB. Questa è una nuova versione dell'operazione DynamoDB. Permette di scrivere ogni attributo incluso nel payload di un messaggio MQTT in una colonna DynamoDB separata.                      |
| roleArn       | Stringa          | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                                            |

| Nome          | Tipo         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| putItem       | PutItemInput | <p>Specifica la tabella DynamoDB in cui verranno scritti i dati del messaggio. Ad esempio:</p> <pre>{ "dynamoDBv2": { "roleArn": "aws:iam:12341251:my-role" "putItem": { "tableName": "my-table" } } }</pre> <p>Ogni attributo nel payload del messaggio verrà scritto in una colonna separata del database DynamoDB.</p>                                                                                                                                                                                                                                                                                              |
| tableName     | Stringa      | Tabella in cui verranno scritti i dati del messaggio.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| lambda        | LambdaAction | Richiama una funzione Lambda.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| functionArn   | Stringa      | ARN della funzione Lambda.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| sns           | SnsAction    | Pubblica in un argomento Amazon SNS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| targetArn     | Stringa      | ARN dell'argomento SNS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| roleArn       | Stringa      | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| messageFormat | Stringa      | <p>(Opzionale) Formato del messaggio da pubblicare. I valori accettati sono "JSON" e "RAW". Il valore predefinito dell'attributo è "RAW". SNS usa questa impostazione per determinare se il payload deve essere analizzato e se devono essere estratti i bit specifici della piattaforma rilevanti del payload. Per ulteriori informazioni sui formati di messaggio SNS, consulta la pagina <a href="https://docs.aws.amazon.com/sns/latest/dg/json-formats.html">https://docs.aws.amazon.com/sns/latest/dg/json-formats.html</a> e fai riferimento alla documentazione ufficiale.</p> <p>Enumerazione: RAW   JSON</p> |
| sqs           | SqsAction    | Pubblica in una coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| roleArn       | Stringa      | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Nome               | Tipo            | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| queueUrl           | Stringa         | URL della coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| useBase64          | booleano        | Specifica se usare la codifica Base64.                                                                                                                                                                                                                                                                                                                                                                                                           |
| kinesis            | KinesisAction   | Scrive i dati in un flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                       |
| roleArn            | Stringa         | ARN del ruolo IAM che concede l'accesso al flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                |
| streamName         | Stringa         | Nome del flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| partitionKey       | Stringa         | Chiave di partizione.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| republish          | RepublishAction | Pubblica in un altro argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                             |
| roleArn            | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                         |
| argomento          | Stringa         | Nome dell'argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| s3                 | S3Action        | Scrive in un bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| roleArn            | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                         |
| bucketName         | Stringa         | Bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| key                | Stringa         | Chiave dell'oggetto.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| cannedAcl          | Stringa         | <p>Lista di controllo degli accessi predefinita Amazon S3 che controlla l'accesso all'oggetto identificato dalla chiave dell'oggetto. Per ulteriori informazioni, consulta la pagina relativa alle <a href="#">liste di controllo degli accessi predefinite S3</a>.</p> <p>Enumerazione: private   public-read   public-read-write   aws-exec-read   authenticated-read   bucket-owner-read   bucket-owner-full-control   log-delivery-write</p> |
| firehose           | FirehoseAction  | Scrive in un flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                                                     |
| roleArn            | Stringa         | Ruolo IAM che concede l'accesso al flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                               |
| deliveryStreamName | Stringa         | Nome del flusso di distribuzione.                                                                                                                                                                                                                                                                                                                                                                                                                |

| Nome             | Tipo                             | Descrizione                                                                                                                                                                                         |
|------------------|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| separator        | Stringa<br>Modello: ([ ] (  ) ,) | Separatore di caratteri che verrà usato per separare i record scritti nel flusso Firehose. I valori validi sono: '\n' (nuova riga), '\t' (tabulazione), '\r\n' (nuova riga Windows), ',' (virgola). |
| cloudwatchMetric | CloudwatchMetricAction           | Acquisisce un parametro CloudWatch.                                                                                                                                                                 |
| roleArn          | Stringa                          | Ruolo IAM che permette l'accesso al parametro CloudWatch.                                                                                                                                           |
| metricNamespace  | Stringa                          | Namespace dei nomi del parametro CloudWatch.                                                                                                                                                        |
| metricName       | Stringa                          | Nome parametro CloudWatch.                                                                                                                                                                          |
| metricValue      | Stringa                          | Valore del parametro CloudWatch.                                                                                                                                                                    |
| metricUnit       | Stringa                          | <a href="#">Unità di misura del parametro supportata da CloudWatch</a> .                                                                                                                            |
| metricTimestamp  | Stringa                          | Uno <a href="#">Timestamp Unix</a> opzionale.                                                                                                                                                       |
| cloudwatchAlarm  | CloudwatchAlarmAction            | Modifica lo stato di un allarme CloudWatch.                                                                                                                                                         |
| roleArn          | Stringa                          | Ruolo IAM che permette l'accesso all'allarme CloudWatch.                                                                                                                                            |
| alarmName        | Stringa                          | Nome dell'allarme CloudWatch.                                                                                                                                                                       |
| stateReason      | Stringa                          | Motivo della modifica dell'allarme.                                                                                                                                                                 |
| stateValue       | Stringa                          | Valore dello stato dell'allarme. I valori accettabili sono: OK, ALARM, INSUFFICIENT_DATA.                                                                                                           |
| elasticsearch    | ElasticsearchAction              | Scrive dati in un dominio Amazon Elasticsearch Service.                                                                                                                                             |
| roleArn          | Stringa                          | ARN del ruolo IAM che ha accesso a Elasticsearch.                                                                                                                                                   |
| endpoint         | Stringa<br>modello: https?://.*  | Endpoint del dominio Elasticsearch.                                                                                                                                                                 |
| index            | Stringa                          | Indice Elasticsearch in cui vuoi archiviare i dati.                                                                                                                                                 |
| type             | Stringa                          | Tipo di documento che stai archiviando.                                                                                                                                                             |
| id               | Stringa                          | Identificatore univoco per il documento che stai archiviando.                                                                                                                                       |

| Nome         | Tipo                                                                                                                                                                                           | Descrizione                                                                                                                                                                         |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| salesforce   | SalesforceAction                                                                                                                                                                               | Invia un messaggio a un flusso di input Salesforce IoT Cloud.                                                                                                                       |
| token        | Stringa<br>Lunghezza min.: 40                                                                                                                                                                  | Token usato per autenticare l'accesso al flusso di input Salesforce IoT Cloud. Il token è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input. |
| url          | Stringa<br>Lunghezza max: 2000<br>modello: https://ingestion-[a-zA-Z0-9]{1,12}.[a-zA-Z0-9]+.((sfdc-matrix.net) (sfdcnow.com))/streams/w <a href="#">1, 20</a> /w <a href="#">1, 20</a> /evento | URL esposto dal flusso di input Salesforce IoT Cloud. L'URL è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input.                             |
| iotAnalytics | IotAnalyticsAction                                                                                                                                                                             | Invia i dati del messaggio a un canale AWS IoT Analytics.                                                                                                                           |
| channelArn   | Stringa                                                                                                                                                                                        | (obsoleto) L'ARN del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                               |
| channelName  | Stringa                                                                                                                                                                                        | Il nome del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                                        |
| roleArn      | Stringa                                                                                                                                                                                        | L'ARN del ruolo con una policy che concede a IoT Analytics l'autorizzazione per l'invio di dati di messaggi tramite IoT Analytics (iotanalytics:BatchPutMessage).                   |
| iotEvents    | IotEventsAction                                                                                                                                                                                | Invia un input a un rilevatore AWS IoT Events.                                                                                                                                      |
| inputName    | Stringa<br>Lunghezza max: 128, min.: 1                                                                                                                                                         | Il nome dell'input AWS IoT Events.                                                                                                                                                  |
| messageId    | Stringa<br>Lunghezza max: 128                                                                                                                                                                  | [Opzionale] Da utilizzare per essere certi che il rilevatore AWS IoT Events elaborerà solo un messaggio di input con un determinato messageId.                                      |
| roleArn      | Stringa                                                                                                                                                                                        | L'ARN del ruolo che concede l'autorizzazione AWS IoT per inviare un messaggio di input a un rilevatore AWS IoT Events. ("Action":"iotevents:BatchPutMessage").                      |

| Nome                | Tipo                | Descrizione                                                                                                                                                                                                                                             |
|---------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| stepFunctions       | StepFunctionsAction | Avvia l'esecuzione di una macchina a stati Step Functions.                                                                                                                                                                                              |
| executionNamePrefix | Stringa             | (Opzionale) All'esecuzione della macchina a stati verrà assegnato un nome costituito da questo prefisso seguito da un UUID. Step Functions crea automaticamente un nome univoco per ogni esecuzione della macchina a stati se non ne viene fornito uno. |
| stateMachineName    | Stringa             | Il nome della macchina a stati Step Functions di cui verrà avviata l'esecuzione.                                                                                                                                                                        |
| roleArn             | Stringa             | L'ARN del ruolo che concede a IoT l'autorizzazione per avviare l'esecuzione di una macchina a stati ("Action":"states:StartExecution").                                                                                                                 |
| ruleDisabled        | booleano            | Specifica se la regola è disabilitata.                                                                                                                                                                                                                  |
| awsIotSqlVersion    | Stringa             | Versione del motore di regole SQL da usare durante la valutazione della regola.                                                                                                                                                                         |
| errorAction         | Action              | Operazione da eseguire quando si verifica un errore.                                                                                                                                                                                                    |
| dynamoDB            | DynamoDBAction      | Scrive in una tabella DynamoDB.                                                                                                                                                                                                                         |
| tableName           | Stringa             | Nome della tabella DynamoDB.                                                                                                                                                                                                                            |
| roleArn             | Stringa             | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                                                                          |
| operation           | Stringa             | Tipo di operazione da eseguire. Segue il modello di sostituzione, per cui può essere <code>\$ operation</code> , ma la sostituzione deve restituire uno dei risultati seguenti: <code>INSERT</code> , <code>UPDATE</code> o <code>DELETE</code> .       |
| hashKeyField        | Stringa             | Nome della chiave hash.                                                                                                                                                                                                                                 |
| hashKeyValue        | Stringa             | Valore della chiave hash.                                                                                                                                                                                                                               |
| hashKeyType         | Stringa             | Tipo di chiave hash. I valori validi sono "STRING" e "NUMBER"<br><br>Enumerazione: STRING   NUMBER                                                                                                                                                      |

| Nome          | Tipo             | Descrizione                                                                                                                                                                                                                                                                                                               |
|---------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rangeKeyField | Stringa          | Nome della chiave di intervallo.                                                                                                                                                                                                                                                                                          |
| rangeKeyValue | Stringa          | Valore della chiave di intervallo.                                                                                                                                                                                                                                                                                        |
| rangeKeyType  | Stringa          | <p>Tipo di chiave di intervallo. I valori validi sono "STRING" e "NUMBER"</p> <p>Enumerazione: STRING   NUMBER</p>                                                                                                                                                                                                        |
| payloadField  | Stringa          | Payload dell'operazione. Questo nome può essere personalizzato.                                                                                                                                                                                                                                                           |
| dynamoDBv2    | DynamoDBv2Action | <p>Scrive in una tabella DynamoDB. Questa è una nuova versione dell'operazione DynamoDB. Permette di scrivere ogni attributo incluso nel payload di un messaggio MQTT in una colonna DynamoDB separata.</p>                                                                                                               |
| roleArn       | Stringa          | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                                                                                                                                            |
| putItem       | PutItemInput     | <p>Specifica la tabella DynamoDB in cui verranno scritti i dati del messaggio. Ad esempio:</p> <pre>{ "dynamoDBv2": { "roleArn": "aws:iam:12341251:my-role" "putItem": { "tableName": "my-table" } } }</pre> <p>Ogni attributo nel payload del messaggio verrà scritto in una colonna separata del database DynamoDB.</p> |
| tableName     | Stringa          | Tabella in cui verranno scritti i dati del messaggio.                                                                                                                                                                                                                                                                     |
| lambda        | LambdaAction     | Richiama una funzione Lambda.                                                                                                                                                                                                                                                                                             |
| functionArn   | Stringa          | ARN della funzione Lambda.                                                                                                                                                                                                                                                                                                |
| sns           | SnsAction        | Pubblica in un argomento Amazon SNS.                                                                                                                                                                                                                                                                                      |
| targetArn     | Stringa          | ARN dell'argomento SNS.                                                                                                                                                                                                                                                                                                   |
| roleArn       | Stringa          | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                  |

| Nome          | Tipo            | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| messageFormat | Stringa         | (Opzionale) Formato del messaggio da pubblicare. I valori accettati sono "JSON" e "RAW". Il valore predefinito dell'attributo è "RAW". SNS usa questa impostazione per determinare se il payload deve essere analizzato e se devono essere estratti i bit specifici della piattaforma rilevanti del payload. Per ulteriori informazioni sui formati di messaggio SNS, consulta la pagina <a href="https://docs.aws.amazon.com/sns/latest/dg/json-formats.html">https://docs.aws.amazon.com/sns/latest/dg/json-formats.html</a> e fai riferimento alla documentazione ufficiale.<br><br>Enumerazione: RAW   JSON |
| sqs           | SqsAction       | Pubblica in una coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| queueUrl      | Stringa         | URL della coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| useBase64     | booleano        | Specifica se usare la codifica Base64.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| kinesis       | KinesisAction   | Scrive i dati in un flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso al flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| streamName    | Stringa         | Nome del flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| partitionKey  | Stringa         | Chiave di partizione.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| republish     | RepublishAction | Pubblica in un altro argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| argomento     | Stringa         | Nome dell'argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| s3            | S3Action        | Scrive in un bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| bucketName    | Stringa         | Bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| key           | Stringa         | Chiave dell'oggetto.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Nome               | Tipo                               | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cannedAcl          | Stringa                            | <p>Lista di controllo degli accessi predefinita Amazon S3 che controlla l'accesso all'oggetto identificato dalla chiave dell'oggetto. Per ulteriori informazioni, consulta la pagina relativa alle <a href="#">liste di controllo degli accessi predefinite S3</a>.</p> <p>Enumerazione: private   public-read   public-read-write   aws-exec-read   authenticated-read   bucket-owner-read   bucket-owner-full-control   log-delivery-write</p> |
| firehose           | FirehoseAction                     | Scrive in un flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                                                     |
| roleArn            | Stringa                            | Ruolo IAM che concede l'accesso al flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                               |
| deliveryStreamName | Stringa                            | Nome del flusso di distribuzione.                                                                                                                                                                                                                                                                                                                                                                                                                |
| separator          | Stringa<br>Modello: ([ ] (  ) (),) | Separatore di caratteri che verrà usato per separare i record scritti nel flusso Firehose. I valori validi sono: '\n' (nuova riga), '\t' (tabulazione), '\r\n' (nuova riga Windows), ',' (virgola).                                                                                                                                                                                                                                              |
| cloudwatchMetric   | CloudwatchMetricAction             | Acquisisce un parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                              |
| roleArn            | Stringa                            | Ruolo IAM che permette l'accesso al parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                        |
| metricNamespace    | Stringa                            | Namespace dei nomi del parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                     |
| metricName         | Stringa                            | Nome parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| metricValue        | Stringa                            | Valore del parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| metricUnit         | Stringa                            | <a href="#">Unità di misura del parametro supportata da CloudWatch</a> .                                                                                                                                                                                                                                                                                                                                                                         |
| metricTimestamp    | Stringa                            | Uno <a href="#">Timestamp Unix</a> opzionale.                                                                                                                                                                                                                                                                                                                                                                                                    |
| cloudwatchAlarm    | CloudwatchAlarmAction              | Modifica lo stato di un allarme CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                      |
| roleArn            | Stringa                            | Ruolo IAM che permette l'accesso all'allarme CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                         |

| Nome          | Tipo                                                                                                                                                                       | Descrizione                                                                                                                                                                         |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| alarmName     | Stringa                                                                                                                                                                    | Nome dell'allarme CloudWatch.                                                                                                                                                       |
| stateReason   | Stringa                                                                                                                                                                    | Motivo della modifica dell'allarme.                                                                                                                                                 |
| stateValue    | Stringa                                                                                                                                                                    | Valore dello stato dell'allarme. I valori accettabili sono: OK, ALARM, INSUFFICIENT_DATA.                                                                                           |
| elasticsearch | ElasticsearchAction                                                                                                                                                        | Scrive dati in un dominio Amazon Elasticsearch Service.                                                                                                                             |
| roleArn       | Stringa                                                                                                                                                                    | ARN del ruolo IAM che ha accesso a Elasticsearch.                                                                                                                                   |
| endpoint      | Stringa<br>modello: https?://.*                                                                                                                                            | Endpoint del dominio Elasticsearch.                                                                                                                                                 |
| index         | Stringa                                                                                                                                                                    | Indice Elasticsearch in cui vuoi archiviare i dati.                                                                                                                                 |
| type          | Stringa                                                                                                                                                                    | Tipo di documento che stai archiviando.                                                                                                                                             |
| id            | Stringa                                                                                                                                                                    | Identificatore univoco per il documento che stai archiviando.                                                                                                                       |
| salesforce    | SalesforceAction                                                                                                                                                           | Invia un messaggio a un flusso di input Salesforce IoT Cloud.                                                                                                                       |
| token         | Stringa<br>Lunghezza min.: 40                                                                                                                                              | Token usato per autenticare l'accesso al flusso di input Salesforce IoT Cloud. Il token è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input. |
| url           | Stringa<br>Lunghezza max: 2000<br>modello: https://ingestion-[a-zA-Z0-9]{1,12}.[a-zA-Z0-9]+.((sfdc-matrix.net) (sfdcnow.com))/streams/w <b>1,20</b> /w <b>1,20</b> /evento | URL esposto dal flusso di input Salesforce IoT Cloud. L'URL è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input.                             |
| iotAnalytics  | iotAnalyticsAction                                                                                                                                                         | Invia i dati del messaggio a un canale AWS IoT Analytics.                                                                                                                           |
| channelArn    | Stringa                                                                                                                                                                    | (obsoleto) L'ARN del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                               |
| channelName   | Stringa                                                                                                                                                                    | Il nome del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                                        |

| Nome                | Tipo                                   | Descrizione                                                                                                                                                                                                                                             |
|---------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn             | Stringa                                | L'ARN del ruolo con una policy che concede a IoT Analytics l'autorizzazione per l'invio di dati di messaggi tramite IoT Analytics (iotanalytics:BatchPutMessage).                                                                                       |
| iotEvents           | IoTEventsAction                        | Invia un input a un rilevatore AWS IoT Events.                                                                                                                                                                                                          |
| inputName           | Stringa<br>Lunghezza max: 128, min.: 1 | Il nome dell'input AWS IoT Events.                                                                                                                                                                                                                      |
| messageId           | Stringa<br>Lunghezza max: 128          | [Opzionale] Da utilizzare per essere certi che il rilevatore AWS IoT Events elaborerà solo un messaggio di input con un determinato messageId.                                                                                                          |
| roleArn             | Stringa                                | L'ARN del ruolo che concede l'autorizzazione AWS IoT per inviare un messaggio di input a un rilevatore AWS IoT Events. ("Action":"iotevents:BatchPutMessage").                                                                                          |
| stepFunctions       | StepFunctionsAction                    | Avvia l'esecuzione di una macchina a stati Step Functions.                                                                                                                                                                                              |
| executionNamePrefix | Stringa                                | (Opzionale) All'esecuzione della macchina a stati verrà assegnato un nome costituito da questo prefisso seguito da un UUID. Step Functions crea automaticamente un nome univoco per ogni esecuzione della macchina a stati se non ne viene fornito uno. |
| stateMachineName    | Stringa                                | Il nome della macchina a stati Step Functions di cui verrà avviata l'esecuzione.                                                                                                                                                                        |
| roleArn             | Stringa                                | L'ARN del ruolo che concede a IoT l'autorizzazione per avviare l'esecuzione di una macchina a stati ("Action":"states:StartExecution").                                                                                                                 |

| Nome | Tipo    | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tags | Stringa | <p>Metadati utilizzabili per la gestione della regola dell'argomento.</p> <p><b>Note</b></p> <p>Per i parametri della richiesta URI, utilizza il formato: ...key1=value1&amp;key2=value2... Per il parametro della riga di comando dell'interfaccia a riga di comando, utilizza il formato: --tags "key1=value1&amp;key2=value2..." Per il file cli-input-json utilizza il formato: "tags": "key1=value1&amp;key2=value2..."</p> |

#### Output

Nessuna

Errori

`SqlParseException`

L'espressione SQL della regola non può essere analizzata correttamente.

`InternalException`

Si è verificato un errore imprevisto.

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceAlreadyExistsException`

La risorsa esiste già.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

`ConflictingResourceUpdateException`

Eccezione relativa ad aggiornamenti in conflitto della risorsa. Questa eccezione viene generata quando due aggiornamenti in sospeso causano un conflitto.

## DeleteAccountAuditConfiguration

Ripristina le impostazioni predefinite per gli audit di Device Defender per l'account. I dati di configurazione immessi vengono eliminati e tutti i controlli di auditing vengono reimpostati come disabilitati.

Riepilogo

```
aws iot delete-account-audit-configuration \
[--delete-scheduled-audits | --no-delete-scheduled-audits] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "deleteScheduledAudits": "boolean"
}
```

Campi di **cli-input-json**

| Nome                  | Tipo     | Descrizione                                             |
|-----------------------|----------|---------------------------------------------------------|
| deleteScheduledAudits | booleano | Se true, tutti gli audit pianificati vengono eliminati. |

Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DeleteAuthorizer

Elimina un'autorizzazione.

Riepilogo

```
aws iot delete-authorizer \
--authorizer-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "authorizerName": "string"
```

}

#### Campi di **cli-input-json**

| Nome           | Tipo                                                                | Descrizione                            |
|----------------|---------------------------------------------------------------------|----------------------------------------|
| authorizerName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=,@-]+ | Nome dell'autorizzazione da eliminare. |

#### Output

Nessuna

Errori

#### **DeleteConflictException**

Non puoi eliminare la risorsa perché è collegata a una o più risorse.

#### **ResourceNotFoundException**

La risorsa specificata non esiste.

#### **InvalidRequestException**

I contenuti della richiesta non sono validi.

#### **ThrottlingException**

La velocità supera il limite.

#### **UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### **ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

#### **InternalFailureException**

Si è verificato un errore imprevisto.

## DeleteBillingGroup

Elimina il gruppo di fatturazione.

#### Riepilogo

```
aws iot delete-billing-group \
 --billing-group-name <value> \
 [--expected-version <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "billingGroupName": "string",
 "expectedVersion": "long"
}
```

#### Campi di **cli-input-json**

| Nome             | Tipo                                                                          | Descrizione                                                                                                                                                                                                                                  |
|------------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| billingGroupName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Il nome del gruppo di fatturazione.                                                                                                                                                                                                          |
| expectedVersion  | Long                                                                          | La versione prevista del gruppo di fatturazione. Se la versione del gruppo di fatturazione non corrisponde alla versione prevista specificata nella richiesta, la richiesta DeleteBillingGroup viene rifiutata con VersionConflictException. |

#### Output

Nessuna

#### Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**VersionConflictException**

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DeleteCACertificate

Elimina un certificato CA registrato.

#### Riepilogo

```
aws iot delete-ca-certificate \
 --certificate-id <value> \
 [--cli-input-json <value>] \

```

```
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "certificateId": "string"
}
```

Campi di **cli-input-json**

| Nome          | Tipo                                                                   | Descrizione                                                                                            |
|---------------|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| certificateId | Stringa<br>Lunghezza max: 64, min.: 64<br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato da eliminare.<br>L'ultima parte dell'ARN del certificato contiene l'ID certificato. |

Output

Nessuna

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`CertificateStateException`

L'operazione del certificato non è consentita.

`ThrottlingException`

La velocità supera il limite.

`UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

`InternalFailureException`

Si è verificato un errore imprevisto.

`ResourceNotFoundException`

La risorsa specificata non esiste.

## DeleteCertificate

Elimina il certificato specificato.

Un certificato non può essere eliminato se è collegato a una policy o a un oggetto IoT o se il suo stato è impostato su ACTIVE. Per eliminare un certificato, usa prima di tutto l'API `DetachPrincipalPolicy`

per scollegare tutte le policy. Usa quindi l'API UpdateCertificate per impostare il certificato sullo stato INACTIVE.

#### Riepilogo

```
aws iot delete-certificate \
 --certificate-id <value> \
 [--force-delete | --no-force-delete] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "certificateId": "string",
 "forceDelete": "boolean"
}
```

#### Campi di cli-input-json

| Nome          | Tipo                                                                           | Descrizione                                                                                  |
|---------------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| certificateId | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato. L'ultima parte dell'ARN del certificato contiene l'ID certificato.       |
| forceDelete   | booleano                                                                       | Impone l'eliminazione di un certificato, se non è attivo e non è associato a un oggetto IoT. |

#### Output

Nessuna

Errori

**CertificateStateException**

L'operazione del certificato non è consentita.

**DeleteConflictException**

Non puoi eliminare la risorsa perché è collegata a una o più risorse.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

#### ResourceNotFoundException

La risorsa specificata non esiste.

## DeleteDynamicThingGroup

Elimina un gruppo di oggetti dinamico.

### Riepilogo

```
aws iot delete-dynamic-thing-group \
 --thing-group-name <value> \
 [--expected-version <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "thingGroupName": "string",
 "expectedVersion": "long"
}
```

### Campi di **cli-input-json**

| Nome            | Tipo                                                                  | Descrizione                                                       |
|-----------------|-----------------------------------------------------------------------|-------------------------------------------------------------------|
| thingGroupName  | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Il nome del gruppo di oggetti dinamico da eliminare.              |
| expectedVersion | Long                                                                  | La versione prevista del gruppo di oggetti dinamico da eliminare. |

### Output

Nessuna

### Errori

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### VersionConflictException

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

#### ThrottlingException

La velocità supera il limite.

### InternalFailureException

Si è verificato un errore imprevisto.

## DeleteJob

Elimina un processo e le relative esecuzioni.

L'eliminazione di un processo potrebbe richiedere del tempo, a seconda del numero di esecuzioni create per il processo e di altri fattori. Mentre il processo viene eliminato, lo stato del processo viene indicato come "DELETION\_IN\_PROGRESS". Il tentativo di eliminare o annullare un processo il cui stato è già "DELETION\_IN\_PROGRESS" restituirà un errore.

Solo 10 processi possono avere contemporaneamente lo stato "DELETION\_IN\_PROGRESS", altrimenti si verificherà un'eccezione LimitExceededException.

### Riepilogo

```
aws iot delete-job \
 --job-id <value> \
 [--force | --no-force] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "jobId": "string",
 "force": "boolean"
}
```

### Campi di cli-input-json

| Nome  | Tipo     | Descrizione                                                                                                                                                                                                                                               |
|-------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId | Stringa  | L'ID del processo da eliminare.<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+                                                                                                                                                       |
| force | booleano | (Opzionale) Quando true, è possibile eliminare un processo con stato "IN_PROGRESS". Altrimenti, è possibile eliminare solo un processo che è in uno stato terminale ("COMPLETED" o "CANCELED") o si verifica un'eccezione. Il valore predefinito è false. |

| Nome | Tipo | Descrizione                                                                                                                                                                                                                                                                                                                                                                              |
|------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |      | <p><b>Note</b></p> <p>L'eliminazione di un processo "IN_PROGRESS" impedirà al dispositivo in cui è in esecuzione il processo di accedere alle informazioni sul processo o di aggiornare lo stato di esecuzione. Prestare attenzione e verificare che tutti i dispositivi in cui sono in esecuzione processi eliminati siano in grado di effettuare il ripristino a uno stato valido.</p> |

#### Output

Nessuna

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `InvalidStateTransitionException`

Un aggiornamento ha tentato di modificare l'esecuzione del processo impostando uno stato non valido in base allo stato corrente dell'esecuzione del processo (ad esempio, un tentativo di modificare una richiesta con stato SUCCESS impostando lo stato IN\_PROGRESS). In questo caso, il corpo del messaggio di errore contiene anche il campo executionState.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `LimitExceededException`

È stato superato un limite.

##### `ThrottlingException`

La velocità supera il limite.

##### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

## DeleteJobExecution

Elimina l'esecuzione di un processo.

#### Riepilogo

```
aws iot delete-job-execution \
--job-id <value> \
--thing-name <value> \
--execution-number <value> \
[--force | --no-force] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "jobId": "string",
 "thingName": "string",
 "executionNumber": "long",
 "force": "boolean"
}
```

#### Campi di **cli-input-json**

| Nome            | Tipo                                                                          | Descrizione                                                                                                                                                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId           | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+    | L'ID del processo la cui esecuzione su un determinato dispositivo verrà eliminata.                                                                                                                                                                                                                                                                |
| thingName       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Il nome dell'oggetto di cui verrà eliminata l'esecuzione del processo.                                                                                                                                                                                                                                                                            |
| executionNumber | Long                                                                          | L'ID dell'esecuzione del processo da eliminare. L'oggetto executionNumber si riferisce all'esecuzione di un particolare processo in un dispositivo specifico.<br><br>Notare che, una volta eliminata l'esecuzione del processo, è possibile che IoT riutilizzi executionNumber, pertanto assicurarsi di ottenere e utilizzare il valore corretto. |
| force           | booleano                                                                      | (Opzionale) Quando true, è possibile eliminare l'esecuzione di un processo con stato "IN_PROGRESS". Altrimenti, è possibile eliminare solo l'esecuzione di un processo che è in uno stato terminale ("SUCCEEDED", "FAILED", "REJECTED", "REMOVED" o "CANCELED") o si verifica un'eccezione. Il valore predefinito è false.                        |

| Nome | Tipo | Descrizione                                                                                                                                                                                                                                                                                                       |
|------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |      | <p><b>Note</b></p> <p>L'eliminazione dell'esecuzione di un processo "IN_PROGRESS" impedirà al dispositivo di accedere alle informazioni sul processo o di aggiornare lo stato di esecuzione. Prestare attenzione e verificare che il dispositivo sia in grado di effettuare il ripristino a uno stato valido.</p> |

#### Output

Nessuna

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `InvalidStateTransitionException`

Un aggiornamento ha tentato di modificare l'esecuzione del processo impostando uno stato non valido in base allo stato corrente dell'esecuzione del processo (ad esempio, un tentativo di modificare una richiesta con stato SUCCESS impostando lo stato IN\_PROGRESS). In questo caso, il corpo del messaggio di errore contiene anche il campo executionState.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `ThrottlingException`

La velocità supera il limite.

##### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

## DeleteOTAUpdate

Elimina un aggiornamento OTA.

#### Riepilogo

```
aws iot delete-ota-update \
--ota-update-id <value> \
[--delete-stream | --no-delete-stream] \
[--force-delete-aws-job | --no-force-delete-aws-job] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "otaUpdateId": "string",
 "deleteStream": "boolean",
 "forceDeleteAWSJob": "boolean"
}
```

#### Campi di cli-input-json

| Nome              | Tipo                                                                | Descrizione                                                                                                                                |
|-------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| otaUpdateId       | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 _]+ | ID aggiornamento OTA da eliminare.                                                                                                         |
| deleteStream      | booleano                                                            | Specifica se il flusso associato a un aggiornamento OTA deve essere eliminato quando viene eliminato l'aggiornamento OTA.                  |
| forceDeleteAWSJob | booleano                                                            | Specifica se il flusso associato al processo AWS con l'aggiornamento OTA deve essere eliminato quando viene eliminato l'aggiornamento OTA. |

#### Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**VersionConflictException**

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

# DeletePolicy

Elimina la policy specificata.

Una policy non può essere eliminata se ha versioni non predefinite o se è collegata a qualsiasi certificato.

Per eliminare una policy, usa l'API DeletePolicyVersion per eliminare tutte le versioni non predefinite della policy, quindi usa l'API DetachPrincipalPolicy per scollegare la policy da qualsiasi certificato e infine usa l'API DeletePolicy per eliminare la policy.

Quando una policy viene eliminata tramite DeletePolicy, con la policy viene eliminata anche la sua versione predefinita.

Riepilogo

```
aws iot delete-policy \
 --policy-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "policyName": "string"
}
```

Campi di **cli-input-json**

| Nome       | Tipo                                                                  | Descrizione                     |
|------------|-----------------------------------------------------------------------|---------------------------------|
| policyName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+ | Nome della policy da eliminare. |

Output

Nessuna

Errori

**DeleteConflictException**

Non puoi eliminare la risorsa perché è collegata a una o più risorse.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## DeletePolicyVersion

Elimina la versione indicata della policy specificata. Non puoi eliminare la versione predefinita di una policy usando questa API. Per eliminare la versione predefinita di una policy, usa DeletePolicy. Per identificare la versione di una policy contrassegnata come versione predefinita, usa ListPolicyVersions.

#### Riepilogo

```
aws iot delete-policy-version \
 --policy-name <value> \
 --policy-version-id <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "policyName": "string",
 "policyVersionId": "string"
}
```

#### Campi di cli-input-json

| Nome            | Tipo                                                                  | Descrizione               |
|-----------------|-----------------------------------------------------------------------|---------------------------|
| policyName      | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+ | Nome della policy.        |
| policyVersionId | Stringa<br><br>Modello: [0-9]+                                        | ID versione della policy. |

#### Output

Nessuna

Errori

#### DeleteConflictException

Non puoi eliminare la risorsa perché è collegata a una o più risorse.

#### ResourceNotFoundException

La risorsa specificata non esiste.

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### **ThrottlingException**

La velocità supera il limite.

#### **UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### **ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

#### **InternalFailureException**

Si è verificato un errore imprevisto.

## DeleteRegistrationCode

Elimina il codice di registrazione di un certificato CA.

#### Riepilogo

```
aws iot delete-registration-code \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
}
```

#### Output

Nessuna

Errori

#### **ThrottlingException**

La velocità supera il limite.

#### **ResourceNotFoundException**

La risorsa specificata non esiste.

#### **UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### **ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

#### **InternalFailureException**

Si è verificato un errore imprevisto.

## DeleteRoleAlias

Elimina un alias del ruolo.

## Riepilogo

```
aws iot delete-role-alias \
--role-alias <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

## Formato di **cli-input-json**

```
{
 "roleAlias": "string"
}
```

## Campi di **cli-input-json**

| Nome      | Tipo                                                                | Descrizione                   |
|-----------|---------------------------------------------------------------------|-------------------------------|
| roleAlias | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=,@-]+ | Alias del ruolo da eliminare. |

## Output

Nessuna

Errori

### DeleteConflictException

Non puoi eliminare la risorsa perché è collegata a una o più risorse.

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ThrottlingException

La velocità supera il limite.

### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

### InternalFailureException

Si è verificato un errore imprevisto.

### ResourceNotFoundException

La risorsa specificata non esiste.

# DeleteScheduledAudit

Elimina un audit pianificato.

## Riepilogo

```
aws iot delete-scheduled-audit \
--scheduled-audit-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "scheduledAuditName": "string"
}
```

Campi di **cli-input-json**

| Nome               | Tipo                                                                         | Descrizione                               |
|--------------------|------------------------------------------------------------------------------|-------------------------------------------|
| scheduledAuditName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Nome dell'audit pianificato da eliminare. |

Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DeleteSecurityProfile

Elimina un profilo di sicurezza di Device Defender.

Riepilogo

```
aws iot delete-security-profile \
--security-profile-name <value> \
[--expected-version <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
```

```

 "securityProfileName": "string",
 "expectedVersion": "long"
}

```

#### Campi di **cli-input-json**

| Nome                | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                          |
|---------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| securityProfileName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_]+ | Nome del profilo di sicurezza da eliminare.                                                                                                                                                                                                                          |
| expectedVersion     | Long                                                                         | Versione prevista del profilo di sicurezza. Viene generata una nuova versione ogni volta che il profilo di sicurezza viene aggiornato. Se specifichi un valore diverso dalla versione effettiva, viene generata un'eccezione <code>VersionConflictException</code> . |

#### Output

Nessuna

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

`VersionConflictException`

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro `--version`.

## DeleteStream

Elimina un flusso.

Riepilogo

```

aws iot delete-stream \
--stream-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]

```

Formato di **cli-input-json**

```
{
 "streamId": "string"
}
```

#### Campi di **cli-input-json**

| Nome     | Tipo    | Descrizione                                                                     |
|----------|---------|---------------------------------------------------------------------------------|
| streamId | Stringa | ID flusso.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ |

Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**DeleteConflictException**

Non puoi eliminare la risorsa perché è collegata a una o più risorse.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DeleteThing

Elimina l'oggetto specificato. Questo comando avrà esito positivo senza alcun errore se l'eliminazione va a buon fine oppure se specifichi un oggetto che non esiste.

Riepilogo

```
aws iot delete-thing \
 --thing-name <value> \
 [--expected-version <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "thingName": "string",
 "expectedVersion": "long"
}
```

#### Campi di **cli-input-json**

| Nome            | Tipo                                                                          | Descrizione                                                                                                                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingName       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome dell'oggetto da eliminare.                                                                                                                                                                                                           |
| expectedVersion | Long                                                                          | Versione prevista del record dell'oggetto nel registro. Se la versione del record nel registro non corrisponde alla versione prevista specificata nella richiesta, la richiesta DeleteThing viene rifiutata con VersionConflictException. |

#### Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**VersionConflictException**

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DeleteThingGroup

Elimina un gruppo di oggetti.

## Riepilogo

```
aws iot delete-thing-group \
--thing-group-name <value> \
[--expected-version <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "thingGroupName": "string",
 "expectedVersion": "long"
}
```

### Campi di **cli-input-json**

| Nome            | Tipo                                                                  | Descrizione                                           |
|-----------------|-----------------------------------------------------------------------|-------------------------------------------------------|
| thingGroupName  | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+ | Nome del gruppo di oggetti da eliminare.              |
| expectedVersion | Long                                                                  | Versione prevista del gruppo di oggetti da eliminare. |

## Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**VersionConflictException**

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

# DeleteThingShadow

Elimina la copia shadow per l'oggetto specificato.

Per ulteriori informazioni, consulta [DeleteThingShadow](#) nella Guida per lo sviluppatore di AWS IoT.

## Riepilogo

```
aws iot-data delete-thing-shadow \
--thing-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "thingName": "string"
}
```

Campi di **cli-input-json**

| Nome      | Tipo                                                                          | Descrizione        |
|-----------|-------------------------------------------------------------------------------|--------------------|
| thingName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto. |

Output

```
{
 "payload": "blob"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome    | Tipo | Descrizione                                |
|---------|------|--------------------------------------------|
| payload | blob | Informazioni sullo stato, in formato JSON. |

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

**MethodNotAllowedException**

La combinazione specificata di verbo HTTP e URI non è supportata.

**UnsupportedDocumentEncodingException**

La codifica non è supportata.

## DeleteThingType

Elimina il tipo di oggetto specificato. Non puoi eliminare un tipo di oggetto se ha altri oggetti associati. Per eliminare un tipo di oggetto, contrassegna prima di tutto come obsoleto chiamando `DeprecateThingType`, quindi rimuovi tutti gli oggetti associati chiamando `UpdateThing` per modificare il tipo di oggetto in qualsiasi oggetto associato e infine usa `DeleteThingType` per eliminare il tipo di oggetto.

Riepilogo

```
aws iot delete-thing-type \
 --thing-type-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "thingTypeName": "string"
}
```

Campi di `cli-input-json`

| Nome          | Tipo                                                                          | Descrizione               |
|---------------|-------------------------------------------------------------------------------|---------------------------|
| thingTypeName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del tipo di oggetto. |

Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## DeleteTopicRule

Elimina la regola.

### Riepilogo

```
aws iot delete-topic-rule \
[--rule-name <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "ruleName": "string"
}
```

### Campi di cli-input-json

| Nome     | Tipo                                                                           | Descrizione        |
|----------|--------------------------------------------------------------------------------|--------------------|
| ruleName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: ^[a-z A-Z 0-9 _]+\$ | Nome della regola. |

### Output

Nessuna

### Errori

#### InternalException

Si è verificato un errore imprevisto.

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ConflictingResourceUpdateException

Eccezione relativa ad aggiornamenti in conflitto della risorsa. Questa eccezione viene generata quando due aggiornamenti in sospeso causano un conflitto.

## DeleteV2LoggingLevel

Elimina un livello di logging.

Riepilogo

```
aws iot delete-v2-logging-level \
--target-type <value> \
--target-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "targetType": "string",
 "targetName": "string"
}
```

Campi di `cli-input-json`

| Nome       | Tipo    | Descrizione                                                                                                                                                       |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| targetType | Stringa | Tipo di risorsa per cui stai configurando il logging. Deve essere <code>THING_Group</code> .<br><br>Enumerazione: <code>DEFAULT</code>   <code>THING_GROUP</code> |
| targetName | Stringa | Nome della risorsa per cui stai configurando il logging.                                                                                                          |

Output

Nessuna

Errori

`InternalException`

Si è verificato un errore imprevisto.

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

## DeprecateThingType

Dichiara obsoleto un tipo di oggetto. Non puoi associare nuovi oggetti a un tipo di oggetto obsoleto.

## Riepilogo

```
aws iot deprecate-thing-type \
 --thing-type-name <value> \
 [--undo-deprecate | --no-undo-deprecate] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "thingTypeName": "string",
 "undoDeprecate": "boolean"
}
```

## Campi di cli-input-json

| Nome          | Tipo                                                                  | Descrizione                                                                                                                                              |
|---------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingTypeName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del tipo di oggetto da dichiarare obsoleto.                                                                                                         |
| undoDeprecate | booleano                                                              | Specifica se non dichiarare più obsoleto un tipo di oggetto obsoleto. Se è true, il tipo di oggetto non sarà più obsoleto e potrai associarlo a oggetti. |

## Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

# DescribeAccountAuditConfiguration

Ottiene informazioni sulle impostazioni di Device Defender Audit per l'account. Le impostazioni includono la modalità di invio delle notifiche degli audit e i controlli di auditing abilitati o disabilitati.

## Riepilogo

```
aws iot describe-account-audit-configuration \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
}
```

## Output

```
{
 "roleArn": "string",
 "auditNotificationTargetConfigurations": {
 "string": {
 "targetArn": "string",
 "roleArn": "string",
 "enabled": "boolean"
 }
 },
 "auditCheckConfigurations": {
 "string": {
 "enabled": "boolean"
 }
 }
}
```

## Campi di output dell'interfaccia a riga di comando

| Nome                                  | Tipo                                     | Descrizione                                                                                                                                                                                                                                                                            |
|---------------------------------------|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn                               | Stringa<br>Lunghezza max: 2048, min.: 20 | ARN del ruolo che concede ad AWS IoT l'autorizzazione per accedere alle informazioni su dispositivi, policy, certificati e altri elementi necessari per eseguire un audit.<br><br>Nella prima chiamata a <code>UpdateAccountAuditConfiguration</code> questo parametro è obbligatorio. |
| auditNotificationTargetConfigurations | mappa                                    | Informazioni sui target a cui vengono inviate le notifiche di auditing per l'account.                                                                                                                                                                                                  |
| targetArn                             | Stringa                                  | ARN del target (argomento SNS) a cui vengono inviate le notifiche di auditing.                                                                                                                                                                                                         |

| Nome                     | Tipo     | Descrizione                                                                                                        |
|--------------------------|----------|--------------------------------------------------------------------------------------------------------------------|
| roleArn                  | Stringa  | ARN del ruolo che concede l'autorizzazione per l'invio delle notifiche al target.<br>Lunghezza max: 2048, min.: 20 |
| enabled                  | booleano | True se le notifiche per il target sono abilitate.                                                                 |
| auditCheckConfigurations | mappa    | Specifica i controlli di auditing abilitati e disabilitati per l'account.                                          |
| enabled                  | booleano | True se il controllo di auditing è abilitato per l'account.                                                        |

Errori

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DescribeAuditTask

Ottiene le informazioni su un audit di Device Defender.

Riepilogo

```
aws iot describe-audit-task \
--task-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "taskId": "string"
}
```

Campi di **cli-input-json**

| Nome   | Tipo    | Descrizione                                                                                            |
|--------|---------|--------------------------------------------------------------------------------------------------------|
| taskId | Stringa | ID dell'audit di cui ottenere le informazioni.<br>Lunghezza max: 40, min.: 1<br>Modello: [a-zA-Z0-9-]+ |

Output

```
{
 "taskStatus": "string",
 "taskType": "string",
```

```

"taskStartTime": "timestamp",
"taskStatistics": {
 "totalChecks": "integer",
 "inProgressChecks": "integer",
 "waitingForDataCollectionChecks": "integer",
 "compliantChecks": "integer",
 "nonCompliantChecks": "integer",
 "failedChecks": "integer",
 "canceledChecks": "integer"
},
"scheduledAuditName": "string",
"auditDetails": {
 "string": {
 "checkRunStatus": "string",
 "checkCompliant": "boolean",
 "totalResourcesCount": "long",
 "nonCompliantResourcesCount": "long",
 "errorCode": "string",
 "message": "string"
 }
}
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome                           | Tipo           | Descrizione                                                                                                                                         |
|--------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| taskStatus                     | Stringa        | Stato dell'audit: un valore tra "IN_PROGRESS", "COMPLETED", "FAILED" o "CANCELED".<br><br>enumerazione: IN_PROGRESS   COMPLETED   FAILED   CANCELED |
| taskType                       | Stringa        | Tipo di audit: "ON_DEMAND_AUDIT_TASK" o "SCHEDULED_AUDIT_TASK".<br><br>enumerazione: ON_DEMAND_AUDIT_TASK   SCHEDULED_AUDIT_TASK                    |
| taskStartTime                  | timestamp      | Ora di inizio dell'audit.                                                                                                                           |
| taskStatistics                 | TaskStatistics | Informazioni statistiche sull'audit.                                                                                                                |
| totalChecks                    | intero         | Numero di controlli nell'audit.                                                                                                                     |
| inProgressChecks               | intero         | Numero di controlli in corso.                                                                                                                       |
| waitingForDataCollectionChecks | intero         | Numero di controlli in attesa della raccolta dei dati.                                                                                              |
| compliantChecks                | intero         | Numero di controlli che hanno trovato risorse conformi.                                                                                             |
| nonCompliantChecks             | intero         | Numero di controlli che hanno trovato risorse non conformi.                                                                                         |
| failedChecks                   | intero         | Numero di controlli                                                                                                                                 |

| Nome                       | Tipo                                                                        | Descrizione                                                                                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| canceledChecks             | intero                                                                      | Numero di controlli non eseguiti perché l'audit è stato annullato.                                                                                                                                                                                                                                            |
| scheduledAuditName         | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 _]+ | Nome dell'audit pianificato (solo se l'audit è di tipo pianificato).                                                                                                                                                                                                                                          |
| auditDetails               | mappa                                                                       | Informazioni dettagliate su ogni controllo eseguito durante l'audit.                                                                                                                                                                                                                                          |
| checkRunStatus             | Stringa                                                                     | Stato di completamento del controllo. Un valore tra "IN_PROGRESS", "WAITING_FOR_DATA_COLLECTION", "CANCELED", "COMPLETED_COMPLIANT", "COMPLETED_NON_COMPLIANT" o "FAILED".<br><br>enumerazione: IN_PROGRESS   WAITING_FOR_DATA_COLLECTION   CANCELED   COMPLETED_COMPLIANT   COMPLETED_NON_COMPLIANT   FAILED |
| checkCompliant             | booleano                                                                    | True se il controllo è stato completato e ha trovato tutte le risorse conformi.                                                                                                                                                                                                                               |
| totalResourcesCount        | Long                                                                        | Numero di risorse su cui è stato eseguito il controllo.                                                                                                                                                                                                                                                       |
| nonCompliantResourcesCount | Long                                                                        | Numero di risorse che dal controllo sono risultate non conformi.                                                                                                                                                                                                                                              |
| errorCode                  | Stringa                                                                     | Codice degli errori rilevati durante l'esecuzione del controllo nel corso dell'audit. Un valore tra "INSUFFICIENT_PERMISSIONS" o "AUDIT_CHECK_DISABLED".                                                                                                                                                      |
| message                    | Stringa<br><br>Lunghezza max: 2048                                          | Messaggio associato agli errori rilevati durante l'esecuzione del controllo nel corso dell'audit.                                                                                                                                                                                                             |

## Errori

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ResourceNotFoundException

La risorsa specificata non esiste.

### ThrottlingException

La velocità supera il limite.

### InternalFailureException

Si è verificato un errore imprevisto.

## DescribeAuthorizer

Describe un'autorizzazione.

### Riepilogo

```
aws iot describe-authorizer \
 --authorizer-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "authorizerName": "string"
}
```

### Campi di cli-input-json

| Nome           | Tipo                                                        | Descrizione                             |
|----------------|-------------------------------------------------------------|-----------------------------------------|
| authorizerName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [w=,@-]+ | Nome dell'autorizzazione da descrivere. |

### Output

```
{
 "authorizerDescription": {
 "authorizerName": "string",
 "authorizerArn": "string",
 "authorizerFunctionArn": "string",
 "tokenKeyName": "string",
 "tokenSigningPublicKeys": {
 "string": "string"
 },
 "status": "string",
 "creationDate": "timestamp",
 "lastModifiedDate": "timestamp"
 }
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome                  | Tipo                  | Descrizione                      |
|-----------------------|-----------------------|----------------------------------|
| authorizerDescription | AuthorizerDescription | Descrizione dell'autorizzazione. |

| Nome                   | Tipo                                                                         | Descrizione                                                                                                         |
|------------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| authorizerName         | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=,@-]+          | Nome dell'autorizzazione.                                                                                           |
| authorizerArn          | Stringa                                                                      | ARN dell'autorizzazione.                                                                                            |
| authorizerFunctionArn  | Stringa                                                                      | ARN della funzione Lambda dell'autorizzazione.                                                                      |
| tokenKeyName           | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Chiave usata per estrarre il token dalle intestazioni HTTP.                                                         |
| tokenSigningPublicKeys | mappa                                                                        | Chiavi pubbliche usate per convalidare la firma del token restituita dal servizio di autenticazione personalizzato. |
| status                 | Stringa                                                                      | Stato dell'autorizzazione.<br><br>Enumerazione: ACTIVE   INACTIVE                                                   |
| creationDate           | Timestamp                                                                    | Timestamp UNIX del momento in cui l'autorizzazione è stata creata.                                                  |
| lastModifiedDate       | Timestamp                                                                    | Timestamp UNIX dell'ultimo aggiornamento dell'autorizzazione.                                                       |

## Errori

### ResourceNotFoundException

La risorsa specificata non esiste.

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ThrottlingException

La velocità supera il limite.

### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

### InternalFailureException

Si è verificato un errore imprevisto.

# DescribeBillingGroup

Restituisce informazioni su un gruppo di fatturazione.

Riepilogo

```
aws iot describe-billing-group \
--billing-group-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "billingGroupName": "string"
}
```

Campi di `cli-input-json`

| Nome             | Tipo                                                                  | Descrizione                         |
|------------------|-----------------------------------------------------------------------|-------------------------------------|
| billingGroupName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+ | Il nome del gruppo di fatturazione. |

Output

```
{
 "billingGroupName": "string",
 "billingGroupId": "string",
 "billingGroupArn": "string",
 "version": "long",
 "billingGroupProperties": {
 "billingGroupDescription": "string"
 },
 "billingGroupMetadata": {
 "creationDate": "timestamp"
 }
}
```

Campi di output dell'interfaccia a riga di comando

| Nome             | Tipo                                                                  | Descrizione                         |
|------------------|-----------------------------------------------------------------------|-------------------------------------|
| billingGroupName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+ | Il nome del gruppo di fatturazione. |
| billingGroupId   | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :-]+  | L'ID del gruppo di fatturazione.    |

| Nome                    | Tipo                                                            | Descrizione                                              |
|-------------------------|-----------------------------------------------------------------|----------------------------------------------------------|
| billingGroupArn         | Stringa                                                         | L'ARN del gruppo di fatturazione.                        |
| version                 | Long                                                            | La versione del gruppo di fatturazione.                  |
| billingGroupProperties  | BillingGroupProperties                                          | Le proprietà del gruppo di fatturazione.                 |
| billingGroupDescription | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [\p{Graph}]* | La descrizione del gruppo di fatturazione.               |
| billingGroupMetadata    | BillingGroupMetadata                                            | Informazioni aggiuntive sul gruppo di fatturazione.      |
| creationDate            | timestamp                                                       | La data e l'ora di creazione del gruppo di fatturazione. |

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ResourceNotFoundException**

La risorsa specificata non esiste.

## DescribeCACertificate

Describe un certificato CA registrato.

Riepilogo

```
aws iot describe-ca-certificate \
--certificate-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "certificateId": "string"
}
```

### Campi di **cli-input-json**

| Nome          | Tipo                                                                           | Descrizione                        |
|---------------|--------------------------------------------------------------------------------|------------------------------------|
| certificateId | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | Identificatore del certificato CA. |

### Output

```
{
 "certificateDescription": {
 "certificateArn": "string",
 "certificateId": "string",
 "status": "string",
 "certificatePem": "string",
 "ownedBy": "string",
 "creationDate": "timestamp",
 "autoRegistrationStatus": "string",
 "lastModifiedDate": "timestamp",
 "customerVersion": "integer",
 "generationId": "string",
 "validity": {
 "notBefore": "timestamp",
 "notAfter": "timestamp"
 }
 },
 "registrationConfig": {
 "templateBody": "string",
 "roleArn": "string"
 }
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome                   | Tipo                                                                           | Descrizione                                                        |
|------------------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------|
| certificateDescription | CACertificateDescription                                                       | Descrizione del certificato CA.                                    |
| certificateArn         | Stringa                                                                        | ARN del certificato CA.                                            |
| certificateId          | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | ID certificato CA.                                                 |
| status                 | Stringa                                                                        | Stato di un certificato CA.<br><br>Enumerazione: ACTIVE   INACTIVE |
| certificatePem         | Stringa<br><br>Lunghezza max: 65536, min.: 1                                   | Dati del certificato CA, in formato PEM.                           |
| ownedBy                | Stringa<br><br>Lunghezza max: 12, min.: 12                                     | Proprietario del certificato CA.                                   |

| Nome                   | Tipo                                         | Descrizione                                                                                                                                                                                   |
|------------------------|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | Modello: [0-9]+                              |                                                                                                                                                                                               |
| creationDate           | Timestamp                                    | Data di creazione del certificato CA.                                                                                                                                                         |
| autoRegistrationStatus | Stringa                                      | Specifica se il certificato CA è configurato per la registrazione automatica dei certificati dei dispositivi. I valori validi sono "ENABLE" e "DISABLE"<br><br>Enumerazione: ENABLE   DISABLE |
| lastModifiedDate       | Timestamp                                    | La data dell'ultima modifica del certificato CA.                                                                                                                                              |
| customerVersion        | intero<br><br>Intervallo - min.: 1           | La versione del cliente del certificato CA.                                                                                                                                                   |
| generationId           | Stringa                                      | L'ID di generazione del certificato CA.                                                                                                                                                       |
| validity               | CertificateValidity                          | Quando il certificato CA è valido.                                                                                                                                                            |
| notBefore              | timestamp                                    | Il certificato non è valido prima di questa data.                                                                                                                                             |
| notAfter               | timestamp                                    | Il certificato non è valido dopo di questa data.                                                                                                                                              |
| registrationConfig     | RegistrationConfig                           | Informazioni sulla configurazione della registrazione.                                                                                                                                        |
| templateBody           | Stringa                                      | Corpo del modello.                                                                                                                                                                            |
| roleArn                | Stringa<br><br>Lunghezza max: 2048, min.: 20 | ARN del ruolo.                                                                                                                                                                                |

## Errori

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ThrottlingException

La velocità supera il limite.

### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

### InternalFailureException

Si è verificato un errore imprevisto.

### ResourceNotFoundException

La risorsa specificata non esiste.

## DescribeCertificate

Ottiene informazioni sul certificato specificato.

### Riepilogo

```
aws iot describe-certificate \
--certificate-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di `cli-input-json`

```
{
 "certificateId": "string"
}
```

### Campi di `cli-input-json`

| Nome          | Tipo                                                                           | Descrizione                                                                            |
|---------------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| certificateId | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato. L'ultima parte dell'ARN del certificato contiene l'ID certificato. |

### Output

```
{
 "certificateDescription": {
 "certificateArn": "string",
 "certificateId": "string",
 "caCertificateId": "string",
 "status": "string",
 "certificatePem": "string",
 "ownedBy": "string",
 "previousOwnedBy": "string",
 "creationDate": "timestamp",
 "lastModifiedDate": "timestamp",
 "customerVersion": "integer",
 "transferData": {
 "transferMessage": "string",
 "rejectReason": "string",
 "transferDate": "timestamp",
 "acceptDate": "timestamp",
 "rejectDate": "timestamp"
 },
 "generationId": "string",
 "validity": {
 "notBefore": "timestamp",
 "notAfter": "timestamp"
 }
 }
}
```

```
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome                   | Tipo                                                                                                                 | Descrizione                                                      |
|------------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| certificateDescription | CertificateDescription                                                                                               | Descrizione del certificato.                                     |
| certificateArn         | Stringa                                                                                                              | ARN del certificato.                                             |
| certificateId          | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+                                       | ID del certificato.                                              |
| caCertificateId        | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+                                       | ID del certificato CA usato per firmare questo certificato.      |
| status                 | Stringa<br><br>Enumerazione: ACTIVE   INACTIVE   REVOKED   PENDING_TRANSFER   REGISTER_INACTIVE   PENDING_ACTIVATION | Stato del certificato.                                           |
| certificatePem         | Stringa<br><br>Lunghezza max: 65536, min.: 1                                                                         | Dati del certificato, in formato PEM.                            |
| ownedBy                | Stringa<br><br>Lunghezza max: 12, min.: 12<br><br>Modello: [0-9]+                                                    | ID dell'account AWS proprietario del certificato.                |
| previousOwnedBy        | Stringa<br><br>Lunghezza max: 12, min.: 12<br><br>Modello: [0-9]+                                                    | ID dell'account AWS del proprietario precedente del certificato. |
| creationDate           | Timestamp                                                                                                            | Data e ora di creazione del certificato.                         |
| lastModifiedDate       | Timestamp                                                                                                            | Data e ora dell'ultima modifica del certificato.                 |
| customerVersion        | intero<br><br>Intervallo - min.: 1                                                                                   | La versione del cliente del certificato.                         |
| transferData           | TransferData                                                                                                         | Dati del trasferimento.                                          |
| transferMessage        | Stringa<br><br>Lunghezza max: 128                                                                                    | Messaggio di trasferimento.                                      |

| Nome         | Tipo                          | Descrizione                                        |
|--------------|-------------------------------|----------------------------------------------------|
| rejectReason | Stringa<br>Lunghezza max: 128 | Motivo per cui il trasferimento è stato rifiutato. |
| transferDate | Timestamp                     | Data in cui il trasferimento è avvenuto.           |
| acceptDate   | Timestamp                     | Data in cui il trasferimento è stato accettato.    |
| rejectDate   | Timestamp                     | Data in cui il trasferimento è stato rifiutato.    |
| generationId | Stringa                       | L'ID di generazione del certificato.               |
| validity     | CertificateValidity           | Quando il certificato è valido.                    |
| notBefore    | timestamp                     | Il certificato non è valido prima di questa data.  |
| notAfter     | timestamp                     | Il certificato non è valido dopo di questa data.   |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

##### InternalFailureException

Si è verificato un errore imprevisto.

##### ResourceNotFoundException

La risorsa specificata non esiste.

## DescribeDefaultAuthorizer

Describe l'autorizzazione predefinita.

#### Riepilogo

```
aws iot describe-default-authorizer \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di cli-input-json

```
{
}
```

Output

```
{
 "authorizerDescription": {
 "authorizerName": "string",
 "authorizerArn": "string",
 "authorizerFunctionArn": "string",
 "tokenKeyName": "string",
 "tokenSigningPublicKeys": {
 "string": "string"
 },
 "status": "string",
 "creationDate": "timestamp",
 "lastModifiedDate": "timestamp"
 }
}
```

Campi di output dell'interfaccia a riga di comando

| Nome                   | Tipo                  | Descrizione                                                                                                                      |
|------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------|
| authorizerDescription  | AuthorizerDescription | Descrizione dell'autorizzazione predefinita.                                                                                     |
| authorizerName         | Stringa               | Nome dell'autorizzazione.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=,@-]+                                            |
| authorizerArn          | Stringa               | ARN dell'autorizzazione.                                                                                                         |
| authorizerFunctionArn  | Stringa               | ARN della funzione Lambda dell'autorizzazione.                                                                                   |
| tokenKeyName           | Stringa               | Chiave usata per estrarre il token dalle intestazioni HTTP.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ |
| tokenSigningPublicKeys | mappa                 | Chiavi pubbliche usate per convalidare la firma del token restituita dal servizio di autenticazione personalizzato.              |
| status                 | Stringa               | Stato dell'autorizzazione.<br><br>Enumerazione: ACTIVE   INACTIVE                                                                |
| creationDate           | Timestamp             | Timestamp UNIX del momento in cui l'autorizzazione è stata creata.                                                               |

| Nome             | Tipo      | Descrizione                                                   |
|------------------|-----------|---------------------------------------------------------------|
| lastModifiedDate | Timestamp | Timestamp UNIX dell'ultimo aggiornamento dell'autorizzazione. |

#### Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DescribeEndpoint

Restituisce un endpoint univoco specifico per l'account AWS che effettua la chiamata.

#### Riepilogo

```
aws iot describe-endpoint \
[--endpoint-type <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "endpointType": "string"
}
```

#### Campi di **cli-input-json**

| Nome         | Tipo    | Descrizione                                                                                                                                                                              |
|--------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| endpointType | Stringa | <p>Tipo di endpoint. I tipi di endpoint validi includono:</p> <ul style="list-style-type: none"> <li>• <b>iot:Data</b>: restituisce un endpoint di dati firmati con VeriSign.</li> </ul> |

| Nome | Tipo | Descrizione                                                                                                                                                                                                                                                                                                                            |
|------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |      | <ul style="list-style-type: none"> <li>• <b>iot:Data-ATS</b>: restituisce un endpoint di dati firmati con ATS.</li> <li>• <b>iot:CredentialProvider</b>: restituisce un endpoint API del fornitore di credenziali AWS IoT.</li> <li>• <b>iot:Jobs</b> - Restituisce un endpoint API dei progetti AWS IoT Device Management.</li> </ul> |

#### Output

```
{
 "endpointAddress": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome            | Tipo    | Descrizione                                                                           |
|-----------------|---------|---------------------------------------------------------------------------------------|
| endpointAddress | Stringa | Endpoint. Il formato dell'endpoint è questo: identificatore.iot.region.amazonaws.com. |

#### Errori

**InternalFailureException**

Si è verificato un errore imprevisto.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ThrottlingException**

La velocità supera il limite.

## DescribeEventConfigurations

Describe le configurazioni dell'evento.

#### Riepilogo

```
aws iot describe-event-configurations \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di cli-input-json

```
{
}
```

Output

```
{
 "eventConfigurations": {
 "string": {
 "Enabled": "boolean"
 }
 },
 "creationDate": "timestamp",
 "lastModifiedDate": "timestamp"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome                | Tipo      | Descrizione                                                 |
|---------------------|-----------|-------------------------------------------------------------|
| eventConfigurations | mappa     | Configurazioni dell'evento.                                 |
| Enabled             | booleano  | True per abilitare la configurazione.                       |
| creationDate        | Timestamp | Data di creazione della configurazione dell'evento.         |
| lastModifiedDate    | timestamp | Data dell'ultima modifica delle configurazioni dell'evento. |

Errori

`InternalFailureException`

Si è verificato un errore imprevisto.

`ThrottlingException`

La velocità supera il limite.

## DescribelIndex

Describe un indice di ricerca.

Riepilogo

```
aws iot describe-index \
 --index-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di cli-input-json

```
{
```

```
{
 "indexName": "string"
}
```

#### Campi di **cli-input-json**

| Nome      | Tipo                                                                          | Descrizione       |
|-----------|-------------------------------------------------------------------------------|-------------------|
| indexName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome dell'indice. |

#### Output

```
{
 "indexName": "string",
 "indexStatus": "string",
 "schema": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome        | Tipo                                                                          | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| indexName   | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome dell'indice.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| indexStatus | Stringa<br><br>Enumerazione: ACTIVE   BUILDING   REBUILDING                   | Stato dell'indice.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| schema      | Stringa                                                                       | Contiene un valore che specifica il tipo di indicizzazione eseguita. I valori validi sono: <ul style="list-style-type: none"><li>• REGISTRY – L'indice dell'oggetto contiene solo dati del registro.</li><li>• REGISTRY_AND_SHADOW – L'indice dell'oggetto contiene i dati shadow e del registro.</li><li>• REGISTRY_AND_CONNECTIVITY_STATUS – L'indice dell'oggetto contiene i dati del registro e i dati sullo stato di connettività dell'oggetto.</li><li>• REGISTRY_AND_SHADOW_AND_CONNECTIVITY_STATUS – L'indice dell'oggetto contiene i dati del registro, i dati shadow e i dati sullo stato di connettività dell'oggetto.</li></ul> |

## Errori

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ThrottlingException

La velocità supera il limite.

### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

### InternalFailureException

Si è verificato un errore imprevisto.

### ResourceNotFoundException

La risorsa specificata non esiste.

## DescribeJob

Describe un processo.

### Riepilogo

```
aws iot describe-job \
--job-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "jobId": "string"
}
```

### Campi di cli-input-json

| Nome  | Tipo                                                                        | Descrizione                                                              |
|-------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------|
| jobId | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Identificatore univoco assegnato al processo al momento della creazione. |

### Output

```
{
 "documentSource": "string",
 "job": {
 "jobArn": "string",
 "jobId": "string",
 "targetSelection": "string",
```

```

 "status": "string",
 "forceCanceled": "boolean",
 "reasonCode": "string",
 "comment": "string",
 "targets": [
 "string"
],
 "description": "string",
 "presignedUrlConfig": {
 "roleArn": "string",
 "expiresInSec": "long"
 },
 "jobExecutionsRolloutConfig": {
 "maximumPerMinute": "integer",
 "exponentialRate": {
 "baseRatePerMinute": "integer",
 "incrementFactor": "double",
 "rateIncreaseCriteria": {
 "numberOfNotifiedThings": "integer",
 "numberOfSucceededThings": "integer"
 }
 }
 },
 "abortConfig": {
 "criteriaList": [
 {
 "failureType": "string",
 "action": "string",
 "thresholdPercentage": "double",
 "minNumberOfExecutedThings": "integer"
 }
]
 },
 "createdAt": "timestamp",
 "lastUpdatedAt": "timestamp",
 "completedAt": "timestamp",
 "jobProcessDetails": {
 "processingTargets": [
 "string"
],
 "numberOfCanceledThings": "integer",
 "numberOfSucceededThings": "integer",
 "numberOfFailedThings": "integer",
 "numberOfRejectedThings": "integer",
 "numberOfQueuedThings": "integer",
 "numberOfInProgressThings": "integer",
 "numberOfRemovedThings": "integer",
 "numberOfTimedOutThings": "integer"
 },
 "timeoutConfig": {
 "inProgressTimeoutInMinutes": "long"
 }
}
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo                                        | Descrizione                                |
|----------------|---------------------------------------------|--------------------------------------------|
| documentSource | Stringa<br><br>Lunghezza max: 1350, min.: 1 | Collegamento S3 al documento del processo. |
| job            | Processo                                    | Informazioni sul processo.                 |

| Nome            | Tipo                                                                        | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobArn          | Stringa                                                                     | ARN che identifica il processo in formato "arn:aws:iot:regione:account:processo/jobId".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| jobId           | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| targetSelection | Stringa                                                                     | Specifica se l'esecuzione del processo continuerà (CONTINUOUS) o se il processo verrà completato dopo che tutti gli oggetti specificati come target avranno completato il processo (SNAPSHOT). Se è continuo, il processo può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Un processo viene ad esempio eseguito in un dispositivo quando l'oggetto che rappresenta il dispositivo viene aggiunto a un gruppo target, anche dopo che il processo è stato completato da tutti gli oggetti originariamente nel gruppo.<br><br>Enumerazione: CONTINUOUS   SNAPSHOT |
| status          | Stringa                                                                     | Stato del processo, IN_PROGRESS, CANCELED, DELETION_IN_PROGRESS o COMPLETED.<br><br>enum: IN_PROGRESS   CANCELED   COMPLETED   DELETION_IN_PROGRESS                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| forceCanceled   | booleano                                                                    | Sarà true se il processo è stato annullato con il parametro opzionale force impostato su true.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| reasonCode      | Stringa<br><br>Lunghezza max: 128<br><br>Modello: [\p{Upper}\p{Digit}_]+    | Se il processo è stato aggiornato, fornisce il codice del motivo dell'aggiornamento.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Nome                       | Tipo                                                 | Descrizione                                                                                                                                                                                                                                                     |
|----------------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| comment                    | Stringa<br>Lunghezza max: 2028<br>Modello: [^\p{C}]+ | Se il processo è stato aggiornato, descrive il motivo dell'aggiornamento.                                                                                                                                                                                       |
| targets                    | elenco<br>Membro: TargetArn                          | Elenco di oggetti e gruppi di oggetti IoT a cui deve essere inviato il processo.                                                                                                                                                                                |
| description                | Stringa<br>Lunghezza max: 2028<br>Modello: [^\p{C}]+ | Breve descrizione di testo del processo.                                                                                                                                                                                                                        |
| presignedUrlConfig         | PresignedUrlConfig                                   | Configurazione per gli URL S3 prefissati.                                                                                                                                                                                                                       |
| roleArn                    | Stringa<br>Lunghezza max: 2048, min.: 20             | L'ARN di un ruolo IAM che concede l'autorizzazione per scaricare file dal bucket S3 in cui vengono archiviati i dati e gli aggiornamenti del processo. Il ruolo deve anche concedere l'autorizzazione per IoT per il download dei file.                         |
| expiresInSec               | Long<br>Intervallo – Max: 3600, min.: 60             | Periodo di validità (in secondi) degli URL prefissati. I valori validi sono compresi tra 60 e 3600 e il valore predefinito è 3600 secondi. Gli URL prefissati vengono generati quando il servizio Jobs riceve una richiesta MQTT per il documento del processo. |
| jobExecutionsRolloutConfig | JobExecutionsRolloutConfig                           | Permette di creare un'implementazione per fasi di un processo.                                                                                                                                                                                                  |
| maximumPerMinute           | intero<br>Intervallo - min.: 1                       | Numero massimo di oggetti che riceveranno una notifica di un processo in sospeso, ogni minuto. Questo parametro permette di creare un'implementazione per fasi.                                                                                                 |
| exponentialRate            | ExponentialRolloutRate                               | La velocità di aumento di un rollout di processo. Questo parametro consente di definire una velocità esponenziale per un rollout di processo.                                                                                                                   |

| Nome                      | Tipo                                                                   | Descrizione                                                                                                                                                                                                   |
|---------------------------|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| baseRatePerMinute         | intero<br><br>Intervallo – Max: 1000, min.: 1                          | Il numero minimo di oggetti che riceveranno una notifica di un processo in sospeso, ogni minuto all'inizio del rollout di processo. Questo parametro consente di definire la velocità iniziale di un rollout. |
| rateIncreaseCriteria      | RateIncreaseCriteria                                                   | I criteri per avviare l'aumento della velocità di rollout per un processo.<br><br>AWS IoT supporta fino a una cifra dopo il decimale (ad esempio, 1,5 ma non 1,55).                                           |
| numberOfNotifiedThings    | intero<br><br>Intervallo - min.: 1                                     | La soglia per il numero di oggetti notificati che avvierà l'aumento della velocità di rollout.                                                                                                                |
| numberOfSucceededThings   | intero<br><br>Intervallo - min.: 1                                     | La soglia per il numero di oggetti completati che avvierà l'aumento della velocità di rollout.                                                                                                                |
| abortConfig               | AbortConfig                                                            | Configurazione dei criteri per interrompere il processo.                                                                                                                                                      |
| criteriaList              | elenco<br><br>member: AbortCriteria<br><br>Classe Java: java.util.List | L'elenco dei criteri di eliminazione per definire regole per interrompere il processo.                                                                                                                        |
| failureType               | Stringa                                                                | Il tipo di errore di esecuzione di processo per definire una regola di avvio dell'interruzione di un processo.<br><br>enum: FAILED   REJECTED   TIMED_OUT   ALL                                               |
| action                    | Stringa                                                                | Il tipo di operazione di eliminazione per avviare l'interruzione di un processo.<br><br>enum: CANCEL                                                                                                          |
| minNumberOfExecutedThings | intero<br><br>Intervallo - min.: 1                                     | Il numero minimo di oggetti eseguiti prima della valutazione della regola di interruzione.                                                                                                                    |
| createdAt                 | Timestamp                                                              | Periodo di tempo, in secondi, dall'epoca (Unix epoch) alla creazione del processo.                                                                                                                            |

| Nome                     | Tipo                                                                          | Descrizione                                                                                                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lastUpdatedAt            | timestamp                                                                     | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento del processo.                                                                                                                        |
| completedAt              | timestamp                                                                     | Periodo di tempo, in secondi, dall'epoca al completamento del processo.                                                                                                                                             |
| jobProcessDetails        | JobProcessDetails                                                             | Dettagli sull'elaborazione del processo.                                                                                                                                                                            |
| processingTargets        | elenco<br><br>Membro: ProcessingTargetName<br><br>Classe Java: java.util.List | I dispositivi di destinazione sui quali viene implementata l'esecuzione del processo. Questo valore sarà nullo al termine dell'implementazione dell'esecuzione dei processi su tutti i dispositivi di destinazione. |
| numberOfCanceledThings   | intero                                                                        | Numero di oggetti che hanno annullato il processo.                                                                                                                                                                  |
| numberOfSucceededThings  | intero                                                                        | Numero di oggetti che hanno completato il processo.                                                                                                                                                                 |
| numberOfFailedThings     | intero                                                                        | Numero di oggetti che non hanno eseguito il processo.                                                                                                                                                               |
| numberOfRejectedThings   | intero                                                                        | Numero di oggetti che hanno rifiutato il processo.                                                                                                                                                                  |
| numberOfQueuedThings     | intero                                                                        | Numero di oggetti che sono in attesa dell'esecuzione del processo.                                                                                                                                                  |
| numberOfInProgressThings | intero                                                                        | Numero di oggetti che stanno attualmente eseguendo il processo.                                                                                                                                                     |
| numberOfRemovedThings    | intero                                                                        | Numero di oggetti per cui non è più pianificata l'esecuzione del processo, perché sono stati eliminati o rimossi dal gruppo che costituiva un target del processo.                                                  |
| numberOfTimedOutThings   | intero                                                                        | Il numero di oggetti il cui stato di esecuzione del processo è <b>TIMED_OUT</b> .                                                                                                                                   |

| Nome                       | Tipo          | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| timeoutConfig              | TimeoutConfig | Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione del processo. Viene avviato un timer quando imposti lo stato di esecuzione del processo su <code>IN_PROGRESS</code> . Se lo stato di esecuzione del processo non è impostato su un altro stato terminale prima del timeout, verrà automaticamente impostato su <code>TIMED_OUT</code> .                                                                                                                                                                                                  |
| inProgressTimeoutInMinutes | Long          | Specifica l'intervallo di tempo, in minuti, a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. L'intervallo di timeout può essere compreso fra 1 minuto e 7 giorni (da 1 a 10080 minuti). Il timer in corso non può essere aggiornato e verrà applicato a tutte le esecuzioni del processo. Se l'esecuzione del processo resta nello stato <code>IN_PROGRESS</code> per un periodo di tempo superiore a quello consentito dall'intervallo, l'esecuzione del processo non andrà a buon fine e verrà impostato lo stato <code>TIMED_OUT</code> terminale. |

## Errori

### `InvalidRequestException`

I contenuti della richiesta non sono validi.

### `ResourceNotFoundException`

La risorsa specificata non esiste.

### `ThrottlingException`

La velocità supera il limite.

### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

## DescribeJobExecution

Ottiene i dettagli di un'esecuzione del processo.

### Riepilogo

```
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]
```

Formato di **cli-input-json**

```
{
 "jobId": "string",
 "thingName": "string",
 "includeJobDocument": "boolean",
 "executionNumber": "long"
}
```

Campi di **cli-input-json**

| Nome               | Tipo                                                                  | Descrizione                                                                                                                                                                      |
|--------------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId              | Stringa<br>Modello: [a-z A-Z 0-9 _-]+ ^\$next                         | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                         |
| thingName          | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto associato al dispositivo in cui è in corso l'esecuzione del processo.                                                                                          |
| includeJobDocument | booleano                                                              | Opzionale. A meno che non sia impostato su false, la risposta contiene il documento del processo. Il valore predefinito è true.                                                  |
| executionNumber    | Long                                                                  | Opzionale. Numero che identifica una determinata esecuzione di un processo in un dispositivo specifico. Se non è specificato, viene restituita l'ultima esecuzione del processo. |

Output

```
{
 "execution": {
 "jobId": "string",
 "thingName": "string",
 "status": "string",
 "statusDetails": {
 "string": "string"
 },
 "queuedAt": "long",
 "startedAt": "long",
 "lastUpdatedAt": "long",
 "approximateSecondsBeforeTimedOut": "long",
 "approximateSecondsAfterTimedOut": "long"
 }
}
```

```

 "versionNumber": "long",
 "executionNumber": "long",
 "jobDocument": "string"
}
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome                             | Tipo                                                                  | Descrizione                                                                                                                                                                                                                                              |
|----------------------------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| execution                        | JobExecution                                                          | Contiene i dati sull'esecuzione di un processo.                                                                                                                                                                                                          |
| jobId                            | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a-z A-Z 0-9 _]+    | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                                                                                 |
| thingName                        | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto che sta eseguendo il processo.                                                                                                                                                                                                         |
| stato                            | Stringa                                                               | Stato dell'esecuzione del processo. Può essere "QUEUED", "IN_PROGRESS", "FAILED", "SUCCESS", "CANCELED", "TIMED_OUT", "REJECTED" o "REMOVED".<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED |
| statusDetails                    | mappa                                                                 | Raccolta di coppie nome/valore che descrivono lo stato dell'esecuzione del processo.                                                                                                                                                                     |
| queuedAt                         | Long                                                                  | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                                                                                               |
| startedAt                        | Long                                                                  | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                                                                                                            |
| lastUpdatedAt                    | Long                                                                  | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                                                                                                             |
| approximateSecondsBeforeTimedOut |                                                                       | Il numero stimato di secondi che rimangono prima che lo stato di esecuzione del processo venga modificato in TIMED_OUT.                                                                                                                                  |

| Nome            | Tipo                            | Descrizione                                                                                                                                                                                                           |
|-----------------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |                                 | L'effettivo timeout dell'esecuzione del processo può verificarsi 60 secondi dopo la durata stimata.                                                                                                                   |
| versionNumber   | Long                            | Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che vengono aggiornate da un dispositivo.                                                            |
| executionNumber | Long                            | Numero che identifica una determinata esecuzione di un processo in un dispositivo specifico. Può essere usato successivamente in comandi che restituiscono o aggiornano le informazioni sull'esecuzione del processo. |
| jobDocument     | Stringa<br>Lunghezza max: 32768 | Contenuto del documento del processo.                                                                                                                                                                                 |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `ThrottlingException`

La velocità supera il limite.

##### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

##### `CertificateValidationException`

Il certificato non è valido.

##### `TerminalStateException`

Il processo è in uno stato terminale.

## DescribeJobExecution

Describe un'esecuzione del processo.

#### Riepilogo

```
aws iot describe-job-execution \
```

```
--job-id <value> \
--thing-name <value> \
[--execution-number <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di `cli-input-json`

```
{
 "jobId": "string",
 "thingName": "string",
 "executionNumber": "long"
}
```

#### Campi di `cli-input-json`

| Nome            | Tipo                                                                  | Descrizione                                                                                                                                    |
|-----------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId           | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+   | Identificatore univoco assegnato al processo al momento della creazione.                                                                       |
| thingName       | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto in cui è in corso l'esecuzione del processo.                                                                                 |
| executionNumber | Long                                                                  | Stringa (costituita dalle cifre comprese tra 0 e 9) usata per specificare l'esecuzione di un determinato processo in un dispositivo specifico. |

#### Output

```
{
 "execution": {
 "jobId": "string",
 "status": "string",
 "forceCanceled": "boolean",
 "statusDetails": {
 "detailsMap": {
 "string": "string"
 }
 },
 "thingArn": "string",
 "queuedAt": "timestamp",
 "startedAt": "timestamp",
 "lastUpdatedAt": "timestamp",
 "executionNumber": "long",
 "versionNumber": "long",
 "approximateSecondsBeforeTimedOut": "long"
 }
}
```

Campi di output dell'interfaccia a riga di comando

| Nome            | Tipo                                                                       | Descrizione                                                                                                                                                                                                             |
|-----------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| execution       | JobExecution                                                               | Informazioni sull'esecuzione del processo.                                                                                                                                                                              |
| jobId           | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a–z A–Z 0–9 _]+ | Identificatore univoco assegnato al processo quando è stato creato.                                                                                                                                                     |
| stato           | Stringa                                                                    | Stato dell'esecuzione del processo (IN_PROGRESS, QUEUED, FAILED, SUCCEEDED, TIMED_OUT, CANCELED o REJECTED).<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED |
| forceCanceled   | booleano                                                                   | Sarà true se l'esecuzione del processo è stata annullata con il parametro opzionale force impostato su true.                                                                                                            |
| statusDetails   | JobExecutionStatusDetails                                                  | Raccolta di coppie nome/valore che descrivono lo stato dell'esecuzione del processo.                                                                                                                                    |
| detailsMap      | mappa                                                                      | Stato di esecuzione del processo.                                                                                                                                                                                       |
| thingArn        | Stringa                                                                    | ARN dell'oggetto in cui è in corso l'esecuzione del processo.                                                                                                                                                           |
| queuedAt        | timestamp                                                                  | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                                                              |
| startedAt       | timestamp                                                                  | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                                                                           |
| lastUpdatedAt   | timestamp                                                                  | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                                                                            |
| executionNumber | Long                                                                       | Stringa (costituita dalle cifre comprese tra 0 e 9) che identifica l'esecuzione di questo determinato processo in questo dispositivo specifico. Può essere usata in comandi che restituiscono o aggiornano le           |

| Nome                             | Tipo | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                  |      | informazioni di esecuzione del processo.                                                                                                                                                                                                                                                                                                                                                                            |
| versionNumber                    | Long | Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che vengono aggiornate da un dispositivo.                                                                                                                                                                                                                                                          |
| approximateSecondsBeforeTimedOut |      | Il numero stimato di secondi che rimangono prima che lo stato di esecuzione del processo venga modificato in TIMED_OUT. L'intervallo di timeout può essere compreso fra 1 minuto e 7 giorni (da 1 a 10080 minuti). L'effettivo timeout dell'esecuzione del processo può verificarsi 60 secondi dopo la durata stimata. Questo valore non sarà incluso se l'esecuzione del processo ha raggiunto lo stato terminale. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ResourceNotFoundException

La risorsa specificata non esiste.

##### ThrottlingException

La velocità supera il limite.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

## DescribeRoleAlias

Describe un alias del ruolo.

#### Riepilogo

```
aws iot describe-role-alias \
--role-alias <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
```

```

 "roleAlias": "string"
}
```

#### Campi di **cli-input-json**

| Nome      | Tipo                                                                | Descrizione                    |
|-----------|---------------------------------------------------------------------|--------------------------------|
| roleAlias | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=,@-]+ | Alias del ruolo da descrivere. |

#### Output

```
{
 "roleAliasDescription": {
 "roleAlias": "string",
 "roleAliasArn": "string",
 "roleArn": "string",
 "owner": "string",
 "credentialDurationSeconds": "integer",
 "creationDate": "timestamp",
 "lastModifiedDate": "timestamp"
 }
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome                      | Tipo                                                                | Descrizione                                                         |
|---------------------------|---------------------------------------------------------------------|---------------------------------------------------------------------|
| roleAliasDescription      | RoleAliasDescription                                                | Descrizione dell'alias del ruolo.                                   |
| roleAlias                 | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=,@-]+ | Alias del ruolo.                                                    |
| roleAliasArn              | Stringa                                                             | L'ARN dell'alias del ruolo.                                         |
| roleArn                   | Stringa                                                             | ARN del ruolo.                                                      |
| owner                     | Stringa<br><br>Lunghezza max: 12, min.: 12<br><br>Modello: [0-9]+   | Proprietario dell'alias del ruolo.                                  |
| credentialDurationSeconds | intero<br><br>Intervallo – Max: 3600, min.: 900                     | Numero di secondi di validità della credenziale.                    |
| creationDate              | Timestamp                                                           | Timestamp UNIX del momento in cui l'alias del ruolo è stato creato. |
| lastModifiedDate          | Timestamp                                                           | Timestamp UNIX dell'ultima modifica dell'alias del ruolo.           |

## Errori

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ThrottlingException

La velocità supera il limite.

### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

### InternalFailureException

Si è verificato un errore imprevisto.

### ResourceNotFoundException

La risorsa specificata non esiste.

## DescribeScheduledAudit

Ottiene le informazioni su un audit pianificato.

### Riepilogo

```
aws iot describe-scheduled-audit \
 --scheduled-audit-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "scheduledAuditName": "string"
}
```

### Campi di cli-input-json

| Nome               | Tipo                                                                         | Descrizione                                                  |
|--------------------|------------------------------------------------------------------------------|--------------------------------------------------------------|
| scheduledAuditName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Nome dell'audit pianificato di cui ottenere le informazioni. |

### Output

```
{
 "frequency": "string",
 "dayOfMonth": "string",
 "dayOfWeek": "string",
 "targetCheckNames": [
 "string"
```

```
],
"scheduledAuditName": "string",
"scheduledAuditArn": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome               | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                 |
|--------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| frequenza          | Stringa                                                                      | Frequenza di esecuzione dell'audit. Un valore tra "DAILY", "WEEKLY", "BIWEEKLY" o "MONTHLY". L'ora di inizio effettiva di ogni audit è determinata dal sistema.<br><br>enumerazione: DAILY   WEEKLY   BIWEEKLY   MONTHLY                                                                                                    |
| dayOfMonth         | Stringa<br><br>modello: ^([1-9] [12][0-9] 3[01])\$ ^LAST\$                   | Giorno del mese in cui viene eseguito l'audit pianificato. Il valore può essere compreso tra "1" e "31" oppure può essere "LAST". Se vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese.                                                             |
| dayOfWeek          | Stringa                                                                      | Giorno della settimana in cui viene eseguito l'audit pianificato. Un valore tra "SUN", "MON", "TUE", "WED", "THU", "FRI" o "SAT".<br><br>enumerazione: SUN   MON   TUE   WED   THU   FRI   SAT                                                                                                                              |
| targetCheckNames   | elenco<br><br>membro: AuditCheckName                                         | Controlli eseguiti durante l'audit pianificato. I controlli devono essere abilitati per l'account. Usa <a href="#">DescribeAccountAuditConfiguration</a> per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati, o <a href="#">UpdateAccountAuditConfiguration</a> per selezionare i controlli abilitati. |
| scheduledAuditName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Nome dell'audit pianificato.                                                                                                                                                                                                                                                                                                |
| scheduledAuditArn  | Stringa                                                                      | ARN dell'audit pianificato.                                                                                                                                                                                                                                                                                                 |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DescribeSecurityProfile

Ottiene le informazioni su un profilo di sicurezza di Device Defender.

Riepilogo

```
aws iot describe-security-profile \
--security-profile-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "securityProfileName": "string"
}
```

Campi di **cli-input-json**

| Nome                | Tipo                                                                  | Descrizione                                                    |
|---------------------|-----------------------------------------------------------------------|----------------------------------------------------------------|
| securityProfileName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del profilo di sicurezza di cui ottenere le informazioni. |

Output

```
{
 "securityProfileName": "string",
 "securityProfileArn": "string",
 "securityProfileDescription": "string",
 "behaviors": [
 {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 }
 }
 }
]
}
```

```

 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "statistic": "string"
 }
 }
],
"alertTargets": {
 "string": {
 "alertTargetArn": "string",
 "roleArn": "string"
 }
},
"additionalMetricsToRetain": [
 "string"
],
"version": "long",
"creationDate": "timestamp",
"lastModifiedDate": "timestamp"
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome                       | Tipo                                                                          | Descrizione                                                                                                               |
|----------------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| securityProfileName        | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del profilo di sicurezza.                                                                                            |
| securityProfileArn         | Stringa                                                                       | ARN del profilo di sicurezza.                                                                                             |
| securityProfileDescription | Stringa<br><br>Lunghezza max: 1000<br><br>Modello: [\p{Graph}]*               | Descrizione del profilo di sicurezza (associata al profilo di sicurezza al momento della creazione o dell'aggiornamento). |
| behaviors                  | elenco<br><br>membro: Behavior                                                | Specifica i comportamenti che, quando violati da un dispositivo (oggetto), causano la generazione di un avviso.           |
| name                       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome assegnato al comportamento.                                                                                          |
| metric                     | Stringa                                                                       | Valore misurato dal comportamento.                                                                                        |
| criteria                   | BehaviorCriteria                                                              | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a metric.                        |
| comparisonOperator         | Stringa                                                                       | Operatore che mette in correlazione l'oggetto                                                                             |

| Nome                                      | Tipo                                                     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           |                                                          | misurato ( <code>metric</code> ) e i criteri (contenenti un <code>value</code> o <code>statisticalThreshold</code> ).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set                                                                                                                                                                                                                                                                                                          |
| <code>value</code>                        | <code>MetricValue</code>                                 | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>count</code>                        | <code>Long</code><br><br>Intervallo - min.: 0            | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <code>cidrs</code>                        | <code>elenco</code><br><br>membro: <code>Cidr</code>     | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <code>ports</code>                        | <code>elenco</code><br><br>membro: <code>Port</code>     | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <code>durationSeconds</code>              | <code>intero</code>                                      | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |
| <code>consecutiveDatapointsToAlarm</code> | <code>intero</code><br><br>Intervallo – Max: 10, min.: 1 | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                      |

| Nome                         | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| consecutiveDatapointsToClear | intero<br><br>Intervallo – Max: 10, min.: 1                                  | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| statisticalThreshold         | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistic                    | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato ( <code>durationSeconds</code> ) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto ( <code>comparisonOperator</code> ) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario si verifica una violazione. |
| alertTargets                 | mappa                                                                        | Destinazione di invio degli avvisi. Gli avvisi vengono sempre inviati alla console.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| alertTargetArn               | Stringa                                                                      | ARN del target di notifica a cui vengono inviati gli avvisi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| roleArn                      | Stringa<br><br>Lunghezza max: 2048, min.: 20                                 | ARN del ruolo che concede l'autorizzazione per l'invio degli avvisi al target di notifica.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Nome                      | Tipo                             | Descrizione                                                                                                                                                                                                                                                  |
|---------------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| additionalMetricsToRetain | elenco<br>membro: BehaviorMetric | Un elenco di parametri i cui dati vengono conservati (archiviati). Per impostazione predefinita, i dati vengono conservati per qualsiasi parametro utilizzato nel behaviors del profilo ma vengono anche conservati per qualsiasi parametro specificato qui. |
| versione                  | Long                             | Versione del profilo di sicurezza. Viene generata una nuova versione ogni volta che il profilo di sicurezza viene aggiornato.                                                                                                                                |
| creationDate              | timestamp                        | Ora della creazione del profilo di sicurezza.                                                                                                                                                                                                                |
| lastModifiedDate          | timestamp                        | Ora dell'ultima modifica del profilo di sicurezza.                                                                                                                                                                                                           |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

## DescribeStream

Ottiene informazioni su un flusso.

#### Riepilogo

```
aws iot describe-stream \
--stream-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di `cli-input-json`

```
{
 "streamId": "string"
}
```

#### Campi di **cli-input-json**

| Nome     | Tipo                                                                 | Descrizione |
|----------|----------------------------------------------------------------------|-------------|
| streamId | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+ | ID flusso.  |

#### Output

```
{
 "streamInfo": {
 "streamId": "string",
 "streamArn": "string",
 "streamVersion": "integer",
 "description": "string",
 "files": [
 {
 "fileId": "integer",
 "s3Location": {
 "bucket": "string",
 "key": "string",
 "version": "string"
 }
 }
],
 "createdAt": "timestamp",
 "lastUpdatedAt": "timestamp",
 "roleArn": "string"
 }
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome          | Tipo                                                                 | Descrizione                        |
|---------------|----------------------------------------------------------------------|------------------------------------|
| streamInfo    | StreamInfo                                                           | Informazioni sul flusso.           |
| streamId      | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+ | ID flusso.                         |
| streamArn     | Stringa                                                              | ARN del flusso.                    |
| streamVersion | intero<br>Intervallo – Max: 65535, min.: 0                           | Versione del flusso.               |
| description   | Stringa<br>Lunghezza max: 2028<br>Modello: [^\p{C}]+                 | Descrizione del flusso.            |
| files         | elenco<br>Membro: StreamFile                                         | File di cui eseguire lo streaming. |

| Nome          | Tipo       | Descrizione                                                                            |
|---------------|------------|----------------------------------------------------------------------------------------|
| fileId        | intero     | ID file.<br>Intervallo – Max: 255, min.: 0                                             |
| s3Location    | S3Location | Posizione del file in S3.                                                              |
| bucket        | Stringa    | Bucket S3.<br>Lunghezza min.: 1                                                        |
| key           | Stringa    | La chiave S3.<br>Lunghezza min.: 1                                                     |
| versione      | Stringa    | Versione del bucket S3                                                                 |
| createdAt     | timestamp  | Data di creazione del flusso.                                                          |
| lastUpdatedAt | Timestamp  | Data dell'ultimo aggiornamento del flusso.                                             |
| roleArn       | Stringa    | Ruolo IAM assunto da AWS IoT per accedere ai file S3.<br>Lunghezza max: 2048, min.: 20 |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `ThrottlingException`

La velocità supera il limite.

##### `UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

## DescribeThing

Ottiene informazioni sull'oggetto specificato.

#### Riepilogo

```
aws iot describe-thing \
--thing-name <value> \
[--cli-input-json <value>] \
```

```
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "thingName": "string"
}
```

#### Campi di cli-input-json

| Nome      | Tipo                                                                  | Descrizione        |
|-----------|-----------------------------------------------------------------------|--------------------|
| thingName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto. |

#### Output

```
{
 "defaultClientId": "string",
 "thingName": "string",
 "thingId": "string",
 "thingArn": "string",
 "thingTypeName": "string",
 "attributes": {
 "string": "string"
 },
 "version": "long",
 "billingGroupName": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome            | Tipo                                                                  | Descrizione                                             |
|-----------------|-----------------------------------------------------------------------|---------------------------------------------------------|
| defaultClientId | Stringa                                                               | ID client predefinito.                                  |
| thingName       | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto.                                      |
| thingId         | Stringa                                                               | ID dell'oggetto da descrivere.                          |
| thingArn        | Stringa                                                               | ARN dell'oggetto da descrivere.                         |
| thingTypeName   | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del tipo di oggetto.                               |
| attributes      | mappa                                                                 | Attributi dell'oggetto.                                 |
| versione        | Long                                                                  | Versione corrente del record dell'oggetto nel registro. |

| Nome                          | Tipo                                                                  | Descrizione                                                                                                                                                                                                                                                       |
|-------------------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               |                                                                       | <p><b>Note</b></p> <p>Per evitare modifiche involontarie alle informazioni contenute nel registro, puoi passare le informazioni sulla versione nel parametro <code>expectedVersion</code> delle chiamate <code>UpdateThing</code> e <code>DeleteThing</code>.</p> |
| <code>billingGroupName</code> | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Il nome del gruppo di fatturazione a cui appartiene l'oggetto.                                                                                                                                                                                                    |

#### Errori

`ResourceNotFoundException`

La risorsa specificata non esiste.

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

`InternalFailureException`

Si è verificato un errore imprevisto.

## DescribeThingGroup

Describe un gruppo di oggetti.

#### Riepilogo

```
aws iot describe-thing-group \
--thing-group-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "thingGroupName": "string"
}
```

#### Campi di **cli-input-json**

| Nome           | Tipo                                                                          | Descrizione                 |
|----------------|-------------------------------------------------------------------------------|-----------------------------|
| thingGroupName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome del gruppo di oggetti. |

#### Output

```
{
 "thingGroupName": "string",
 "thingGroupId": "string",
 "thingGroupArn": "string",
 "version": "long",
 "thingGroupProperties": {
 "thingGroupDescription": "string",
 "attributePayload": {
 "attributes": {
 "string": "string"
 },
 "merge": "boolean"
 }
 },
 "thingGroupMetadata": {
 "parentGroupName": "string",
 "rootToParentThingGroups": [
 {
 "groupName": "string",
 "groupArn": "string"
 }
],
 "creationDate": "timestamp"
 },
 "indexName": "string",
 "queryString": "string",
 "queryVersion": "string",
 "status": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo                                                                          | Descrizione                 |
|----------------|-------------------------------------------------------------------------------|-----------------------------|
| thingGroupName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome del gruppo di oggetti. |
| thingGroupId   | Stringa<br><br>Lunghezza max: 128, min.: 1                                    | ID gruppo di oggetti.       |

| Nome                    | Tipo                                                                          | Descrizione                                                                                                                                                                                                                                                                                                                                |
|-------------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | Modello: [a–z A–Z 0–9 -]+                                                     |                                                                                                                                                                                                                                                                                                                                            |
| thingGroupArn           | Stringa                                                                       | ARN del gruppo di oggetti.                                                                                                                                                                                                                                                                                                                 |
| versione                | Long                                                                          | Versione del gruppo di oggetti.                                                                                                                                                                                                                                                                                                            |
| thingGroupProperties    | ThingGroupProperties                                                          | Proprietà del gruppo di oggetti.                                                                                                                                                                                                                                                                                                           |
| thingGroupDescription   | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [\p{Graph}] <sup>*</sup>   | Descrizione del gruppo di oggetti.                                                                                                                                                                                                                                                                                                         |
| attributePayload        | AttributePayload                                                              | Attributi del gruppo di oggetti in formato JSON.                                                                                                                                                                                                                                                                                           |
| attributes              | mappa                                                                         | Stringa JSON contenente fino a tre coppie chiave/valore in formato JSON. Ad esempio:<br><br><code>\ "attributes\ ":"<br/>{\ "string1\ ":"<br/>"string2\ "}</code>                                                                                                                                                                          |
| merge                   | booleano                                                                      | Specifica se l'elenco di attributi fornito in AttributePayload deve essere unito agli attributi archiviati nel registro, anziché sovrascrivere questi ultimi.<br><br>Per rimuovere un attributo, chiama UpdateThing con un valore di attributo vuoto.<br><br><b>Note</b><br><br>L'attributo merge è valido solo quando chiavi UpdateThing. |
| thingGroupMetadata      | ThingGroupMetadata                                                            | Metadati del gruppo di oggetti.                                                                                                                                                                                                                                                                                                            |
| parentGroupName         | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_-]+ | Nome del gruppo di oggetti padre.                                                                                                                                                                                                                                                                                                          |
| rootToParentThingGroups | elenco<br><br>Membro: GroupNameAndArn<br><br>Classe Java: java.util.List      | Gruppo di oggetti padre root.                                                                                                                                                                                                                                                                                                              |
| groupName               | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_-]+ | Nome del gruppo.                                                                                                                                                                                                                                                                                                                           |

| Nome         | Tipo                                                                         | Descrizione                                                                                  |
|--------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| groupArn     | Stringa                                                                      | ARN del gruppo.                                                                              |
| creationDate | timestamp                                                                    | Timestamp UNIX del momento in cui il gruppo di oggetti è stato creato.                       |
| indexName    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_]+ | Il nome d'indice del gruppo di oggetti dinamico.                                             |
| queryString  | Stringa<br><br>Lunghezza min.: 1                                             | La stringa di query per la ricerca del gruppo di oggetti dinamico.                           |
| queryVersion | Stringa                                                                      | La versione di query del gruppo di oggetti dinamico.                                         |
| status       | Stringa                                                                      | Lo stato del gruppo di oggetti dinamico.<br><br>Enumerazione: ACTIVE   BUILDING   REBUILDING |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

## DescribeThingRegistrationTask

Describe un'attività di provisioning in blocco di oggetti.

#### Riepilogo

```
aws iot describe-thing-registration-task \
--task-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di `cli-input-json`

```
{
 "taskId": "string"
}
```

#### Campi di **cli-input-json**

| Nome   | Tipo                             | Descrizione  |
|--------|----------------------------------|--------------|
| taskId | Stringa<br><br>Lunghezza max: 40 | ID attività. |

#### Output

```
{
 "taskId": "string",
 "creationDate": "timestamp",
 "lastModifiedDate": "timestamp",
 "templateBody": "string",
 "inputFileBucket": "string",
 "inputFileKey": "string",
 "roleArn": "string",
 "status": "string",
 "message": "string",
 "successCount": "integer",
 "failureCount": "integer",
 "percentageProgress": "integer"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome             | Tipo                                                                              | Descrizione                                                      |
|------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------|
| taskId           | Stringa<br><br>Lunghezza max: 40                                                  | ID attività.                                                     |
| creationDate     | Timestamp                                                                         | Data di creazione dell'attività.                                 |
| lastModifiedDate | Timestamp                                                                         | Data dell'ultima modifica dell'attività.                         |
| templateBody     | Stringa                                                                           | Modello dell'attività.                                           |
| inputFileBucket  | Stringa<br><br>Lunghezza max: 256, min.: 3<br><br>modello: [a-zA-Z0-9._-]+        | Bucket S3 che contiene il file di input.                         |
| inputFileKey     | Stringa<br><br>Lunghezza max: 1024, min.: 1<br><br>modello: [a-zA-Z0-9!_.*'()/-]+ | Chiave del file di input.                                        |
| roleArn          | Stringa<br><br>Lunghezza max: 2048, min.: 20                                      | ARN del ruolo che concede l'accesso al bucket del file di input. |

| Nome               | Tipo                                     | Descrizione                                                                                                                         |
|--------------------|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| status             | Stringa                                  | Stato dell'attività di provisioning in blocco di oggetti.<br>Enumerazione: InProgress   Completed   Failed   Cancelled   Cancelling |
| message            | Stringa<br>Lunghezza max: 2048           | Messaggio.                                                                                                                          |
| successCount       | intero                                   | Numero di oggetti di cui è stato effettuato il provisioning.                                                                        |
| failureCount       | intero                                   | Numero di oggetti di cui non è riuscito il provisioning.                                                                            |
| percentageProgress | intero<br>Intervallo – Max: 100, min.: 0 | Avanzamento dell'attività di provisioning in blocco espresso come percentuale.                                                      |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ThrottlingException`

La velocità supera il limite.

##### `UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

## DescribeThingType

Ottiene informazioni sul tipo di oggetto specificato.

#### Riepilogo

```
aws iot describe-thing-type \
--thing-type-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "thingTypeName": "string"
}
```

#### Campi di **cli-input-json**

| Nome          | Tipo                                                                       | Descrizione               |
|---------------|----------------------------------------------------------------------------|---------------------------|
| thingTypeName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z0-9:_-]+ | Nome del tipo di oggetto. |

#### Output

```
{
 "thingTypeName": "string",
 "thingTypeId": "string",
 "thingTypeArn": "string",
 "thingTypeProperties": {
 "thingTypeDescription": "string",
 "searchableAttributes": [
 "string"
],
 "thingTypeMetadata": {
 "deprecated": "boolean",
 "deprecationDate": "timestamp",
 "creationDate": "timestamp"
 }
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome                 | Tipo                                                                       | Descrizione                                                                                                                                                      |
|----------------------|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingTypeName        | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z0-9:_-]+ | Nome del tipo di oggetto.                                                                                                                                        |
| thingTypeId          | Stringa                                                                    | ID tipo di oggetto.                                                                                                                                              |
| thingTypeArn         | Stringa                                                                    | ARN del tipo di oggetto.                                                                                                                                         |
| thingTypeProperties  | ThingTypeProperties                                                        | ThingTypeProperties contiene informazioni sul tipo di oggetto, tra cui una descrizione e un elenco di nomi di attributi dell'oggetto che possono essere cercati. |
| thingTypeDescription | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [\p{Graph}]*            | Descrizione del tipo di oggetto.                                                                                                                                 |

| Nome                 | Tipo                                                           | Descrizione                                                                                                                                                                                                    |
|----------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| searchableAttributes | elenco<br>Membro: AttributeName<br>Classe Java: java.util.List | Elenco di nomi di attributi dell'oggetto che è possibile cercare.                                                                                                                                              |
| thingTypeMetadata    | ThingTypeMetadata                                              | ThingTypeMetadata contiene informazioni aggiuntive sul tipo di oggetto, tra cui data e ora di creazione, un valore indicante se il tipo di oggetto è obsoleto e data e ora in cui è stato dichiarato obsoleto. |
| deprecated           | booleano                                                       | Specifica se il tipo di oggetto è obsoleto. Se è true, a questo tipo non possono essere associati nuovi oggetti.                                                                                               |
| deprecationDate      | Timestamp                                                      | Data e ora in cui il tipo di oggetto è stato dichiarato obsoleto.                                                                                                                                              |
| creationDate         | Timestamp                                                      | Data e ora di creazione del tipo di oggetto.                                                                                                                                                                   |

#### Errori

##### ResourceNotFoundException

La risorsa specificata non esiste.

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

##### InternalFailureException

Si è verificato un errore imprevisto.

## DetachPolicy

Scollega una policy da un target specificato.

#### Riepilogo

```
aws iot detach-policy \
--policy-name <value> \
--target <value> \
```

```
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "policyName": "string",
 "target": "string"
}
```

Campi di **cli-input-json**

| Nome       | Tipo                                                                  | Descrizione                               |
|------------|-----------------------------------------------------------------------|-------------------------------------------|
| policyName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+ | Policy da scollegare.                     |
| target     | Stringa                                                               | Target da cui la policy verrà scollegata. |

Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

**LimitExceededException**

È stato superato un limite.

## DetachPrincipalPolicy

Rimuove la policy indicata dal certificato specificato.

Nota: questa API è obsoleta. Usa invece DetachPolicy.

Riepilogo

```
aws iot detach-principal-policy \
--policy-name <value> \
```

```
--principal <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "policyName": "string",
 "principal": "string"
}
```

Campi di **cli-input-json**

| Nome       | Tipo                                                                  | Descrizione                                                                                                                                                                          |
|------------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| policyName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+ | Nome della policy da scollegare.                                                                                                                                                     |
| principal  | Stringa                                                               | Entità principale.<br><br>Se l'entità principale è un certificato, specifica l'ARN del certificato. Se l'entità principale è un'identità di Amazon Cognito, specifica l'ID identità. |

Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DetachSecurityProfile

Elimina l'associazione di un profilo di sicurezza di Device Defender da un gruppo di oggetti o dall'account.

## Riepilogo

```
aws iot detach-security-profile \
--security-profile-name <value> \
--security-profile-target-arn <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "securityProfileName": "string",
 "securityProfileTargetArn": "string"
}
```

### Campi di cli-input-json

| Nome                     | Tipo    | Descrizione                                                                                            |
|--------------------------|---------|--------------------------------------------------------------------------------------------------------|
| securityProfileName      | Stringa | Profilo di sicurezza scollegato.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ |
| securityProfileTargetArn | Stringa | ARN del gruppo di oggetti da cui viene scollegato il profilo di sicurezza.                             |

### Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

# DetachThingPrincipal

Scollega l'entità principale indicata dall'oggetto specificato. Un principale può essere certificati X.509, utenti IAM, gruppi e ruoli, identità Amazon Cognito o identità federate.

## Note

Questa chiamata è asincrona. La propagazione del distacco potrebbe richiedere alcuni secondi.

## Riepilogo

```
aws iot detach-thing-principal \
--thing-name <value> \
--principal <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "thingName": "string",
 "principal": "string"
}
```

## Campi di cli-input-json

| Nome      | Tipo                                                                          | Descrizione                                                                                                                                                                                                       |
|-----------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto.                                                                                                                                                                                                |
| principal | Stringa                                                                       | Se l'entità principale è un certificato, questo valore deve essere l'ARN del certificato. Se l'entità principale è un'identità di Amazon Cognito, questo valore deve essere l'ID dell'identità di Amazon Cognito. |

## Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## DisableTopicRule

Disabilita la regola.

Riepilogo

```
aws iot disable-topic-rule \
 --rule-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "ruleName": "string"
}
```

Campi di **cli-input-json**

| Nome     | Tipo                                                                           | Descrizione                        |
|----------|--------------------------------------------------------------------------------|------------------------------------|
| ruleName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: ^[a-z A-Z 0-9 _]+\$ | Nome della regola da disabilitare. |

Output

Nessuna

Errori

**InternalException**

Si è verificato un errore imprevisto.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ConflictingResourceUpdateException**

Eccezione relativa ad aggiornamenti in conflitto della risorsa. Questa eccezione viene generata quando due aggiornamenti in sospeso causano un conflitto.

## EnableTopicRule

Abilita la regola.

Riepilogo

```
aws iot enable-topic-rule \
 --rule-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "ruleName": "string"
}
```

Campi di **cli-input-json**

| Nome     | Tipo                                                                           | Descrizione                                    |
|----------|--------------------------------------------------------------------------------|------------------------------------------------|
| ruleName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: ^[a-z A-Z 0-9 _]+\$ | Nome della regola dell'argomento da abilitare. |

Output

Nessuna

Errori

**InternalException**

Si è verificato un errore imprevisto.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ConflictingResourceUpdateException**

Eccezione relativa ad aggiornamenti in conflitto della risorsa. Questa eccezione viene generata quando due aggiornamenti in sospeso causano un conflitto.

## GetEffectivePolicies

Consente di ottenere un elenco delle policy che hanno effetto sul comportamento delle autorizzazioni del dispositivo specificato durante la connessione al gateway di dispositivo AWS IoT.

Riepilogo

```
aws iot get-effective-policies \
 [--principal <value>] \
 [--cognito-identity-pool-id <value>] \
 [--thing-name <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "principal": "string",
 "cognitoIdentityPoolId": "string",
 "thingName": "string"
}
```

#### Campi di cli-input-json

| Nome                  | Tipo    | Descrizione                                                                              |
|-----------------------|---------|------------------------------------------------------------------------------------------|
| principal             | Stringa | Entità principale.                                                                       |
| cognitoIdentityPoolId | Stringa | ID pool di identità di Cognito.                                                          |
| thingName             | Stringa | Nome dell'oggetto.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ |

#### Output

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

#### Campi di output dell'interfaccia a riga di comando

| Nome              | Tipo                                                                     | Descrizione                 |
|-------------------|--------------------------------------------------------------------------|-----------------------------|
| effectivePolicies | elenco<br><br>Membro: EffectivePolicy<br><br>Classe Java: java.util.List | Policy valide.              |
| policyName        | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+    | Nome della policy.          |
| policyArn         | Stringa                                                                  | ARN della policy.           |
| policyDocument    | Stringa                                                                  | Documento della policy IAM. |

#### Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

**LimitExceededException**

È stato superato un limite.

## GetIndexingConfiguration

Ottiene la configurazione della ricerca.

Riepilogo

```
aws iot get-indexing-configuration \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
}
```

Output

```
{
 "thingIndexingConfiguration": {
 "thingIndexingMode": "string",
 "thingConnectivityIndexingMode": "string"
 },
 "thingGroupIndexingConfiguration": {
 "thingGroupIndexingMode": "string"
 }
}
```

Campi di output dell'interfaccia a riga di comando

| Nome                       | Tipo                       | Descrizione                                                  |
|----------------------------|----------------------------|--------------------------------------------------------------|
| thingIndexingConfiguration | ThingIndexingConfiguration | Configurazione dell'indicizzazione di oggetti.               |
| thingIndexingMode          | Stringa                    | Modalità di indicizzazione di oggetti. I valori validi sono: |

| Nome                            | Tipo                            | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 |                                 | <ul style="list-style-type: none"> <li>• REGISTRY – L'indice dell'oggetto contiene solo dati del registro.</li> <li>• REGISTRY_AND_SHADOW – L'indice dell'oggetto contiene i dati shadow e del registro.</li> <li>• OFF – L'indicizzazione di oggetti è disabilitata.</li> </ul> <p>Enumerazione: OFF   REGISTRY   REGISTRY_AND_SHADOW</p>                                                                                                      |
| thingConnectivityIndexingMode   | Stringa                         | <p>La modalità di indicizzazione della connettività. I valori validi sono:</p> <ul style="list-style-type: none"> <li>• STATUS – L'indice dell'oggetto contiene lo stato di connettività. Per abilitare l'indicizzazione della connettività degli oggetti, thingIndexMode non deve essere impostato su OFF.</li> <li>• OFF – L'indicizzazione dello stato della connettività degli oggetti è disabilitato.</li> </ul> <p>enum: OFF   STATUS</p> |
| thingGroupIndexingConfiguration | ThingGroupIndexingConfiguration | Configurazione dell'indice.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| thingGroupIndexingMode          | Stringa                         | <p>Modalità di indicizzazione di gruppi di oggetti.</p> <p>enumerazione: OFF   ON</p>                                                                                                                                                                                                                                                                                                                                                           |

## Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

`InternalFailureException`

Si è verificato un errore imprevisto.

# GetJobDocument

Ottiene un documento del processo.

Riepilogo

```
aws iot get-job-document \
--job-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "jobId": "string"
}
```

Campi di **cli-input-json**

| Nome  | Tipo                                                                       | Descrizione                                                              |
|-------|----------------------------------------------------------------------------|--------------------------------------------------------------------------|
| jobId | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a–z A–Z 0–9 _]+ | Identificatore univoco assegnato al processo al momento della creazione. |

Output

```
{
 "document": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome     | Tipo                                | Descrizione                           |
|----------|-------------------------------------|---------------------------------------|
| document | Stringa<br><br>Lunghezza max: 32768 | Contenuto del documento del processo. |

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

## GetLoggingOptions

Ottiene le opzioni di logging.

NOTA: l'utilizzo di questo comando non è consigliato. Usa invece `GetV2LoggingOptions`.

Riepilogo

```
aws iot get-logging-options \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
}
```

Output

```
{
 "roleArn": "string",
 "logLevel": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome     | Tipo    | Descrizione                                                                 |
|----------|---------|-----------------------------------------------------------------------------|
| roleArn  | Stringa | ARN del ruolo IAM che concede l'accesso.                                    |
| logLevel | Stringa | Livello di logging.<br>Enumerazione: DEBUG   INFO   ERROR   WARN   DISABLED |

Errori

`InternalException`

Si è verificato un errore imprevisto.

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

## GetOTAUpdate

Ottiene un aggiornamento OTA.

Riepilogo

```
aws iot get-ota-update \
```

```
--ota-update-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "otaUpdateId": "string"
}
```

Campi di **cli-input-json**

| Nome        | Tipo                                                                 | Descrizione           |
|-------------|----------------------------------------------------------------------|-----------------------|
| otaUpdateId | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+ | ID aggiornamento OTA. |

Output

```
{
 "otaUpdateInfo": {
 "otaUpdateId": "string",
 "otaUpdateArn": "string",
 "creationDate": "timestamp",
 "lastModifiedDate": "timestamp",
 "description": "string",
 "targets": [
 "string"
],
 "awsJobExecutionsRolloutConfig": {
 "maximumPerMinute": "integer"
 },
 "targetSelection": "string",
 "otaUpdateFiles": [
 {
 "fileName": "string",
 "fileVersion": "string",
 "fileLocation": {
 "stream": {
 "streamId": "string",
 "fileId": "integer"
 },
 "s3Location": {
 "bucket": "string",
 "key": "string",
 "version": "string"
 }
 },
 "codeSigning": {
 "awsSignerJobId": "string",
 "startSigningJobParameter": {
 "signingProfileParameter": {
 "certificateArn": "string",
 "platform": "string",
 "certificatePathOnDevice": "string"
 },
 "signingProfileName": "string",
 "destination": {
 "s3Destination": {
 "bucket": "string",
 "key": "string"
 }
 }
 }
 }
 }
]
 }
}
```

```

 "bucket": "string",
 "prefix": "string"
 }
},
"customCodeSigning": {
 "signature": {
 "inlineDocument": "blob"
 },
 "certificateChain": {
 "certificateName": "string",
 "inlineDocument": "string"
 },
 "hashAlgorithm": "string",
 "signatureAlgorithm": "string"
}
],
"attributes": {
 "string": "string"
}
}
],
"otaUpdateStatus": "string",
"awsIotJobId": "string",
"awsIotJobArn": "string",
"errorInfo": {
 "code": "string",
 "message": "string"
},
"additionalParameters": {
 "string": "string"
}
}
}
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome             | Tipo                                                                        | Descrizione                                            |
|------------------|-----------------------------------------------------------------------------|--------------------------------------------------------|
| otaUpdateInfo    | OTAUpdateInfo                                                               | Informazioni sull'aggiornamento OTA.                   |
| otaUpdateId      | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 _]+ | ID aggiornamento OTA.                                  |
| otaUpdateArn     | Stringa                                                                     | ARN dell'aggiornamento OTA.                            |
| creationDate     | timestamp                                                                   | Data di creazione dell'aggiornamento OTA.              |
| lastModifiedDate | Timestamp                                                                   | Data dell'ultimo aggiornamento dell'aggiornamento OTA. |
| description      | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+                | Descrizione dell'aggiornamento OTA.                    |
| targets          | elenco                                                                      | Target dell'aggiornamento OTA.                         |

| Nome                          | Tipo                                                                | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | Membro: Target                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| awsJobExecutionsRolloutConfig | AwsJobExecutionsRolloutConfig                                       | Configurazione per l'implementazione degli aggiornamenti OTA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| maximumPerMinute              | intero<br>Intervallo – Max: 1000, min.: 1                           | Numero massimo di esecuzioni del processo di aggiornamento OTA avviate al minuto.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| targetSelection               | Stringa                                                             | Specifica se l'esecuzione dell'aggiornamento OTA continuerà (CONTINUOUS) o se l'aggiornamento verrà completato dopo che tutti gli oggetti specificati come target avranno completato l'aggiornamento OTA (SNAPSHOT). Se è continuo, l'aggiornamento OTA può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un aggiornamento OTA verrà eseguito in un oggetto quando l'oggetto viene aggiunto a un gruppo target, anche dopo che l'aggiornamento OTA è stato completato da tutti gli oggetti originariamente nel gruppo.<br><br>Enumerazione: CONTINUOUS   SNAPSHOT |
| otaUpdateFiles                | elenco<br>Membro: OTAUpdateFile                                     | Elenco di file associati all'aggiornamento OTA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| fileName                      | Stringa                                                             | Nome del file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| fileVersion                   | Stringa                                                             | Versione del file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| fileLocation                  | FileLocation                                                        | Percorso del firmware aggiornato.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| stream                        | Flusso                                                              | Flusso contenente l'aggiornamento OTA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| streamId                      | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 _]+ | ID flusso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| fileId                        | intero<br>Intervallo – Max: 255, min.: 0                            | ID di un file associato a un flusso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Nome                     | Tipo                         | Descrizione                                                           |
|--------------------------|------------------------------|-----------------------------------------------------------------------|
| s3Location               | S3Location                   | Percorso del firmware aggiornato in S3.                               |
| bucket                   | Stringa<br>Lunghezza min.: 1 | Bucket S3.                                                            |
| key                      | Stringa<br>Lunghezza min.: 1 | La chiave S3.                                                         |
| versione                 | Stringa                      | Versione del bucket S3                                                |
| codeSigning              | CodeSigning                  | Metodo di firma del codice del file.                                  |
| awsSignerJobId           | Stringa                      | ID dell'elemento AWSSignerJob che è stato creato per firmare il file. |
| startSigningJobParameter | StartSigningJobParameter     | Describe il processo di firma del codice.                             |
| signingProfileParameter  | SigningProfileParameter      | Describe il profilo di firma del codice.                              |
| certificateArn           | Stringa                      | ARN del certificato.                                                  |
| platform                 | Stringa                      | Piattaforma hardware del tuo dispositivo.                             |
| certificatePathOnDevice  | Stringa                      | Percorso del certificato di firma del codice sul tuo dispositivo.     |
| signingProfileName       | Stringa                      | Nome del profilo di firma del codice.                                 |
| destinazione             | Destinazione                 | Percorso in cui scrivere il file firmato del codice.                  |
| s3Destination            | S3Destination                | Describe il percorso del firmware aggiornato in S3.                   |
| bucket                   | Stringa<br>Lunghezza min.: 1 | Bucket S3 che contiene il firmware aggiornato.                        |
| prefisso                 | Stringa                      | Prefisso S3.                                                          |
| customCodeSigning        | CustomCodeSigning            | Metodo personalizzato per la firma del codice di un file.             |
| signature                | CodeSigningSignature         | Firma per il file.                                                    |
| inlineDocument           | blob                         | Rappresentazione binaria codificata in base64 della firma del codice. |
| certificateChain         | CodeSigningCertificateChain  | Catena di certificati.                                                |

| Nome                 | Tipo      | Descrizione                                                                                                                          |
|----------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------|
| certificateName      | Stringa   | Nome del certificato.                                                                                                                |
| inlineDocument       | Stringa   | Rappresentazione binaria codificata in base64 della catena di certificati di firma del codice.                                       |
| hashAlgorithm        | Stringa   | Algoritmo hash usato per firmare il codice del file.                                                                                 |
| signatureAlgorithm   | Stringa   | Algoritmo di firma usato per firmare il codice del file.                                                                             |
| attributes           | mappa     | Elenco di coppie nome/attributo.                                                                                                     |
| otaUpdateStatus      | Stringa   | Stato dell'aggiornamento OTA.<br><br>Enumerazione:<br>CREATE_PENDING  <br>CREATE_IN_PROGRESS<br>  CREATE_COMPLETE  <br>CREATE_FAILED |
| awsIoTJobId          | Stringa   | Job ID AWS IoT associato all'aggiornamento OTA.                                                                                      |
| awsIoTJobArn         | Stringa   | ARN del processo AWS IoT associato all'aggiornamento OTA.                                                                            |
| errorInfo            | ErrorInfo | Informazioni sull'errore associate all'aggiornamento OTA.                                                                            |
| code                 | Stringa   | Codice di errore.                                                                                                                    |
| message              | Stringa   | Messaggio di errore.                                                                                                                 |
| additionalParameters | mappa     | Raccolta di coppie nome/valore.                                                                                                      |

## Errori

### `InvalidRequestException`

I contenuti della richiesta non sono validi.

### `ThrottlingException`

La velocità supera il limite.

### `UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

### `InternalFailureException`

Si è verificato un errore imprevisto.

### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

#### ResourceNotFoundException

La risorsa specificata non esiste.

## GetPendingJobExecutions

Ottiene l'elenco di tutti i processi per un oggetto che non si trovano in uno stato terminale.

### Riepilogo

```
aws iot-jobs-data get-pending-job-executions \
--thing-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "thingName": "string"
}
```

### Campi di cli-input-json

| Nome      | Tipo                                                                          | Descrizione                                      |
|-----------|-------------------------------------------------------------------------------|--------------------------------------------------|
| thingName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto che sta eseguendo il processo. |

### Output

```
{
 "inProgressJobs": [
 {
 "jobId": "string",
 "queuedAt": "long",
 "startedAt": "long",
 "lastUpdatedAt": "long",
 "versionNumber": "long",
 "executionNumber": "long"
 }
],
 "queuedJobs": [
 {
 "jobId": "string",
 "queuedAt": "long",
 "startedAt": "long",
 "lastUpdatedAt": "long",
 "versionNumber": "long",
 "executionNumber": "long"
 }
]
}
```

Campi di output dell'interfaccia a riga di comando

| Nome            | Tipo                                                                 | Descrizione                                                                                                                                                               |
|-----------------|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| inProgressJobs  | elenco<br>Membro: JobExecutionSummary<br>Classe Java: java.util.List | Elenco di oggetti JobExecutionSummary con stato IN_PROGRESS.                                                                                                              |
| jobId           | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+  | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                  |
| queuedAt        | Long                                                                 | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                |
| startedAt       | Long                                                                 | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                             |
| lastUpdatedAt   | Long                                                                 | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                              |
| versionNumber   | Long                                                                 | Versione dell'esecuzione del processo. Le versioni di esecuzione dei processi vengono incrementate ogni volta che AWS IoT Jobs riceve un aggiornamento da un dispositivo. |
| executionNumber | Long                                                                 | Numerosche identifica una determinata esecuzione di un processo in un dispositivo specifico.                                                                              |
| queuedJobs      | elenco<br>Membro: JobExecutionSummary<br>Classe Java: java.util.List | Elenco di oggetti JobExecutionSummary con stato QUEUED.                                                                                                                   |
| jobId           | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+  | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                  |
| queuedAt        | Long                                                                 | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                |

| Nome            | Tipo | Descrizione                                                                                                                                                               |
|-----------------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| startedAt       | Long | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                             |
| lastUpdatedAt   | Long | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                              |
| versionNumber   | Long | Versione dell'esecuzione del processo. Le versioni di esecuzione dei processi vengono incrementate ogni volta che AWS IoT Jobs riceve un aggiornamento da un dispositivo. |
| executionNumber | Long | Numero che identifica una determinata esecuzione di un processo in un dispositivo specifico.                                                                              |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `ThrottlingException`

La velocità supera il limite.

##### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

##### `CertificateValidationException`

Il certificato non è valido.

## GetPolicy

Ottiene informazioni sulla policy specificata con il documento della policy della versione predefinita.

#### Riepilogo

```
aws iot get-policy \
--policy-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di `cli-input-json`

```
{
```

```

 "policyName": "string"
}
```

#### Campi di **cli-input-json**

| Nome       | Tipo                                                                  | Descrizione        |
|------------|-----------------------------------------------------------------------|--------------------|
| policyName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+ | Nome della policy. |

#### Output

```
{
 "policyName": "string",
 "policyArn": "string",
 "policyDocument": "string",
 "defaultVersionId": "string",
 "creationDate": "timestamp",
 "lastModifiedDate": "timestamp",
 "generationId": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome             | Tipo                                                                  | Descrizione                                |
|------------------|-----------------------------------------------------------------------|--------------------------------------------|
| policyName       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+ | Nome della policy.                         |
| policyArn        | Stringa                                                               | ARN della policy.                          |
| policyDocument   | Stringa                                                               | Documento JSON che descrive la policy.     |
| defaultVersionId | Stringa<br><br>Modello: [0-9]+                                        | ID versione della policy predefinita.      |
| creationDate     | Timestamp                                                             | La data di creazione della policy.         |
| lastModifiedDate | Timestamp                                                             | La data dell'ultima modifica della policy. |
| generationId     | Stringa                                                               | L'ID di generazione della policy.          |

#### Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

#### ThrottlingException

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## GetPolicyVersion

Ottiene informazioni sulla versione della policy specificata.

### Riepilogo

```
aws iot get-policy-version \
--policy-name <value> \
--policy-version-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "policyName": "string",
 "policyVersionId": "string"
}
```

### Campi di cli-input-json

| Nome            | Tipo    | Descrizione                                                              |
|-----------------|---------|--------------------------------------------------------------------------|
| policyName      | Stringa | Nome della policy.<br>Lunghezza max: 128, min.: 1<br>modello: [w+=,.@-]+ |
| policyVersionId | Stringa | ID versione della policy.<br>Modello: [0-9]+                             |

### Output

```
{
 "policyArn": "string",
 "policyName": "string",
 "policyDocument": "string",
 "policyVersionId": "string",
 "isDefaultVersion": "boolean",
 "creationDate": "timestamp",
 "lastModifiedDate": "timestamp",
 "generationId": "string"
```

}

### Campi di output dell'interfaccia a riga di comando

| Nome             | Tipo                                                              | Descrizione                                                 |
|------------------|-------------------------------------------------------------------|-------------------------------------------------------------|
| policyArn        | Stringa                                                           | ARN della policy.                                           |
| policyName       | Stringa<br><br>Lunghezza max: 128, min.: 1<br>modello: [w+=,.@-]+ | Nome della policy.                                          |
| policyDocument   | Stringa                                                           | Documento JSON che descrive la policy.                      |
| policyVersionId  | Stringa<br><br>Modello: [0-9]+                                    | ID versione della policy.                                   |
| isDefaultVersion | booleano                                                          | Specifica se la versione della policy è quella predefinita. |
| creationDate     | Timestamp                                                         | La data di creazione della versione della policy.           |
| lastModifiedDate | Timestamp                                                         | La data dell'ultima modifica della versione della policy.   |
| generationId     | Stringa                                                           | L'ID di generazione della versione della policy.            |

### Errori

#### ResourceNotFoundException

La risorsa specificata non esiste.

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### ThrottlingException

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## GetRegistrationCode

Ottiene un codice di registrazione usato per registrare un certificato CA con AWS IoT.

### Riepilogo

```
aws iot get-registration-code \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
}
```

### Output

```
{
 "registrationCode": "string"
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome             | Tipo                                                                   | Descrizione                                 |
|------------------|------------------------------------------------------------------------|---------------------------------------------|
| registrationCode | Stringa<br>Lunghezza max: 64, min.: 64<br>Modello: (0x)?[a-f A-F 0-9]+ | Codice di registrazione del certificato CA. |

### Errori

#### ThrottlingException

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

#### InvalidRequestException

I contenuti della richiesta non sono validi.

## GetStatistics

Ottiene le statistiche sugli oggetti che corrispondono alla query specificata.

### Riepilogo

```
aws iot get-statistics \
[--index-name <value>] \
--query-string <value> \
[--aggregation-field <value>] \
[--query-version <value>] \
```

```
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "indexName": "string",
 "queryString": "string",
 "aggregationField": "string",
 "queryVersion": "string"
}
```

#### Campi di cli-input-json

| Nome             | Tipo                                                                  | Descrizione                                                                                                                                                           |
|------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| indexName        | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'indice su cui eseguire una ricerca. Il valore predefinito è AWS_Things.                                                                                     |
| queryString      | Stringa<br>Lunghezza min.: 1                                          | La query usata per eseguire la ricerca. È possibile specificare "*" per la stringa di query per ottenere il numero di tutti gli oggetti indicizzati nell'account AWS. |
| aggregationField | Stringa<br>Lunghezza min.: 1                                          | Nome del campo di aggregazione. Attualmente non è supportato.                                                                                                         |
| queryVersion     | Stringa                                                               | La versione della query usata per eseguire la ricerca.                                                                                                                |

#### Output

```
{
 "statistics": {
 "count": "integer"
 }
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome       | Tipo        | Descrizione                                                                                                             |
|------------|-------------|-------------------------------------------------------------------------------------------------------------------------|
| statistics | Statistiche | Le statistiche restituite dal servizio di indicizzazione del parco istanze basate sul campo di aggregazione e di query. |
| count      | intero      | Numero di oggetti che corrispondono alla query.                                                                         |

#### Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidQueryException**

La query non è valida.

**InvalidAggregationException**

L'aggregazione non è valida.

**IndexNotReadyException**

L'indice non è pronto.

## GetThingShadow

Ottiene la copia shadow per l'oggetto specificato.

Per ulteriori informazioni, consulta [GetThingShadow](#) nella Guida per lo sviluppatore di AWS IoT.

**Riepilogo**

```
aws iot-data get-thing-shadow \
 --thing-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

**Formato di cli-input-json**

```
{
 "thingName": "string"
}
```

**Campi di cli-input-json**

| Nome      | Tipo                                                                          | Descrizione        |
|-----------|-------------------------------------------------------------------------------|--------------------|
| thingName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto. |

#### Output

```
{
 "payload": "blob"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome    | Tipo | Descrizione                                |
|---------|------|--------------------------------------------|
| payload | blob | Informazioni sullo stato, in formato JSON. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ResourceNotFoundException

La risorsa specificata non esiste.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

##### InternalFailureException

Si è verificato un errore imprevisto.

##### MethodNotAllowedException

La combinazione specificata di verbo HTTP e URI non è supportata.

##### UnsupportedDocumentEncodingException

La codifica non è supportata.

## GetTopicRule

Ottiene informazioni sulla regola.

#### Riepilogo

```
aws iot get-topic-rule \
 --rule-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "ruleName": "string"
}
```

### Campi di **cli-input-json**

| Nome     | Tipo                                                                        | Descrizione        |
|----------|-----------------------------------------------------------------------------|--------------------|
| ruleName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: ^[a-zA-Z0-9_]+\$ | Nome della regola. |

### Output

```
{
 "ruleArn": "string",
 "rule": {
 "ruleName": "string",
 "sql": "string",
 "description": "string",
 "createdAt": "timestamp",
 "actions": [
 {
 "dynamoDB": {
 "tableName": "string",
 "roleArn": "string",
 "operation": "string",
 "hashKeyField": "string",
 "hashKeyValue": "string",
 "hashKeyType": "string",
 "rangeKeyField": "string",
 "rangeKeyValue": "string",
 "rangeKeyType": "string",
 "payloadField": "string"
 },
 "dynamoDBv2": {
 "roleArn": "string",
 "putItem": {
 "tableName": "string"
 }
 },
 "lambda": {
 "functionArn": "string"
 },
 "sns": {
 "targetArn": "string",
 "roleArn": "string",
 "messageFormat": "string"
 },
 "sqs": {
 "roleArn": "string",
 "queueUrl": "string",
 "useBase64": "boolean"
 },
 "kinesis": {
 "roleArn": "string",
 "streamName": "string",
 "partitionKey": "string"
 },
 "republish": {
 "roleArn": "string",
 "topic": "string"
 },
 "s3": {
 "roleArn": "string",
 "bucket": "string",
 "key": "string"
 }
 }
]
 }
}
```

```
 "bucketName": "string",
 "key": "string",
 "cannedAcl": "string"
 },
 "firehose": {
 "roleArn": "string",
 "deliveryStreamName": "string",
 "separator": "string"
 },
 "cloudwatchMetric": {
 "roleArn": "string",
 "metricNamespace": "string",
 "metricName": "string",
 "metricValue": "string",
 "metricUnit": "string",
 "metricTimestamp": "string"
 },
 "cloudwatchAlarm": {
 "roleArn": "string",
 "alarmName": "string",
 "stateReason": "string",
 "stateValue": "string"
 },
 "elasticsearch": {
 "roleArn": "string",
 "endpoint": "string",
 "index": "string",
 "type": "string",
 "id": "string"
 },
 "salesforce": {
 "token": "string",
 "url": "string"
 },
 "iotAnalytics": {
 "channelArn": "string",
 "channelName": "string",
 "roleArn": "string"
 },
 "iotEvents": {
 "inputName": "string",
 "messageId": "string",
 "roleArn": "string"
 },
 "stepFunctions": {
 "executionNamePrefix": "string",
 "stateMachineName": "string",
 "roleArn": "string"
 }
},
],
"ruleDisabled": "boolean",
"awsIotSqlVersion": "string",
"errorAction": {
 "dynamoDB": {
 "tableName": "string",
 "roleArn": "string",
 "operation": "string",
 "hashKeyField": "string",
 "hashKeyValue": "string",
 "hashKeyType": "string",
 "rangeKeyField": "string",
 "rangeKeyValue": "string",
 "rangeKeyType": "string",
 "payloadField": "string"
 },
}
```

```
"dynamoDBv2": {
 "roleArn": "string",
 "putItem": {
 "tableName": "string"
 }
},
"lambda": {
 "functionArn": "string"
},
"sns": {
 "targetArn": "string",
 "roleArn": "string",
 "messageFormat": "string"
},
"sqs": {
 "roleArn": "string",
 "queueUrl": "string",
 "useBase64": "boolean"
},
"kinesis": {
 "roleArn": "string",
 "streamName": "string",
 "partitionKey": "string"
},
"republish": {
 "roleArn": "string",
 "topic": "string"
},
"s3": {
 "roleArn": "string",
 "bucketName": "string",
 "key": "string",
 "cannedAcl": "string"
},
"firehose": {
 "roleArn": "string",
 "deliveryStreamName": "string",
 "separator": "string"
},
"cloudwatchMetric": {
 "roleArn": "string",
 "metricNamespace": "string",
 "metricName": "string",
 "metricValue": "string",
 "metricUnit": "string",
 "metricTimestamp": "string"
},
"cloudwatchAlarm": {
 "roleArn": "string",
 "alarmName": "string",
 "stateReason": "string",
 "stateValue": "string"
},
"elasticsearch": {
 "roleArn": "string",
 "endpoint": "string",
 "index": "string",
 "type": "string",
 "id": "string"
},
"salesforce": {
 "token": "string",
 "url": "string"
},
"iotAnalytics": {
 "channelArn": "string",
 "roleArn": "string"
}
```

```
 "channelName": "string",
 "roleArn": "string"
 },
 "iotEvents": {
 "inputName": "string",
 "messageId": "string",
 "roleArn": "string"
 },
 "stepFunctions": {
 "executionNamePrefix": "string",
 "stateMachineName": "string",
 "roleArn": "string"
 }
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome        | Tipo                                                                           | Descrizione                                                                                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ruleArn     | Stringa                                                                        | ARN della regola.                                                                                                                                                                                                      |
| rule        | TopicRule                                                                      | Regola.                                                                                                                                                                                                                |
| ruleName    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: ^[a-z A-Z 0-9 _]+\$ | Nome della regola.                                                                                                                                                                                                     |
| sql         | Stringa                                                                        | Istruzione SQL usata per eseguire query sull'argomento. Quando usi una query SQL con più righe, assicurati di applicare un carattere di escape ai caratteri di nuova riga.                                             |
| description | Stringa                                                                        | Descrizione della regola.                                                                                                                                                                                              |
| createdAt   | Timestamp                                                                      | Data e ora di creazione della regola.                                                                                                                                                                                  |
| actions     | elenco<br><br>Membro: Action                                                   | Operazioni associate alla regola.                                                                                                                                                                                      |
| dynamoDB    | DynamoDBAction                                                                 | Scrive in una tabella DynamoDB.                                                                                                                                                                                        |
| tableName   | Stringa                                                                        | Nome della tabella DynamoDB.                                                                                                                                                                                           |
| roleArn     | Stringa                                                                        | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                                         |
| operation   | Stringa                                                                        | Tipo di operazione da eseguire. Segue il modello di sostituzione, per cui può essere <b>operation</b> , ma la sostituzione deve restituire uno dei risultati seguenti: <b>INSERT</b> , <b>UPDATE</b> o <b>DELETE</b> . |

| Nome          | Tipo             | Descrizione                                                                                                                                                                                                                                                                                                               |
|---------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hashKeyField  | Stringa          | Nome della chiave hash.                                                                                                                                                                                                                                                                                                   |
| hashKeyValue  | Stringa          | Valore della chiave hash.                                                                                                                                                                                                                                                                                                 |
| hashKeyType   | Stringa          | <p>Tipo di chiave hash. I valori validi sono "STRING" e "NUMBER"</p> <p>Enumerazione: STRING   NUMBER</p>                                                                                                                                                                                                                 |
| rangeKeyField | Stringa          | Nome della chiave di intervallo.                                                                                                                                                                                                                                                                                          |
| rangeKeyValue | Stringa          | Valore della chiave di intervallo.                                                                                                                                                                                                                                                                                        |
| rangeKeyType  | Stringa          | <p>Tipo di chiave di intervallo. I valori validi sono "STRING" e "NUMBER"</p> <p>Enumerazione: STRING   NUMBER</p>                                                                                                                                                                                                        |
| payloadField  | Stringa          | Payload dell'operazione. Questo nome può essere personalizzato.                                                                                                                                                                                                                                                           |
| dynamoDBv2    | DynamoDBv2Action | Scrive in una tabella DynamoDB. Questa è una nuova versione dell'operazione DynamoDB. Permette di scrivere ogni attributo incluso nel payload di un messaggio MQTT in una colonna DynamoDB separata.                                                                                                                      |
| roleArn       | Stringa          | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                                                                                                                                            |
| putItem       | PutItemInput     | <p>Specifica la tabella DynamoDB in cui verranno scritti i dati del messaggio. Ad esempio:</p> <pre>{ "dynamoDBv2": { "roleArn": "aws:iam:12341251:my-role" "putItem": { "tableName": "my-table" } } }</pre> <p>Ogni attributo nel payload del messaggio verrà scritto in una colonna separata del database DynamoDB.</p> |
| tableName     | Stringa          | Tabella in cui verranno scritti i dati del messaggio.                                                                                                                                                                                                                                                                     |
| lambda        | LambdaAction     | Richiama una funzione Lambda.                                                                                                                                                                                                                                                                                             |
| functionArn   | Stringa          | ARN della funzione Lambda.                                                                                                                                                                                                                                                                                                |

| Nome          | Tipo            | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sns           | SnsAction       | Pubblica in un argomento Amazon SNS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| targetArn     | Stringa         | ARN dell'argomento SNS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| messageFormat | Stringa         | (Opzionale) Formato del messaggio da pubblicare. I valori accettati sono "JSON" e "RAW". Il valore predefinito dell'attributo è "RAW". SNS usa questa impostazione per determinare se il payload deve essere analizzato e se devono essere estratti i bit specifici della piattaforma rilevanti del payload. Per ulteriori informazioni sui formati di messaggio SNS, consulta la pagina <a href="https://docs.aws.amazon.com/sns/latest/dg/json-formats.html">https://docs.aws.amazon.com/sns/latest/dg/json-formats.html</a> e fai riferimento alla documentazione ufficiale.<br><br>Enumerazione: RAW   JSON |
| sqs           | SqsAction       | Pubblica in una coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| queueUrl      | Stringa         | URL della coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| useBase64     | booleano        | Specifica se usare la codifica Base64.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| kinesis       | KinesisAction   | Scrive i dati in un flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso al flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| streamName    | Stringa         | Nome del flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| partitionKey  | Stringa         | Chiave di partizione.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| republish     | RepublishAction | Pubblica in un altro argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| argomento     | Stringa         | Nome dell'argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Nome               | Tipo                                  | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| s3                 | S3Action                              | Scrive in un bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| roleArn            | Stringa                               | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                         |
| bucketName         | Stringa                               | Bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| key                | Stringa                               | Chiave dell'oggetto.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| cannedAcl          | Stringa                               | <p>Lista di controllo degli accessi predefinita Amazon S3 che controlla l'accesso all'oggetto identificato dalla chiave dell'oggetto. Per ulteriori informazioni, consulta la pagina relativa alle <a href="#">liste di controllo degli accessi predefinite S3</a>.</p> <p>Enumerazione: private   public-read   public-read-write   aws-exec-read   authenticated-read   bucket-owner-read   bucket-owner-full-control   log-delivery-write</p> |
| firehose           | FirehoseAction                        | Scrive in un flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                                                     |
| roleArn            | Stringa                               | Ruolo IAM che concede l'accesso al flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                               |
| deliveryStreamName | Stringa                               | Nome del flusso di distribuzione.                                                                                                                                                                                                                                                                                                                                                                                                                |
| separator          | Stringa<br><br>Modello: ([ ]) ( ) (,) | Separatore di caratteri che verrà usato per separare i record scritti nel flusso Firehose. I valori validi sono: '\n' (nuova riga), '\t' (tabulazione), '\r\n' (nuova riga Windows), ',' (virgola).                                                                                                                                                                                                                                              |
| cloudwatchMetric   | CloudwatchMetricAction                | Acquisisce un parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                              |
| roleArn            | Stringa                               | Ruolo IAM che permette l'accesso al parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                        |
| metricNamespace    | Stringa                               | Namespace dei nomi del parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                     |
| metricName         | Stringa                               | Nome parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| metricValue        | Stringa                               | Valore del parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| metricUnit         | Stringa                               | <a href="#">Unità di misura del parametro supportata da CloudWatch</a> .                                                                                                                                                                                                                                                                                                                                                                         |

| Nome            | Tipo                                                                                                                                                                                           | Descrizione                                                                                                                                                                         |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| metricTimestamp | Stringa                                                                                                                                                                                        | Uno <a href="#">Timestamp Unix</a> opzionale.                                                                                                                                       |
| cloudwatchAlarm | CloudwatchAlarmAction                                                                                                                                                                          | Modifica lo stato di un allarme CloudWatch.                                                                                                                                         |
| roleArn         | Stringa                                                                                                                                                                                        | Ruolo IAM che permette l'accesso all'allarme CloudWatch.                                                                                                                            |
| alarmName       | Stringa                                                                                                                                                                                        | Nome dell'allarme CloudWatch.                                                                                                                                                       |
| stateReason     | Stringa                                                                                                                                                                                        | Motivo della modifica dell'allarme.                                                                                                                                                 |
| stateValue      | Stringa                                                                                                                                                                                        | Valore dello stato dell'allarme. I valori accettabili sono: OK, ALARM, INSUFFICIENT_DATA.                                                                                           |
| elasticsearch   | ElasticsearchAction                                                                                                                                                                            | Scrive dati in un dominio Amazon Elasticsearch Service.                                                                                                                             |
| roleArn         | Stringa                                                                                                                                                                                        | ARN del ruolo IAM che ha accesso a Elasticsearch.                                                                                                                                   |
| endpoint        | Stringa<br>modello: https?://.*                                                                                                                                                                | Endpoint del dominio Elasticsearch.                                                                                                                                                 |
| index           | Stringa                                                                                                                                                                                        | Indice Elasticsearch in cui vuoi archiviare i dati.                                                                                                                                 |
| type            | Stringa                                                                                                                                                                                        | Tipo di documento che stai archiviando.                                                                                                                                             |
| id              | Stringa                                                                                                                                                                                        | Identificatore univoco per il documento che stai archiviando.                                                                                                                       |
| salesforce      | SalesforceAction                                                                                                                                                                               | Invia un messaggio a un flusso di input Salesforce IoT Cloud.                                                                                                                       |
| token           | Stringa<br>Lunghezza min.: 40                                                                                                                                                                  | Token usato per autenticare l'accesso al flusso di input Salesforce IoT Cloud. Il token è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input. |
| url             | Stringa<br>Lunghezza max: 2000<br>modello: https://ingestion-[a-zA-Z0-9]{1,12}.[a-zA-Z0-9]+.((sfdc-matrix.net) (sfdcnow.com))/streams/w <a href="#">1, 20</a> /w <a href="#">1, 20</a> /evento | URL esposto dal flusso di input Salesforce IoT Cloud. L'URL è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input.                             |
| iotAnalytics    | IotAnalyticsAction                                                                                                                                                                             | Invia i dati del messaggio a un canale AWS IoT Analytics.                                                                                                                           |

| Nome                | Tipo                                   | Descrizione                                                                                                                                                                                                                                             |
|---------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| channelArn          | Stringa                                | (obsoleto) L'ARN del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                                                                                                   |
| channelName         | Stringa                                | Il nome del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                                                                                                            |
| roleArn             | Stringa                                | L'ARN del ruolo con una policy che concede a IoT Analytics l'autorizzazione per l'invio di dati di messaggi tramite IoT Analytics (iotanalytics:BatchPutMessage).                                                                                       |
| iotEvents           | iotEventsAction                        | Invia un input a un rilevatore AWS IoT Events.                                                                                                                                                                                                          |
| inputName           | Stringa<br>Lunghezza max: 128, min.: 1 | Il nome dell'input AWS IoT Events.                                                                                                                                                                                                                      |
| messageId           | Stringa<br>Lunghezza max: 128          | [Opzionale] Da utilizzare per essere certi che il rilevatore AWS IoT Events elaborerà solo un messaggio di input con un determinato messageId.                                                                                                          |
| roleArn             | Stringa                                | L'ARN del ruolo che concede l'autorizzazione AWS IoT per inviare un messaggio di input a un rilevatore AWS IoT Events. ("Action":"iotevents:BatchPutMessage").                                                                                          |
| stepFunctions       | StepFunctionsAction                    | Avvia l'esecuzione di una macchina a stati Step Functions.                                                                                                                                                                                              |
| executionNamePrefix | Stringa                                | (Opzionale) All'esecuzione della macchina a stati verrà assegnato un nome costituito da questo prefisso seguito da un UUID. Step Functions crea automaticamente un nome univoco per ogni esecuzione della macchina a stati se non ne viene fornito uno. |
| stateMachineName    | Stringa                                | Il nome della macchina a stati Step Functions di cui verrà avviata l'esecuzione.                                                                                                                                                                        |
| roleArn             | Stringa                                | L'ARN del ruolo che concede a IoT l'autorizzazione per avviare l'esecuzione di una macchina a stati ("Action":"states:StartExecution").                                                                                                                 |

| Nome             | Tipo             | Descrizione                                                                                                                                                                                                                                      |
|------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ruleDisabled     | booleano         | Specifica se la regola è disabilitata.                                                                                                                                                                                                           |
| awslotSqlVersion | Stringa          | Versione del motore di regole SQL da usare durante la valutazione della regola.                                                                                                                                                                  |
| errorAction      | Action           | Operazione da eseguire quando si verifica un errore.                                                                                                                                                                                             |
| dynamoDB         | DynamoDBAction   | Scrive in una tabella DynamoDB.                                                                                                                                                                                                                  |
| tableName        | Stringa          | Nome della tabella DynamoDB.                                                                                                                                                                                                                     |
| roleArn          | Stringa          | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                                                                   |
| operation        | Stringa          | Tipo di operazione da eseguire. Segue il modello di sostituzione, per cui può essere <code>\$operation</code> , ma la sostituzione deve restituire uno dei risultati seguenti: <code>INSERT</code> , <code>UPDATE</code> o <code>DELETE</code> . |
| hashKeyField     | Stringa          | Nome della chiave hash.                                                                                                                                                                                                                          |
| hashKeyValue     | Stringa          | Valore della chiave hash.                                                                                                                                                                                                                        |
| hashKeyType      | Stringa          | Tipo di chiave hash. I valori validi sono "STRING" e "NUMBER"<br><br>Enumerazione: STRING   NUMBER                                                                                                                                               |
| rangeKeyField    | Stringa          | Nome della chiave di intervallo.                                                                                                                                                                                                                 |
| rangeKeyValue    | Stringa          | Valore della chiave di intervallo.                                                                                                                                                                                                               |
| rangeKeyType     | Stringa          | Tipo di chiave di intervallo. I valori validi sono "STRING" e "NUMBER"<br><br>Enumerazione: STRING   NUMBER                                                                                                                                      |
| payloadField     | Stringa          | Payload dell'operazione. Questo nome può essere personalizzato.                                                                                                                                                                                  |
| dynamoDBv2       | DynamoDBv2Action | Scrive in una tabella DynamoDB. Questa è una nuova versione dell'operazione DynamoDB. Permette di scrivere ogni attributo incluso nel payload di un messaggio MQTT in una colonna DynamoDB separata.                                             |

| Nome          | Tipo         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn       | Stringa      | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| putItem       | PutItemInput | <p>Specifica la tabella DynamoDB in cui verranno scritti i dati del messaggio. Ad esempio:</p> <pre>{ "dynamoDBv2": { "roleArn": "aws:iam:12341251:my-role" "putItem": { "tableName": "my-table" } } }</pre> <p>Ogni attributo nel payload del messaggio verrà scritto in una colonna separata del database DynamoDB.</p>                                                                                                                                                                                                                                                                                              |
| tableName     | Stringa      | Tabella in cui verranno scritti i dati del messaggio.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| lambda        | LambdaAction | Richiama una funzione Lambda.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| functionArn   | Stringa      | ARN della funzione Lambda.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| sns           | SnsAction    | Pubblica in un argomento Amazon SNS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| targetArn     | Stringa      | ARN dell'argomento SNS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| roleArn       | Stringa      | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| messageFormat | Stringa      | <p>(Opzionale) Formato del messaggio da pubblicare. I valori accettati sono "JSON" e "RAW". Il valore predefinito dell'attributo è "RAW". SNS usa questa impostazione per determinare se il payload deve essere analizzato e se devono essere estratti i bit specifici della piattaforma rilevanti del payload. Per ulteriori informazioni sui formati di messaggio SNS, consulta la pagina <a href="https://docs.aws.amazon.com/sns/latest/dg/json-formats.html">https://docs.aws.amazon.com/sns/latest/dg/json-formats.html</a> e fai riferimento alla documentazione ufficiale.</p> <p>Enumerazione: RAW   JSON</p> |
| sqs           | SqsAction    | Pubblica in una coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Nome         | Tipo            | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn      | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                         |
| queueUrl     | Stringa         | URL della coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| useBase64    | booleano        | Specifica se usare la codifica Base64.                                                                                                                                                                                                                                                                                                                                                                                                           |
| kinesis      | KinesisAction   | Scrive i dati in un flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                       |
| roleArn      | Stringa         | ARN del ruolo IAM che concede l'accesso al flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                |
| streamName   | Stringa         | Nome del flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| partitionKey | Stringa         | Chiave di partizione.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| republish    | RepublishAction | Pubblica in un altro argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                             |
| roleArn      | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                         |
| argomento    | Stringa         | Nome dell'argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| s3           | S3Action        | Scrive in un bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| roleArn      | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                         |
| bucketName   | Stringa         | Bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| key          | Stringa         | Chiave dell'oggetto.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| cannedAcl    | Stringa         | <p>Lista di controllo degli accessi predefinita Amazon S3 che controlla l'accesso all'oggetto identificato dalla chiave dell'oggetto. Per ulteriori informazioni, consulta la pagina relativa alle <a href="#">liste di controllo degli accessi predefinite S3</a>.</p> <p>Enumerazione: private   public-read   public-read-write   aws-exec-read   authenticated-read   bucket-owner-read   bucket-owner-full-control   log-delivery-write</p> |
| firehose     | FirehoseAction  | Scrive in un flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                                                     |
| roleArn      | Stringa         | Ruolo IAM che concede l'accesso al flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                               |

| Nome               | Tipo                              | Descrizione                                                                                                                                                                                         |
|--------------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| deliveryStreamName | Stringa                           | Nome del flusso di distribuzione.                                                                                                                                                                   |
| separator          | Stringa<br>Modello: ([ ]) ( ) (.) | Separatore di caratteri che verrà usato per separare i record scritti nel flusso Firehose. I valori validi sono: '\n' (nuova riga), '\t' (tabulazione), '\r\n' (nuova riga Windows), ',' (virgola). |
| cloudwatchMetric   | CloudwatchMetricAction            | Acquisisce un parametro CloudWatch.                                                                                                                                                                 |
| roleArn            | Stringa                           | Ruolo IAM che permette l'accesso al parametro CloudWatch.                                                                                                                                           |
| metricNamespace    | Stringa                           | Namespace dei nomi del parametro CloudWatch.                                                                                                                                                        |
| metricName         | Stringa                           | Nome parametro CloudWatch.                                                                                                                                                                          |
| metricValue        | Stringa                           | Valore del parametro CloudWatch.                                                                                                                                                                    |
| metricUnit         | Stringa                           | <a href="#">Unità di misura del parametro</a> supportata da CloudWatch.                                                                                                                             |
| metricTimestamp    | Stringa                           | Uno <a href="#">Timestamp Unix</a> opzionale.                                                                                                                                                       |
| cloudwatchAlarm    | CloudwatchAlarmAction             | Modifica lo stato di un allarme CloudWatch.                                                                                                                                                         |
| roleArn            | Stringa                           | Ruolo IAM che permette l'accesso all'allarme CloudWatch.                                                                                                                                            |
| alarmName          | Stringa                           | Nome dell'allarme CloudWatch.                                                                                                                                                                       |
| stateReason        | Stringa                           | Motivo della modifica dell'allarme.                                                                                                                                                                 |
| stateValue         | Stringa                           | Valore dello stato dell'allarme. I valori accettabili sono: OK, ALARM, INSUFFICIENT_DATA.                                                                                                           |
| elasticsearch      | ElasticsearchAction               | Scrive dati in un dominio Amazon Elasticsearch Service.                                                                                                                                             |
| roleArn            | Stringa                           | ARN del ruolo IAM che ha accesso a Elasticsearch.                                                                                                                                                   |
| endpoint           | Stringa<br>modello: https?://.*   | Endpoint del dominio Elasticsearch.                                                                                                                                                                 |
| index              | Stringa                           | Indice Elasticsearch in cui vuoi archiviare i dati.                                                                                                                                                 |
| type               | Stringa                           | Tipo di documento che stai archiviando.                                                                                                                                                             |

| Nome         | Tipo                                                                                                                                                                               | Descrizione                                                                                                                                                                         |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id           | Stringa                                                                                                                                                                            | Identificatore univoco per il documento che stai archiviando.                                                                                                                       |
| salesforce   | SalesforceAction                                                                                                                                                                   | Invia un messaggio a un flusso di input Salesforce IoT Cloud.                                                                                                                       |
| token        | Stringa<br><br>Lunghezza min.: 40                                                                                                                                                  | Token usato per autenticare l'accesso al flusso di input Salesforce IoT Cloud. Il token è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input. |
| url          | Stringa<br><br>Lunghezza max: 2000<br><br>modello: https://ingestion-[a-zA-Z0-9]{1,12}.[a-zA-Z0-9]+.((sfdc-matrix.net) (sfdcnow.com))/streams/w <b>1,20</b> /w <b>1,20</b> /evento | URL esposto dal flusso di input Salesforce IoT Cloud. L'URL è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input.                             |
| iotAnalytics | IoTAnalyticsAction                                                                                                                                                                 | Invia i dati del messaggio a un canale AWS IoT Analytics.                                                                                                                           |
| channelArn   | Stringa                                                                                                                                                                            | (obsoleto) L'ARN del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                               |
| channelName  | Stringa                                                                                                                                                                            | Il nome del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                                        |
| roleArn      | Stringa                                                                                                                                                                            | L'ARN del ruolo con una policy che concede a IoT Analytics l'autorizzazione per l'invio di dati di messaggi tramite IoT Analytics (iotanalytics:BatchPutMessage).                   |
| iotEvents    | IoTEventsAction                                                                                                                                                                    | Invia un input a un rilevatore AWS IoT Events.                                                                                                                                      |
| inputName    | Stringa<br><br>Lunghezza max: 128, min.: 1                                                                                                                                         | Il nome dell'input AWS IoT Events.                                                                                                                                                  |
| messageld    | Stringa<br><br>Lunghezza max: 128                                                                                                                                                  | [Opzionale] Da utilizzare per essere certi che il rilevatore AWS IoT Events elaborerà solo un messaggio di input con un determinato messageld.                                      |

| Nome                | Tipo                | Descrizione                                                                                                                                                                                                                                             |
|---------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn             | Stringa             | L'ARN del ruolo che concede l'autorizzazione AWS IoT per inviare un messaggio di input a un rilevatore AWS IoT Events. ("Action":"iotevents:BatchPutMessage").                                                                                          |
| stepFunctions       | StepFunctionsAction | Avvia l'esecuzione di una macchina a stati Step Functions.                                                                                                                                                                                              |
| executionNamePrefix | Stringa             | (Opzionale) All'esecuzione della macchina a stati verrà assegnato un nome costituito da questo prefisso seguito da un UUID. Step Functions crea automaticamente un nome univoco per ogni esecuzione della macchina a stati se non ne viene fornito uno. |
| stateMachineName    | Stringa             | Il nome della macchina a stati Step Functions di cui verrà avviata l'esecuzione.                                                                                                                                                                        |
| roleArn             | Stringa             | L'ARN del ruolo che concede a IoT l'autorizzazione per avviare l'esecuzione di una macchina a stati ("Action":"states:StartExecution").                                                                                                                 |

## Errori

### InternalException

Si è verificato un errore imprevisto.

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

## GetV2LoggingOptions

Ottiene le opzioni di logging granulare.

### Riepilogo

```
aws iot get-v2-logging-options \
```

```
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
}
```

Output

```
{
 "roleArn": "string",
 "defaultLogLevel": "string",
 "disableAllLogs": "boolean"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome            | Tipo     | Descrizione                                                                         |
|-----------------|----------|-------------------------------------------------------------------------------------|
| roleArn         | Stringa  | ARN del ruolo IAM usato da AWS IoT per scrivere nei log di CloudWatch.              |
| defaultLogLevel | Stringa  | Livello di log predefinito.<br>Enumerazione: DEBUG   INFO   ERROR   WARN   DISABLED |
| disableAllLogs  | booleano | Disabilita tutti i log.                                                             |

Errori

`InternalException`

Si è verificato un errore imprevisto.

`NotConfiguredException`

La risorsa non è configurata.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

## ListActiveViolations

Elenca le violazioni attive per un determinato profilo di sicurezza di Device Defender.

Riepilogo

```
aws iot list-active-violations \
[--thing-name <value>] \
[--security-profile-name <value>] \
[--next-token <value>] \
[--max-results <value>] \

```

```
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "thingName": "string",
 "securityProfileName": "string",
 "nextToken": "string",
 "maxResults": "integer"
}
```

#### Campi di **cli-input-json**

| Nome                | Tipo    | Descrizione                                                                                                                                                 |
|---------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingName           | Stringa | Nome dell'oggetto per il quale vengono elencate le violazioni attive.<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+                         |
| securityProfileName | Stringa | Nome del profilo di sicurezza di Device Defender per il quale vengono elencate le violazioni.<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ |
| nextToken           | Stringa | Token per il set di risultati successivo.                                                                                                                   |
| maxResults          | intero  | Numero massimo di risultati da restituire per volta.<br>Intervallo – Max: 250, min.: 1                                                                      |

#### Output

```
{
 "activeViolations": [
 {
 "violationId": "string",
 "thingName": "string",
 "securityProfileName": "string",
 "behavior": {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 },
 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 }
 }
 }
 }
]
}
```

```

 "statistic": "string"
 }
},
"lastViolationValue": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
},
"lastViolationTime": "timestamp",
"violationStartTime": "timestamp"
},
],
"nextToken": "string"
}
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome                | Tipo                                                                          | Descrizione                                                                                        |
|---------------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| activeViolations    | elenco<br>membro: ActiveViolation                                             | Elenco di violazioni attive.                                                                       |
| violationId         | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 -]+   | ID della violazione attiva.                                                                        |
| thingName           | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto responsabile della violazione attiva.                                            |
| securityProfileName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Profilo di sicurezza il cui comportamento causa una violazione.                                    |
| behavior            | Behavior                                                                      | Comportamento che viene violato.                                                                   |
| name                | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome assegnato al comportamento.                                                                   |
| metric              | Stringa                                                                       | Valore misurato dal comportamento.                                                                 |
| criteria            | BehaviorCriteria                                                              | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a metric. |

| Nome               | Tipo                             | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| comparisonOperator | Stringa                          | Operatore che mette in correlazione l'oggetto misurato ( <code>metric</code> ) e i criteri (contenenti un <code>value</code> o <code>statisticalThreshold</code> ).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set                                                                                                                                                                                                                                                            |
| value              | MetricValue                      | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count              | Long<br><br>Intervallo - min.: 0 | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cidrs              | elenco<br><br>membro: Cidr       | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports              | elenco<br><br>membro: Port       | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds    | intero                           | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |

| Nome                         | Tipo                                                                     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| consecutiveDatapointsToAlarm | intero<br>Intervallo – Max: 10, min.: 1                                  | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| consecutiveDatapointsToClear | intero<br>Intervallo – Max: 10, min.: 1                                  | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| statisticalThreshold         | StatisticalThreshold                                                     | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistic                    | Stringa<br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato ( <code>durationSeconds</code> ) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto ( <code>comparisonOperator</code> ) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario si verifica una violazione. |
| lastViolationValue           | MetricValue                                                              | Valore del parametro (misurazione) che ha causato la violazione più recente.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| count                        | Long<br>Intervallo - min.: 0                                             | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Nome               | Tipo                   | Descrizione                                                                                                                                       |
|--------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| cids               | elenco<br>membro: Cidr | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .  |
| ports              | elenco<br>membro: Port | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> . |
| lastViolationTime  | timestamp              | Ora in cui si è verificata la violazione più recente.                                                                                             |
| violationStartTime | timestamp              | Ora di inizio della violazione.                                                                                                                   |
| nextToken          | Stringa                | Token che è possibile usare per recuperare il set di risultati successivo oppure <code>null</code> se non ci sono risultati aggiuntivi.           |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

## ListAttachedPolicies

Elenca le policy collegate al gruppo di oggetti specificato.

#### Riepilogo

```
aws iot list-attached-policies \
--target <value> \
[--recursive | --no-recursive] \
[--marker <value>] \
[--page-size <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "target": "string",
```

```

 "recursive": "boolean",
 "marker": "string",
 "pageSize": "integer"
}

```

### Campi di **cli-input-json**

| Nome      | Tipo                                         | Descrizione                                                   |
|-----------|----------------------------------------------|---------------------------------------------------------------|
| target    | Stringa                                      | Gruppo per cui le policy verranno elencate.                   |
| recursive | booleano                                     | Se è true, elenca in modo ricorsivo le policy collegate.      |
| marker    | Stringa<br>Modello: [A-Z a-z 0-9 +/]++={0,2} | Token usato per recuperare il successivo set di risultati.    |
| pageSize  | intero<br>Intervallo – Max: 250, min.: 1     | Numero massimo di risultati da restituire per ogni richiesta. |

### Output

```
{
 "policies": [
 {
 "policyName": "string",
 "policyArn": "string"
 }
],
 "nextMarker": "string"
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome       | Tipo                                                          | Descrizione                                                                                     |
|------------|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| policies   | elenco<br>Membro: Policy<br>Classe Java: java.util.List       | Policy.                                                                                         |
| policyName | Stringa<br>Lunghezza max: 128, min.: 1<br>modello: [w+=,.@-]+ | Nome della policy.                                                                              |
| policyArn  | Stringa                                                       | ARN della policy.                                                                               |
| nextMarker | Stringa<br>Modello: [A-Z a-z 0-9 +/]++={0,2}                  | Token per recuperare il successivo set di risultati oppure null se non ci sono altri risultati. |

### Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

**LimitExceededException**

È stato superato un limite.

## ListAuditFindings

Elenca i risultati di un audit di Device Defender o degli audit eseguiti durante un periodo di tempo specificato. I risultati vengono conservati per 180 giorni.

Riepilogo

```
aws iot list-audit-findings \
[--task-id <value>] \
[--check-name <value>] \
[--resource-identifier <value>] \
[--max-results <value>] \
[--next-token <value>] \
[--start-time <value>] \
[--end-time <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di cli-input-json

```
{
 "taskId": "string",
 "checkName": "string",
 "resourceIdentifier": {
 "deviceCertificateId": "string",
 "caCertificateId": "string",
 "cognitoIdentityPoolId": "string",
 "clientId": "string",
 "policyVersionIdentifier": {
 "policyName": "string",
 "policyVersionId": "string"
 },
 "account": "string"
 },
 "maxResults": "integer",
 "nextToken": "string",
 "startTime": "timestamp",
 "endTime": "timestamp"
```

}

### Campi di **cli-input-json**

| Nome                    | Tipo                                                                           | Descrizione                                                                                                                                         |
|-------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| taskId                  | Stringa<br><br>Lunghezza max: 40, min.: 1<br><br>Modello: [a–z A–Z 0–9 -]+     | Filtro che limita i risultati all'audit con l'ID specificato. Devi specificare il valore di taskId oppure di startTime ed endTime, ma non entrambi. |
| checkName               | Stringa                                                                        | Filtro che limita i risultati al controllo di auditing specificato.                                                                                 |
| resourceIdentifier      | ResourceIdentifier                                                             | Informazioni che identificano la risorsa non conforme.                                                                                              |
| deviceCertificateId     | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a–f A–F 0–9]+ | ID del certificato collegato alla risorsa.                                                                                                          |
| caCertificateId         | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a–f A–F 0–9]+ | ID del certificato CA usato per autorizzare il certificato.                                                                                         |
| cognitoIdentityPoolId   | Stringa                                                                        | ID del pool di identità Cognito.                                                                                                                    |
| clientId                | Stringa                                                                        | ID client.                                                                                                                                          |
| policyVersionIdentifier | PolicyVersionIdentifier                                                        | Versione della policy associata alla risorsa.                                                                                                       |
| policyName              | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+          | Nome della policy.                                                                                                                                  |
| policyVersionId         | Stringa<br><br>Modello: [0–9]+                                                 | ID della versione della policy associata alla risorsa.                                                                                              |
| account                 | Stringa<br><br>Lunghezza max: 12, min.: 12<br><br>Modello: [0–9]+              | Account a cui è associata la risorsa.                                                                                                               |
| maxResults              | intero<br><br>Intervallo – Max: 250, min.: 1                                   | Numero massimo di risultati da restituire per volta. Il valore predefinito è 25.                                                                    |
| nextToken               | Stringa                                                                        | Token per il set di risultati successivo.                                                                                                           |
| startTime               | timestamp                                                                      | Filtro che limita i risultati a quelli trovati dopo l'ora specificata. Devi                                                                         |

| Nome    | Tipo      | Descrizione                                                                                                                                                      |
|---------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |           | specificare il valore di startTime ed endTime oppure di taskId, ma non entrambi.                                                                                 |
| endTime | timestamp | Filtro che limita i risultati a quelli trovati prima dell'ora specificata. Devi specificare il valore di startTime ed endTime oppure di taskId, ma non entrambi. |

### Output

```
{
 "findings": [
 {
 "taskId": "string",
 "checkName": "string",
 "taskStartTime": "timestamp",
 "findingTime": "timestamp",
 "severity": "string",
 "nonCompliantResource": {
 "resourceType": "string",
 "resourceIdentifier": {
 "deviceCertificateId": "string",
 "caCertificateId": "string",
 "cognitoIdentityPoolId": "string",
 "clientId": "string",
 "policyVersionIdentifier": {
 "policyName": "string",
 "policyVersionId": "string"
 },
 "account": "string"
 },
 "additionalInfo": {
 "string": "string"
 }
 },
 "relatedResources": [
 {
 "resourceType": "string",
 "resourceIdentifier": {
 "deviceCertificateId": "string",
 "caCertificateId": "string",
 "cognitoIdentityPoolId": "string",
 "clientId": "string",
 "policyVersionIdentifier": {
 "policyName": "string",
 "policyVersionId": "string"
 },
 "account": "string"
 },
 "additionalInfo": {
 "string": "string"
 }
 }
],
 "reasonForNonCompliance": "string",
 "reasonForNonComplianceCode": "string"
 }
],
 "nextToken": "string"
}
```

}

#### Campi di output dell'interfaccia a riga di comando

| Nome                  | Tipo                                                                           | Descrizione                                                                                                                                                                     |
|-----------------------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| risultati             | elenco<br><br>membro: AuditFinding                                             | Risultati dell'audit.                                                                                                                                                           |
| taskId                | Stringa<br><br>Lunghezza max: 40, min.: 1<br><br>Modello: [a–z A–Z 0–9 -]+     | ID dell'audit che ha generato il risultato                                                                                                                                      |
| checkName             | Stringa                                                                        | Controllo di auditing che ha generato il risultato.                                                                                                                             |
| taskStartTime         | timestamp                                                                      | Ora di inizio dell'audit.                                                                                                                                                       |
| findingTime           | timestamp                                                                      | Ora in cui è stato trovato il risultato.                                                                                                                                        |
| severity              | Stringa                                                                        | Gravità del risultato.<br><br>enumerazione: CRITICAL   HIGH   MEDIUM   LOW                                                                                                      |
| nonCompliantResource  | NonCompliantResource                                                           | Risorsa risultata non conforme dal controllo di auditing.                                                                                                                       |
| resourceType          | Stringa                                                                        | Tipo della risorsa non conforme.<br><br>enumerazione:<br>DEVICE_CERTIFICATE<br>  CA_CERTIFICATE<br>  IOT_POLICY<br>  COGNITO_IDENTITY_POOL<br>  CLIENT_ID<br>  ACCOUNT_SETTINGS |
| resourceIdentifier    | ResourceIdentifier                                                             | Informazioni che identificano la risorsa non conforme.                                                                                                                          |
| deviceCertificateId   | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato collegato alla risorsa.                                                                                                                                      |
| caCertificateId       | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato CA usato per autorizzare il certificato.                                                                                                                     |
| cognitoIdentityPoolId | Stringa                                                                        | ID del pool di identità Cognito.                                                                                                                                                |
| clientId              | Stringa                                                                        | ID client.                                                                                                                                                                      |

| Nome                    | Tipo                                                                                                                                                   | Descrizione                                                 |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| policyVersionIdentifier | PolicyVersionIdentifier                                                                                                                                | Versione della policy associata alla risorsa.               |
| policyName              | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w+=,.@-]+                                                                                  | Nome della policy.                                          |
| policyVersionId         | Stringa<br><br>Modello: [0-9]+                                                                                                                         | ID della versione della policy associata alla risorsa.      |
| account                 | Stringa<br><br>Lunghezza max: 12, min.: 12<br><br>Modello: [0-9]+                                                                                      | Account a cui è associata la risorsa.                       |
| additionalInfo          | mappa                                                                                                                                                  | Informazioni aggiuntive sulla risorsa non conforme.         |
| relatedResources        | elenco<br><br>membro: RelatedResource                                                                                                                  | Elenco delle risorse correlate.                             |
| resourceType            | Stringa<br><br>enumerazione:<br>DEVICE_CERTIFICATE<br>  CA_CERTIFICATE<br>  IOT_POLICY<br>  COGNITO_IDENTITY_POOL<br>  CLIENT_ID<br>  ACCOUNT_SETTINGS | Il tipo di risorsa.                                         |
| resourceIdentifier      | ResourceIdentifier                                                                                                                                     | Informazioni che identificano la risorsa.                   |
| deviceCertificateId     | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+                                                                         | ID del certificato collegato alla risorsa.                  |
| caCertificateId         | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+                                                                         | ID del certificato CA usato per autorizzare il certificato. |
| cognitoIdentityPoolId   | Stringa                                                                                                                                                | ID del pool di identità Cognito.                            |
| clientId                | Stringa                                                                                                                                                | ID client.                                                  |
| policyVersionIdentifier | PolicyVersionIdentifier                                                                                                                                | Versione della policy associata alla risorsa.               |

| Nome                       | Tipo                                                          | Descrizione                                                                                                                             |
|----------------------------|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| policyName                 | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [w+=,.@-]+ | Nome della policy.                                                                                                                      |
| policyVersionId            | Stringa<br>Modello: [0-9]+                                    | ID della versione della policy associata alla risorsa.                                                                                  |
| account                    | Stringa<br>Lunghezza max: 12, min.: 12<br>Modello: [0-9]+     | Account a cui è associata la risorsa.                                                                                                   |
| additionalInfo             | mappa                                                         | Informazioni aggiuntive sulla risorsa.                                                                                                  |
| reasonForNonCompliance     | Stringa                                                       | Motivo per cui la risorsa è risultata non conforme.                                                                                     |
| reasonForNonComplianceCode | Stringa                                                       | Codice che indica il motivo per cui la risorsa è risultata non conforme.                                                                |
| nextToken                  | Stringa                                                       | Token che è possibile usare per recuperare il set di risultati successivo oppure <code>null</code> se non ci sono risultati aggiuntivi. |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

## ListAuditTasks

Elenca gli audit di Device Defender eseguiti durante un determinato periodo di tempo.

#### Riepilogo

```
aws iot list-audit-tasks \
--start-time <value> \
--end-time <value> \
[--task-type <value>] \
[--task-status <value>] \
[--next-token <value>] \
[--max-results <value>] \
```

```
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "startTime": "timestamp",
 "endTime": "timestamp",
 "taskType": "string",
 "taskStatus": "string",
 "nextToken": "string",
 "maxResults": "integer"
}
```

#### Campi di **cli-input-json**

| Nome       | Tipo                                     | Descrizione                                                                                                                                                                                                                                                 |
|------------|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| startTime  | Timestamp                                | Inizio del periodo di tempo. Le informazioni sull'audit vengono conservate per un periodo di tempo limitato (180 giorni). Se viene richiesto un orario di inizio precedente ai risultati conservati, viene generata un'eccezione "InvalidRequestException". |
| endTime    | timestamp                                | Fine del periodo di tempo.                                                                                                                                                                                                                                  |
| taskType   | Stringa                                  | Filtro che limita l'output al tipo di audit specificato: può essere un valore tra "ON_DEMAND_AUDIT_TASK" o "SCHEDULED_AUDIT_TASK".<br><br>enumerazione:<br>ON_DEMAND_AUDIT_TASK   SCHEDULED_AUDIT_TASK                                                      |
| taskStatus | Stringa                                  | Filtro che limita l'output agli audit con lo stato di completamento specificato: può essere un valore tra "IN_PROGRESS", "COMPLETED", "FAILED" o "CANCELED".<br><br>enumerazione: IN_PROGRESS   COMPLETED   FAILED   CANCELED                               |
| nextToken  | Stringa                                  | Token per il set di risultati successivo.                                                                                                                                                                                                                   |
| maxResults | intero<br>Intervallo – Max: 250, min.: 1 | Numero massimo di risultati da restituire per volta. Il valore predefinito è 25.                                                                                                                                                                            |

#### Output

```
{
 "tasks": [
 {
 "taskId": "string",
 "taskStatus": "string",
 "taskType": "string"
 }
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome       | Tipo                                                                       | Descrizione                                                                                                                                         |
|------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| attività   | elenco<br><br>membro: AuditTaskMetadata<br><br>Classe Java: java.util.List | Audit eseguiti durante il periodo di tempo specificato.                                                                                             |
| taskId     | Stringa<br><br>Lunghezza max: 40, min.: 1<br><br>Modello: [a-z A-Z 0-9 -]+ | ID dell'audit.                                                                                                                                      |
| taskStatus | Stringa                                                                    | Stato dell'audit: un valore tra "IN_PROGRESS", "COMPLETED", "FAILED" o "CANCELED".<br><br>enumerazione: IN_PROGRESS   COMPLETED   FAILED   CANCELED |
| taskType   | Stringa                                                                    | Tipo di audit: un valore tra "ON_DEMAND_AUDIT_TASK" o "SCHEDULED_AUDIT_TASK".<br><br>enumerazione:<br>ON_DEMAND_AUDIT_TASK   SCHEDULED_AUDIT_TASK   |
| nextToken  | Stringa                                                                    | Token che è possibile usare per recuperare il set di risultati successivo oppure null se non ci sono risultati aggiuntivi.                          |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

### InternalFailureException

Si è verificato un errore imprevisto.

## ListAuthorizers

Elenca le autorizzazioni registrate nell'account.

### Riepilogo

```
aws iot list-authorizers \
[--page-size <value>] \
[--marker <value>] \
[--ascending-order | --no-ascending-order] \
[--status <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di **cli-input-json**

```
{
 "pageSize": "integer",
 "marker": "string",
 "ascendingOrder": "boolean",
 "status": "string"
}
```

### Campi di **cli-input-json**

| Nome           | Tipo     | Descrizione                                                                                         |
|----------------|----------|-----------------------------------------------------------------------------------------------------|
| pageSize       | intero   | Numero massimo di risultati da restituire per volta.<br>Intervallo – Max: 250, min.: 1              |
| marker         | Stringa  | Contrassegno usato per ottenere il successivo set di risultati.<br>Modello: [A-Z a-z 0-9 +/]+={0,2} |
| ascendingOrder | booleano | Restituisce l'elenco delle autorizzazioni in ordine alfabetico crescente.                           |
| status         | Stringa  | Stato della richiesta di elenco delle autorizzazioni.<br>Enumerazione: ACTIVE   INACTIVE            |

### Output

```
{
 "authorizers": [
 {
 "authorizerName": "string",
```

```

 "authorizerArn": "string"
 }
],
"nextMarker": "string"
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo                                                                       | Descrizione                                                     |
|----------------|----------------------------------------------------------------------------|-----------------------------------------------------------------|
| authorizers    | elenco<br><br>Membro: AuthorizerSummary<br><br>Classe Java: java.util.List | Autorizzazioni.                                                 |
| authorizerName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=,@-]+        | Nome dell'autorizzazione.                                       |
| authorizerArn  | Stringa                                                                    | ARN dell'autorizzazione.                                        |
| nextMarker     | Stringa<br><br>Modello: [A–Z a–z 0–9 +/]++{0,2}                            | Contrassegno usato per ottenere il successivo set di risultati. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

##### InternalFailureException

Si è verificato un errore imprevisto.

## ListBillingGroups

Elenca i gruppi di fatturazione creati.

#### Riepilogo

```

aws iot list-billing-groups \
[--next-token <value>] \
[--max-results <value>] \

```

```
[--name-prefix-filter <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "nextToken": "string",
 "maxResults": "integer",
 "namePrefixFilter": "string"
}
```

#### Campi di cli-input-json

| Nome             | Tipo                                                                          | Descrizione                                                                                     |
|------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| nextToken        | Stringa                                                                       | Token usato per recuperare il successivo set di risultati.                                      |
| maxResults       | intero                                                                        | Numero massimo di risultati da restituire per ogni richiesta.<br>Intervallo – Max: 250, min.: 1 |
| namePrefixFilter | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Limita i risultati ai gruppi di fatturazione, in cui i nomi hanno il prefisso dato.             |

#### Output

```
{
 "billingGroups": [
 {
 "groupName": "string",
 "groupArn": "string"
 }
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome          | Tipo                                                                          | Descrizione                          |
|---------------|-------------------------------------------------------------------------------|--------------------------------------|
| billingGroups | elenco<br><br>Membro: GroupNameAndArn<br><br>Classe Java: java.util.List      | L'elenco dei gruppi di fatturazione. |
| groupName     | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del gruppo.                     |
| groupArn      | Stringa                                                                       | ARN del gruppo.                      |

| Nome      | Tipo    | Descrizione                                                                                              |
|-----------|---------|----------------------------------------------------------------------------------------------------------|
| nextToken | Stringa | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `ThrottlingException`

La velocità supera il limite.

## ListCACertificates

Elenca i certificati CA registrati per l'account AWS.

I risultati vengono restituiti nella pagina con una dimensione di pagina predefinita pari a 25. Puoi usare il contrassegno restituito per recuperare risultati aggiuntivi.

#### Riepilogo

```
aws iot list-ca-certificates \
[--page-size <value>] \
[--marker <value>] \
[--ascending-order | --no-ascending-order] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato `cli-input-json`

```
{
 "pageSize": "integer",
 "marker": "string",
 "ascendingOrder": "boolean"
}
```

#### Campi di `cli-input-json`

| Nome     | Tipo    | Descrizione                                                                           |
|----------|---------|---------------------------------------------------------------------------------------|
| pageSize | intero  | Dimensione della pagina dei risultati.<br>Intervallo – Max: 250, min.: 1              |
| marker   | Stringa | Contrassegno per il successivo set di risultati.<br>Modello: [A-Z a-z 0-9 +/]++={0,2} |

| Nome           | Tipo     | Descrizione                       |
|----------------|----------|-----------------------------------|
| ascendingOrder | booleano | Determina l'ordine dei risultati. |

#### Output

```
{
 "certificates": [
 {
 "certificateArn": "string",
 "certificateId": "string",
 "status": "string",
 "creationDate": "timestamp"
 }
],
 "nextMarker": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo                                                                                                                   | Descrizione                                                                                                                              |
|----------------|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| certificates   | elenco<br>Membro: CACertificate<br>Classe Java: java.util.List                                                         | Certificati CA registrati nell'account AWS.                                                                                              |
| certificateArn | Stringa                                                                                                                | ARN del certificato CA.                                                                                                                  |
| certificateId  | Stringa<br>Lunghezza max: 64, min.: 64<br>Modello: (0x)?[a-f A-F 0-9]+                                                 | ID del certificato CA.                                                                                                                   |
| status         | Stringa<br>Il valore di stato REGISTER_INACTIVE è obsoleto e non deve essere usato.<br>Enumerazione: ACTIVE   INACTIVE | Stato del certificato CA.<br>Il valore di stato REGISTER_INACTIVE è obsoleto e non deve essere usato.<br>Enumerazione: ACTIVE   INACTIVE |
| creationDate   | Timestamp                                                                                                              | Data di creazione del certificato CA.                                                                                                    |
| nextMarker     | Stringa<br>Modello: [A-Z a-z 0-9 +/]++={0,2}                                                                           | Posizione corrente all'interno dell'elenco di certificati CA.                                                                            |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

#### ThrottlingException

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## ListCertificates

Elenca i certificati registrati nell'account AWS.

I risultati vengono restituiti nella pagina con una dimensione di pagina predefinita pari a 25. Puoi usare il contrassegno restituito per recuperare risultati aggiuntivi.

#### Riepilogo

```
aws iot list-certificates \
[--page-size <value>] \
[--marker <value>] \
[--ascending-order | --no-ascending-order] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "pageSize": "integer",
 "marker": "string",
 "ascendingOrder": "boolean"
}
```

#### Campi di cli-input-json

| Nome           | Tipo                                         | Descrizione                                                                                                                           |
|----------------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| pageSize       | intero                                       | Dimensione della pagina dei risultati.<br>Intervallo – Max: 250, min.: 1                                                              |
| marker         | Stringa<br>Modello: [A-Z a-z 0-9 +/]++={0,2} | Contrassegno per il successivo set di risultati.                                                                                      |
| ascendingOrder | booleano                                     | Specifica l'ordine per i risultati.<br>Se è True, i risultati vengono restituiti in ordine crescente, in base alla data di creazione. |

#### Output

```
{
```

```

"certificates": [
 {
 "certificateArn": "string",
 "certificateId": "string",
 "status": "string",
 "creationDate": "timestamp"
 }
],
"nextMarker": "string"
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo                                                                                                                                                                                                 | Descrizione                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| certificates   | elenco<br><br>Membro: Certificate<br><br>Classe Java: java.util.List                                                                                                                                 | Descrizioni dei certificati.                                                                     |
| certificateArn | Stringa                                                                                                                                                                                              | ARN del certificato.                                                                             |
| certificateId  | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+                                                                                                                       | ID del certificato. L'ultima parte dell'ARN del certificato contiene l'ID certificato.           |
| status         | Stringa<br><br>Il valore di stato REGISTER_INACTIVE è obsoleto e non deve essere usato.<br><br>Enumerazione: ACTIVE   INACTIVE   REVOKED   PENDING_TRANSFER   REGISTER_INACTIVE   PENDING_ACTIVATION | Stato del certificato.                                                                           |
| creationDate   | Timestamp                                                                                                                                                                                            | Data e ora di creazione del certificato.                                                         |
| nextMarker     | Stringa<br><br>Modello: [A-Z a-z 0-9 +/]++={0,2}                                                                                                                                                     | Contrassegno per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## ListCertificatesByCA

Elenca i certificati dei dispositivi firmati dal certificato CA specificato.

### Riepilogo

```
aws iot list-certificates-by-ca \
--ca-certificate-id <value> \
[--page-size <value>] \
[--marker <value>] \
[--ascending-order | --no-ascending-order] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "caCertificateId": "string",
 "pageSize": "integer",
 "marker": "string",
 "ascendingOrder": "boolean"
}
```

### Campi di cli-input-json

| Nome            | Tipo     | Descrizione                                                                                                                                                                                                       |
|-----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| caCertificateId | Stringa  | ID del certificato CA. Questa operazione elencherà tutti i certificati registrati dei dispositivi che sono stati firmati da questo certificato CA.<br>Lunghezza max: 64, min.: 64<br>Modello: (0x)?[a-f A-F 0-9]+ |
| pageSize        | intero   | Dimensione della pagina dei risultati.<br>Intervallo – Max: 250, min.: 1                                                                                                                                          |
| marker          | Stringa  | Contrassegno per il successivo set di risultati.<br>Modello: [A-Z a-z 0-9 +/]++={0,2}                                                                                                                             |
| ascendingOrder  | booleano | Specifica l'ordine per i risultati. Se è True, i risultati vengono restituiti in ordine crescente, in base alla data di creazione.                                                                                |

### Output

```
{
```

```

"certificates": [
 {
 "certificateArn": "string",
 "certificateId": "string",
 "status": "string",
 "creationDate": "timestamp"
 }
],
"nextMarker": "string"
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo                                                                                                                                                                                                 | Descrizione                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| certificates   | elenco<br><br>Membro: Certificate<br><br>Classe Java: java.util.List                                                                                                                                 | Certificati dei dispositivi firmati dal certificato CA specificato.                              |
| certificateArn | Stringa                                                                                                                                                                                              | ARN del certificato.                                                                             |
| certificateId  | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+                                                                                                                       | ID del certificato. L'ultima parte dell'ARN del certificato contiene l'ID certificato.           |
| status         | Stringa<br><br>Il valore di stato REGISTER_INACTIVE è obsoleto e non deve essere usato.<br><br>Enumerazione: ACTIVE   INACTIVE   REVOKED   PENDING_TRANSFER   REGISTER_INACTIVE   PENDING_ACTIVATION | Stato del certificato.                                                                           |
| creationDate   | Timestamp                                                                                                                                                                                            | Data e ora di creazione del certificato.                                                         |
| nextMarker     | Stringa<br><br>Modello: [A-Z a-z 0-9 +/]++={0,2}                                                                                                                                                     | Contrassegno per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## ListIndices

Elenca gli indici di ricerca.

### Riepilogo

```
aws iot list-indices \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "nextToken": "string",
 "maxResults": "integer"
}
```

### Campi di cli-input-json

| Nome       | Tipo                                     | Descrizione                                                                                              |
|------------|------------------------------------------|----------------------------------------------------------------------------------------------------------|
| nextToken  | Stringa                                  | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |
| maxResults | intero<br>Intervallo – Max: 500, min.: 1 | Numero massimo di risultati da restituire per volta.                                                     |

### Output

```
{
 "indexNames": [
 "string"
],
 "nextToken": "string"
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome       | Tipo                                                       | Descrizione        |
|------------|------------------------------------------------------------|--------------------|
| indexNames | elenco<br>Membro: IndexName<br>Classe Java: java.util.List | Nomi degli indici. |

| Nome      | Tipo    | Descrizione                                                                                              |
|-----------|---------|----------------------------------------------------------------------------------------------------------|
| nextToken | Stringa | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

##### InternalFailureException

Si è verificato un errore imprevisto.

## ListJobExecutionsForJob

Elenca le esecuzioni per un processo.

#### Riepilogo

```
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]
```

#### Formato di cli-input-json

```
{
 "jobId": "string",
 "status": "string",
 "maxResults": "integer",
 "nextToken": "string"
}
```

#### Campi di cli-input-json

| Nome  | Tipo    | Descrizione                                                                                            |
|-------|---------|--------------------------------------------------------------------------------------------------------|
| jobId | Stringa | Identificatore univoco assegnato al processo al momento della creazione.<br>Lunghezza max: 64, min.: 1 |

| Nome       | Tipo                                     | Descrizione                                                                                                                           |
|------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
|            | Modello: [a–z A–Z 0–9 _]+                |                                                                                                                                       |
| stato      | Stringa                                  | <p>Stato del processo.</p> <p>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED</p> |
| maxResults | intero<br>Intervallo – Max: 250, min.: 1 | Numero massimo di risultati da restituire per ogni richiesta.                                                                         |
| nextToken  | Stringa                                  | Token usato per recuperare il successivo set di risultati.                                                                            |

#### Output

```
{
 "executionSummaries": [
 {
 "thingArn": "string",
 "jobExecutionSummary": {
 "status": "string",
 "queuedAt": "timestamp",
 "startedAt": "timestamp",
 "lastUpdatedAt": "timestamp",
 "executionNumber": "long"
 }
 }
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome                | Tipo                                                                          | Descrizione                                                                                      |
|---------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| executionSummaries  | elenco<br>Membro:<br>JobExecutionSummaryForJob<br>Classe Java: java.util.List | Elenco dei riepiloghi di esecuzione del processo.                                                |
| thingArn            | Stringa                                                                       | ARN dell'oggetto in cui è in corso l'esecuzione del processo.                                    |
| jobExecutionSummary | JobExecutionSummary                                                           | Contiene un sottoinsieme delle informazioni sull'esecuzione di un processo.                      |
| stato               | Stringa                                                                       | <p>Stato dell'esecuzione del processo.</p> <p>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED</p> |

| Nome            | Tipo      | Descrizione                                                                                                                                                                                                                                                            |
|-----------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |           | FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED                                                                                                                                                                                                                     |
| queuedAt        | timestamp | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                                                                                                             |
| startedAt       | timestamp | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                                                                                                                          |
| lastUpdatedAt   | timestamp | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                                                                                                                           |
| executionNumber | Long      | Stringa (costituita dalle cifre comprese tra 0 e 9) che identifica l'esecuzione di questo determinato processo in questo dispositivo specifico. Può essere usato successivamente in comandi che restituiscono o aggiornano le informazioni di esecuzione del processo. |
| nextToken       | Stringa   | Token per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi.                                                                                                                                                                              |

## Errori

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ResourceNotFoundException

La risorsa specificata non esiste.

### ThrottlingException

La velocità supera il limite.

### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

## ListJobExecutionsForThing

Elenca le esecuzioni del processo per l'oggetto specificato.

### Riepilogo

```
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]
```

Formato di **cli-input-json**

```
{
 "thingName": "string",
 "status": "string",
 "maxResults": "integer",
 "nextToken": "string"
}
```

Campi di **cli-input-json**

| Nome       | Tipo    | Descrizione                                                                                                                                                                                  |
|------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingName  | Stringa | Nome dell'oggetto.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+                                                                                                     |
| stato      | Stringa | Filtro opzionale che permette di cercare processi che hanno lo stato specificato.<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED |
| maxResults | intero  | Numero massimo di risultati da restituire per ogni richiesta.<br><br>Intervallo – Max: 250, min.: 1                                                                                          |
| nextToken  | Stringa | Token usato per recuperare il successivo set di risultati.                                                                                                                                   |

Output

```
{
 "executionSummaries": [
 {
 "jobId": "string",
 "jobExecutionSummary": {
 "status": "string",
 "queuedAt": "timestamp",
 "startedAt": "timestamp",
 "lastUpdatedAt": "timestamp",
 "executionNumber": "long"
 }
 }
],
 "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome                | Tipo                                                                                    | Descrizione                                                                                                                                                                                                                                                            |
|---------------------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| executionSummaries  | elenco<br><br>Membro:<br>JobExecutionSummaryForThing<br><br>Classe Java: java.util.List | Elenco dei riepiloghi di esecuzione del processo.                                                                                                                                                                                                                      |
| jobId               | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+              | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                                                                                               |
| jobExecutionSummary | JobExecutionSummary                                                                     | Contiene un sottoinsieme delle informazioni sull'esecuzione di un processo.                                                                                                                                                                                            |
| stato               | Stringa                                                                                 | Stato dell'esecuzione del processo.<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED                                                                                                                         |
| queuedAt            | timestamp                                                                               | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                                                                                                             |
| startedAt           | timestamp                                                                               | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                                                                                                                          |
| lastUpdatedAt       | timestamp                                                                               | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                                                                                                                           |
| executionNumber     | Long                                                                                    | Stringa (costituita dalle cifre comprese tra 0 e 9) che identifica l'esecuzione di questo determinato processo in questo dispositivo specifico. Può essere usato successivamente in comandi che restituiscono o aggiornano le informazioni di esecuzione del processo. |
| nextToken           | Stringa                                                                                 | Token per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi.                                                                                                                                                                              |

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

## ListJobs

Elenca i processi.

### Riepilogo

```
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]
```

### Formato di cli-input-json

```
{
 "status": "string",
 "targetSelection": "string",
 "maxResults": "integer",
 "nextToken": "string",
 "thingGroupName": "string",
 "thingGroupId": "string"
}
```

### Campi di **cli-input-json**

| Nome            | Tipo    | Descrizione                                                                                                                                                                        |
|-----------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| stato           | Stringa | Filtro opzionale che permette di cercare processi che hanno lo stato specificato.<br><br>enum: IN_PROGRESS   CANCELED   COMPLETED   DELETION_IN_PROGRESS                           |
| targetSelection | Stringa | Specifica se l'esecuzione del processo continuerà (CONTINUOUS) o se il processo verrà completato dopo che tutti gli oggetti specificati come target avranno completato il processo |

| Nome           | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                              | (SNAPSHOT). Se è continuo, il processo può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un processo verrà eseguito in un oggetto quando l'oggetto viene aggiunto a un gruppo target, anche dopo che il processo è stato completato da tutti gli oggetti originariamente nel gruppo.<br><br>Enumerazione: CONTINUOUS   SNAPSHOT |
| maxResults     | intero<br><br>Intervallo – Max: 250, min.: 1                                 | Numero massimo di risultati da restituire per ogni richiesta.                                                                                                                                                                                                                                                                                                                      |
| nextToken      | Stringa                                                                      | Token usato per recuperare il successivo set di risultati.                                                                                                                                                                                                                                                                                                                         |
| thingGroupName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_]+ | Filtro che limita i processi restituiti a quelli per il gruppo specificato.                                                                                                                                                                                                                                                                                                        |
| thingGroupId   | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 -]+  | Filtro che limita i processi restituiti a quelli per il gruppo specificato.                                                                                                                                                                                                                                                                                                        |

## Output

```
{
 "jobs": [
 {
 "jobArn": "string",
 "jobId": "string",
 "thingGroupId": "string",
 "targetSelection": "string",
 "status": "string",
 "createdAt": "timestamp",
 "lastUpdatedAt": "timestamp",
 "completedAt": "timestamp"
 }
],
 "nextToken": "string"
}
```

## Campi di output dell'interfaccia a riga di comando

| Nome | Tipo   | Descrizione         |
|------|--------|---------------------|
| jobs | elenco | Elenco di processi. |

| Nome            | Tipo                                                                        | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | Membro: JobSummary<br><br>Classe Java: java.util.List                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| jobArn          | Stringa                                                                     | ARN del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| jobId           | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+  | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| thingGroupId    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 -]+ | ID del gruppo di oggetti.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| targetSelection | Stringa                                                                     | Specifica se l'esecuzione del processo continuerà (CONTINUOUS) o se il processo verrà completato dopo che tutti gli oggetti specificati come target avranno completato il processo (SNAPSHOT). Se è continuo, il processo può anche essere eseguito in un oggetto quando viene rilevata una modifica in un target. Ad esempio, un processo verrà eseguito in un oggetto quando l'oggetto viene aggiunto a un gruppo target, anche dopo che il processo è stato completato da tutti gli oggetti originariamente nel gruppo.<br><br>Enumerazione: CONTINUOUS   SNAPSHOT |
| status          | Stringa                                                                     | Stato di riepilogo del processo.<br><br>enum: IN_PROGRESS   CANCELED   COMPLETED   DELETION_IN_PROGRESS                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| createdAt       | Timestamp                                                                   | Periodo di tempo, in secondi, dall'epoca (Unix epoch) alla creazione del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| lastUpdatedAt   | timestamp                                                                   | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| completedAt     | timestamp                                                                   | Periodo di tempo, in secondi, dall'epoca al completamento del processo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Nome      | Tipo    | Descrizione                                                                               |
|-----------|---------|-------------------------------------------------------------------------------------------|
| nextToken | Stringa | Token per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ResourceNotFoundException

La risorsa specificata non esiste.

##### ThrottlingException

La velocità supera il limite.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

## ListOTAUpdates

Elenca gli aggiornamenti OTA.

#### Riepilogo

```
aws iot list-ota-updates \
[--max-results <value>] \
[--next-token <value>] \
[--ota-update-status <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "maxResults": "integer",
 "nextToken": "string",
 "otaUpdateStatus": "string"
}
```

#### Campi di cli-input-json

| Nome       | Tipo    | Descrizione                                                                            |
|------------|---------|----------------------------------------------------------------------------------------|
| maxResults | intero  | Numero massimo di risultati da restituire per volta.<br>Intervallo – Max: 250, min.: 1 |
| nextToken  | Stringa | Token usato per recuperare il successivo set di risultati.                             |

| Nome            | Tipo    | Descrizione                                                                                                                                                |
|-----------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| otaUpdateStatus | Stringa | <p>Stato del processo di aggiornamento OTA.</p> <p>Enumerazione:<br/>CREATE_PENDING  <br/>CREATE_IN_PROGRESS  <br/>CREATE_COMPLETE  <br/>CREATE_FAILED</p> |

#### Output

```
{
 "otaUpdates": [
 {
 "otaUpdateId": "string",
 "otaUpdateArn": "string",
 "creationDate": "timestamp"
 }
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome         | Tipo      | Descrizione                                                                        |
|--------------|-----------|------------------------------------------------------------------------------------|
| otaUpdates   | elenco    | Elenco di processi di aggiornamento OTA.<br>Membro: OTAUpdateSummary               |
| otaUpdateId  | Stringa   | ID aggiornamento OTA.<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+ |
| otaUpdateArn | Stringa   | ARN dell'aggiornamento OTA.                                                        |
| creationDate | timestamp | Data di creazione dell'aggiornamento OTA.                                          |
| nextToken    | Stringa   | Token da usare per ottenere il successivo set di risultati.                        |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### InternalFailureException

Si è verificato un errore imprevisto.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

## ListOutgoingCertificates

Elenca i certificati in fase di trasferimento ma non ancora accettati.

### Riepilogo

```
aws iot list-outgoing-certificates \
[--page-size <value>] \
[--marker <value>] \
[--ascending-order | --no-ascending-order] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "pageSize": "integer",
 "marker": "string",
 "ascendingOrder": "boolean"
}
```

### Campi di cli-input-json

| Nome           | Tipo     | Descrizione                                                                                                                           |
|----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| pageSize       | intero   | Dimensione della pagina dei risultati.<br>Intervallo – Max: 250, min.: 1                                                              |
| marker         | Stringa  | Contrassegno per il successivo set di risultati.<br>Modello: [A–Z a–z 0–9 +/]++={0,2}                                                 |
| ascendingOrder | booleano | Specifica l'ordine per i risultati.<br>Se è True, i risultati vengono restituiti in ordine crescente, in base alla data di creazione. |

### Output

```
{
 "outgoingCertificates": [
 {
 "certificateArn": "string",
 "certificateId": "string",
 "transferredTo": "string",
 "transferDate": "timestamp",
 "transferMessage": "string",
```

```

 "creationDate": "timestamp"
 }
],
"nextMarker": "string"
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome                 | Tipo                                                                   | Descrizione                                                   |
|----------------------|------------------------------------------------------------------------|---------------------------------------------------------------|
| outgoingCertificates | elenco<br>Membro: OutgoingCertificate<br>Classe Java: java.util.List   | Certificati in fase di trasferimento ma non ancora accettati. |
| certificateArn       | Stringa                                                                | ARN del certificato.                                          |
| certificateId        | Stringa<br>Lunghezza max: 64, min.: 64<br>Modello: (0x)?[a-f A-F 0-9]+ | ID certificato.                                               |
| transferredTo        | Stringa<br>Lunghezza max: 12, min.: 12<br>Modello: [0-9]+              | Account AWS in cui è stato eseguito il trasferimento.         |
| transferDate         | Timestamp                                                              | Data di avvio del trasferimento.                              |
| transferMessage      | Stringa<br>Lunghezza max: 128                                          | Messaggio di trasferimento.                                   |
| creationDate         | Timestamp                                                              | Data di creazione del certificato.                            |
| nextMarker           | Stringa<br>Modello: [A-Z a-z 0-9 +/]+={0,2}                            | Contrassegno per il successivo set di risultati.              |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

##### InternalFailureException

Si è verificato un errore imprevisto.

# ListPolicies

Elenca le policy.

Riepilogo

```
aws iot list-policies \
[--marker <value>] \
[--page-size <value>] \
[--ascending-order | --no-ascending-order] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "marker": "string",
 "pageSize": "integer",
 "ascendingOrder": "boolean"
}
```

Campi di **cli-input-json**

| Nome           | Tipo                                        | Descrizione                                                                                                     |
|----------------|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| marker         | Stringa<br>Modello: [A-Z a-z 0-9 +/]+={0,2} | Contrassegno per il successivo set di risultati.                                                                |
| pageSize       | intero<br>Intervallo – Max: 250, min.: 1    | Dimensione della pagina dei risultati.                                                                          |
| ascendingOrder | booleano                                    | Specifica l'ordine per i risultati. Se è true, i risultati vengono restituiti in ordine di creazione crescente. |

Output

```
{
 "policies": [
 {
 "policyName": "string",
 "policyArn": "string"
 }
],
 "nextMarker": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome     | Tipo                     | Descrizione               |
|----------|--------------------------|---------------------------|
| policies | elenco<br>Membro: Policy | Descrizioni delle policy. |

| Nome       | Tipo                                                                  | Descrizione                                                                                      |
|------------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
|            | Classe Java: java.util.List                                           |                                                                                                  |
| policyName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w+=,.@-]+ | Nome della policy.                                                                               |
| policyArn  | Stringa                                                               | ARN della policy.                                                                                |
| nextMarker | Stringa<br><br>Modello: [A-Z a-z 0-9 +/]+={0,2}                       | Contrassegno per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

##### InternalFailureException

Si è verificato un errore imprevisto.

## ListPolicyPrincipals

Elenca le entità principali associate alla policy specificata.

Nota: questa API è obsoleta. Usa invece ListTargetsForPolicy.

#### Riepilogo

```
aws iot list-policy-principals \
--policy-name <value> \
[--marker <value>] \
[--page-size <value>] \
[--ascending-order | --no-ascending-order] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "policyName": "string",
 "marker": "string",
 "pageSize": "integer",
 "ascendingOrder": "boolean"
}
```

### Campi di **cli-input-json**

| Nome           | Tipo                                                          | Descrizione                                                                                                     |
|----------------|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| policyName     | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [w+=,.@-]+ | Nome della policy.                                                                                              |
| marker         | Stringa<br>Modello: [A-Z a-z 0-9 +/]+={0,2}                   | Contrassegno per il successivo set di risultati.                                                                |
| pageSize       | intero<br>Intervallo – Max: 250, min.: 1                      | Dimensione della pagina dei risultati.                                                                          |
| ascendingOrder | booleano                                                      | Specifica l'ordine per i risultati. Se è true, i risultati vengono restituiti in ordine di creazione crescente. |

### Output

```
{
 "principals": [
 "string"
],
 "nextMarker": "string"
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome       | Tipo                                                          | Descrizione                                                                                      |
|------------|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| principals | elenco<br>Membro: PrincipalArn<br>Classe Java: java.util.List | Descrizioni delle entità principali.                                                             |
| nextMarker | Stringa<br>Modello: [A-Z a-z 0-9 +/]+={0,2}                   | Contrassegno per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

### Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## ListPolicyVersions

Elenca le versioni della policy specificata e identifica la versione predefinita.

### Riepilogo

```
aws iot list-policy-versions \
--policy-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "policyName": "string"
}
```

### Campi di cli-input-json

| Nome       | Tipo    | Descrizione                                                              |
|------------|---------|--------------------------------------------------------------------------|
| policyName | Stringa | Nome della policy.<br>Lunghezza max: 128, min.: 1<br>modello: [w+=, @-]+ |

### Output

```
{
 "policyVersions": [
 {
 "versionId": "string",
 "isDefaultVersion": "boolean",
 "createDate": "timestamp"
 }
]
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo   | Descrizione            |
|----------------|--------|------------------------|
| policyVersions | elenco | Versioni della policy. |

| Nome             | Tipo                                                 | Descrizione                                                 |
|------------------|------------------------------------------------------|-------------------------------------------------------------|
|                  | Membro: PolicyVersion<br>Classe Java: java.util.List |                                                             |
| versionId        | Stringa<br>Modello: [0-9]+                           | ID versione della policy.                                   |
| isDefaultVersion | booleano                                             | Specifica se la versione della policy è quella predefinita. |
| createDate       | timestamp                                            | Data e ora di creazione della policy.                       |

#### Errori

`ResourceNotFoundException`

La risorsa specificata non esiste.

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

`InternalFailureException`

Si è verificato un errore imprevisto.

## ListPrincipalPolicies

Elenca le policy collegate all'entità principale specificata. Se usi un'identità di Cognito, l'ID deve essere in formato di identità di Amazon Cognito.

Nota: questa API è obsoleta. Usa invece ListAttachedPolicies.

#### Riepilogo

```
aws iot list-principal-policies \
--principal <value> \
[--marker <value>] \
[--page-size <value>] \
[--ascending-order | --no-ascending-order] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "principal": "string",
 "marker": "string",
 "pageSize": "integer",
 "ascendingOrder": "boolean"
}
```

#### Campi di **cli-input-json**

| Nome           | Tipo     | Descrizione                                                                                                     |
|----------------|----------|-----------------------------------------------------------------------------------------------------------------|
| principal      | Stringa  | Entità principale.                                                                                              |
| marker         | Stringa  | Contrassegno per il successivo set di risultati.<br>Modello: [A-Z a-z 0-9 +/]{0,2}                              |
| pageSize       | intero   | Dimensione della pagina dei risultati.<br>Intervallo – Max: 250, min.: 1                                        |
| ascendingOrder | booleano | Specifica l'ordine per i risultati. Se è true, i risultati vengono restituiti in ordine di creazione crescente. |

#### Output

```
{
 "policies": [
 {
 "policyName": "string",
 "policyArn": "string"
 }
],
 "nextMarker": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome       | Tipo    | Descrizione                                                                                                                        |
|------------|---------|------------------------------------------------------------------------------------------------------------------------------------|
| policies   | elenco  | Policy.<br>Membro: Policy<br>Classe Java: java.util.List                                                                           |
| policyName | Stringa | Nome della policy.<br>Lunghezza max: 128, min.: 1<br>modello: [w+=,.@-]+                                                           |
| policyArn  | Stringa | ARN della policy.                                                                                                                  |
| nextMarker | Stringa | Contrassegno per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi.<br>Modello: [A-Z a-z 0-9 +/]{0,2} |

## Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## ListPrincipalThings

Elenca gli oggetti associati all'entità principale specificata. Un principale può essere certificati X.509, utenti IAM, gruppi e ruoli, identità Amazon Cognito o identità federate.

### Riepilogo

```
aws iot list-principal-things \
[--next-token <value>] \
[--max-results <value>] \
--principal <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "nextToken": "string",
 "maxResults": "integer",
 "principal": "string"
}
```

### Campi di **cli-input-json**

| Nome       | Tipo    | Descrizione                                                                                       |
|------------|---------|---------------------------------------------------------------------------------------------------|
| nextToken  | Stringa | Token usato per recuperare il successivo set di risultati.                                        |
| maxResults | intero  | Numero massimo di risultati da restituire in questa operazione.<br>Intervallo – Max: 250, min.: 1 |

| Nome      | Tipo    | Descrizione        |
|-----------|---------|--------------------|
| principal | Stringa | Entità principale. |

#### Output

```
{
 "things": [
 "string"
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome      | Tipo                        | Descrizione                                                                                              |
|-----------|-----------------------------|----------------------------------------------------------------------------------------------------------|
| things    | elenco<br>Membro: ThingName | Oggetti.                                                                                                 |
| nextToken | Stringa                     | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

##### InternalFailureException

Si è verificato un errore imprevisto.

##### ResourceNotFoundException

La risorsa specificata non esiste.

## ListRoleAliases

Elenca gli alias del ruolo registrati nell'account.

#### Riepilogo

```
aws iot list-role-aliases \
```

```
[--page-size <value>] \
[--marker <value>] \
[--ascending-order | --no-ascending-order] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "pageSize": "integer",
 "marker": "string",
 "ascendingOrder": "boolean"
}
```

Campi di **cli-input-json**

| Nome           | Tipo     | Descrizione                                                                                          |
|----------------|----------|------------------------------------------------------------------------------------------------------|
| pageSize       | intero   | Numero massimo di risultati da restituire per volta.<br>Intervallo – Max: 250, min.: 1               |
| marker         | Stringa  | Contrassegno usato per ottenere il successivo set di risultati.<br>Modello: [A–Z a–z 0–9 +/]++={0,2} |
| ascendingOrder | booleano | Restituisce l'elenco degli alias del ruolo in ordine alfabetico crescente.                           |

Output

```
{
 "roleAliases": [
 "string"
],
 "nextMarker": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome        | Tipo    | Descrizione                                                                                          |
|-------------|---------|------------------------------------------------------------------------------------------------------|
| roleAliases | elenco  | Alias del ruolo.<br>Membro: RoleAlias<br>Classe Java: java.util.List                                 |
| nextMarker  | Stringa | Contrassegno usato per ottenere il successivo set di risultati.<br>Modello: [A–Z a–z 0–9 +/]++={0,2} |

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

#### ThrottlingException

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## ListScheduledAudits

Elenca tutti gli audit pianificati.

### Riepilogo

```
aws iot list-scheduled-audits \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "nextToken": "string",
 "maxResults": "integer"
}
```

### Campi di cli-input-json

| Nome       | Tipo    | Descrizione                                                                      |
|------------|---------|----------------------------------------------------------------------------------|
| nextToken  | Stringa | Token per il set di risultati successivo.                                        |
| maxResults | intero  | Numero massimo di risultati da restituire per volta. Il valore predefinito è 25. |

### Output

```
{
 "scheduledAudits": [
 {
 "scheduledAuditName": "string",
 "scheduledAuditArn": "string",
 "frequency": "string",
 "dayOfMonth": "string",
 "dayOfWeek": "string"
```

```

 },
 "nextToken": "string"
 }
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome               | Tipo                                                                               | Descrizione                                                                                                                                                                                                         |
|--------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| scheduledAudits    | elenco<br><br>membro:<br>ScheduledAuditMetadata<br><br>Classe Java: java.util.List | Elenco di audit pianificati.                                                                                                                                                                                        |
| scheduledAuditName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+        | Nome dell'audit pianificato.                                                                                                                                                                                        |
| scheduledAuditArn  | Stringa                                                                            | ARN dell'audit pianificato.                                                                                                                                                                                         |
| frequenza          | Stringa                                                                            | Frequenza di esecuzione dell'audit.<br><br>enumerazione: DAILY   WEEKLY   BIWEEKLY   MONTHLY                                                                                                                        |
| dayOfMonth         | Stringa<br><br>modello: ^([1-9] [12][0-9] 3[01])\$ <br>^LAST\$                     | Giorno del mese in cui viene eseguito l'audit pianificato (se frequency è "MONTHLY"). Se vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese. |
| dayOfWeek          | Stringa                                                                            | Giorno della settimana in cui viene eseguito l'audit pianificato (se frequency è "WEEKLY" o "BIWEEKLY").<br><br>enumerazione: SUN   MON   TUE   WED   THU   FRI   SAT                                               |
| nextToken          | Stringa                                                                            | Token che è possibile usare per recuperare il set di risultati successivo oppure null se non ci sono risultati aggiuntivi.                                                                                          |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

#### InternalFailureException

Si è verificato un errore imprevisto.

## ListSecurityProfiles

Elenca i profili di sicurezza di Device Defender creati. Puoi usare i filtri per elencare solo i profili di sicurezza associati a un gruppo di oggetti oppure solo quelli associati all'account.

Riepilogo

```
aws iot list-security-profiles \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "nextToken": "string",
 "maxResults": "integer"
}
```

Campi di **cli-input-json**

| Nome       | Tipo    | Descrizione                                                                            |
|------------|---------|----------------------------------------------------------------------------------------|
| nextToken  | Stringa | Token per il set di risultati successivo.                                              |
| maxResults | intero  | Numero massimo di risultati da restituire per volta.<br>Intervallo – Max: 250, min.: 1 |

Output

```
{
 "securityProfileIdentifiers": [
 {
 "name": "string",
 "arn": "string"
 }
],
 "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome                       | Tipo                                                                       | Descrizione                                                     |
|----------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------|
| securityProfileIdentifiers | elenco<br>membro: SecurityProfileIdentifier<br>Classe Java: java.util.List | Elenco di identificatori dei profili di sicurezza (nomi e ARN). |

| Nome      | Tipo                                                                  | Descrizione                                                                                                                             |
|-----------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| name      | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+ | Nome assegnato al profilo di sicurezza.                                                                                                 |
| arn       | Stringa                                                               | ARN del profilo di sicurezza.                                                                                                           |
| nextToken | Stringa                                                               | Token che è possibile usare per recuperare il set di risultati successivo oppure <code>null</code> se non ci sono risultati aggiuntivi. |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

## ListSecurityProfilesForTarget

Elenca i profili di sicurezza di Device Defender collegati a un target (gruppo di oggetti).

#### Riepilogo

```
aws iot list-security-profiles-for-target \
[--next-token <value>] \
[--max-results <value>] \
[--recursive | --no-recursive] \
--security-profile-target-arn <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di `cli-input-json`

```
{
 "nextToken": "string",
 "maxResults": "integer",
 "recursive": "boolean",
 "securityProfileTargetArn": "string"
}
```

#### Campi di `cli-input-json`

| Nome      | Tipo    | Descrizione                               |
|-----------|---------|-------------------------------------------|
| nextToken | Stringa | Token per il set di risultati successivo. |

| Nome                     | Tipo                                     | Descrizione                                                                          |
|--------------------------|------------------------------------------|--------------------------------------------------------------------------------------|
| maxResults               | intero<br>Intervallo – Max: 250, min.: 1 | Numero massimo di risultati da restituire per volta.                                 |
| recursive                | booleano                                 | Se è true, restituisce anche i gruppi figlio.                                        |
| securityProfileTargetArn | Stringa                                  | ARN del target (gruppo di oggetti) di cui ottenere i profili di sicurezza collegati. |

#### Output

```
{
 "securityProfileTargetMappings": [
 {
 "securityProfileIdentifier": {
 "name": "string",
 "arn": "string"
 },
 "target": {
 "arn": "string"
 }
 },
 "nextToken": "string"
 }
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome                          | Tipo                                                                                 | Descrizione                                                                    |
|-------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| securityProfileTargetMappings | elenco<br>membro:<br>SecurityProfileTargetMapping<br><br>Classe Java: java.util.List | Elenco di profili di sicurezza e dei target associati.                         |
| securityProfileIdentifier     | SecurityProfileIdentifier                                                            | Informazioni che identificano il profilo di sicurezza.                         |
| name                          | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_]+         | Nome assegnato al profilo di sicurezza.                                        |
| arn                           | Stringa                                                                              | ARN del profilo di sicurezza.                                                  |
| target                        | SecurityProfileTarget                                                                | Informazioni sul target (gruppo di oggetti) associato al profilo di sicurezza. |
| arn                           | Stringa                                                                              | ARN del profilo di sicurezza.                                                  |
| nextToken                     | Stringa                                                                              | Token che è possibile usare per recuperare il set di risultati                 |

| Nome | Tipo | Descrizione                                                              |
|------|------|--------------------------------------------------------------------------|
|      |      | successivo oppure <code>null</code> se non ci sono risultati aggiuntivi. |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

## ListStreams

Elenca tutti i flussi nell'account AWS.

#### Riepilogo

```
aws iot list-streams \
[--max-results <value>] \
[--next-token <value>] \
[--ascending-order | --no-ascending-order] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di `cli-input-json`

```
{
 "maxResults": "integer",
 "nextToken": "string",
 "ascendingOrder": "boolean"
}
```

#### Campi di `cli-input-json`

| Nome                        | Tipo     | Descrizione                                                                             |
|-----------------------------|----------|-----------------------------------------------------------------------------------------|
| <code>maxResults</code>     | intero   | Numero massimo di risultati da restituire per volta.<br>Intervallo – Max: 250, min.: 1  |
| <code>nextToken</code>      | Stringa  | Token usato per ottenere il successivo set di risultati.                                |
| <code>ascendingOrder</code> | booleano | Imposta questo parametro su true per restituire l'elenco di flussi in ordine crescente. |

## Output

```
{
 "streams": [
 {
 "streamId": "string",
 "streamArn": "string",
 "streamVersion": "integer",
 "description": "string"
 }
],
 "nextToken": "string"
}
```

## Campi di output dell'interfaccia a riga di comando

| Nome          | Tipo                                                                 | Descrizione                                              |
|---------------|----------------------------------------------------------------------|----------------------------------------------------------|
| streams       | elenco<br>Membro: StreamSummary                                      | Elenco di flussi.                                        |
| streamId      | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 _-]+ | ID flusso.                                               |
| streamArn     | Stringa                                                              | ARN del flusso.                                          |
| streamVersion | intero<br>Intervallo – Max: 65535, min.: 0                           | Versione del flusso.                                     |
| description   | Stringa<br>Lunghezza max: 2028<br>Modello: [^\p{C}]+                 | Descrizione del flusso.                                  |
| nextToken     | Stringa                                                              | Token usato per ottenere il successivo set di risultati. |

## Errori

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ThrottlingException

La velocità supera il limite.

### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

### InternalFailureException

Si è verificato un errore imprevisto.

# ListTagsForResource

Elenca i tag (metadati) che hai assegnato alla risorsa.

Riepilogo

```
aws iot list-tags-for-resource \
--resource-arn <value> \
[--next-token <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "resourceArn": "string",
 "nextToken": "string"
}
```

Campi di **cli-input-json**

| Nome        | Tipo    | Descrizione                                                |
|-------------|---------|------------------------------------------------------------|
| resourceArn | Stringa | L'ARN della risorsa.                                       |
| nextToken   | Stringa | Token usato per recuperare il successivo set di risultati. |

Output

```
{
 "tags": [
 {
 "Key": "string",
 "Value": "string"
 }
],
 "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome      | Tipo                                                     | Descrizione                                                    |
|-----------|----------------------------------------------------------|----------------------------------------------------------------|
| tags      | elenco<br>member: Tag<br><br>Classe Java: java.util.List | L'elenco dei tag assegnato alla risorsa.                       |
| Chiave    | Stringa                                                  | La chiave del tag.                                             |
| Valore    | Stringa                                                  | Il valore del tag.                                             |
| nextToken | Stringa                                                  | Token usato per ottenere il successivo set di risultati oppure |

| Nome | Tipo | Descrizione                               |
|------|------|-------------------------------------------|
|      |      | null se non ci sono risultati aggiuntivi. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### InternalFailureException

Si è verificato un errore imprevisto.

##### ResourceNotFoundException

La risorsa specificata non esiste.

##### ThrottlingException

La velocità supera il limite.

## ListTargetsForPolicy

Elenca i target per la policy specificata.

#### Riepilogo

```
aws iot list-targets-for-policy \
--policy-name <value> \
[--marker <value>] \
[--page-size <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "policyName": "string",
 "marker": "string",
 "pageSize": "integer"
}
```

#### Campi di cli-input-json

| Nome       | Tipo    | Descrizione                                                                                              |
|------------|---------|----------------------------------------------------------------------------------------------------------|
| policyName | Stringa | Nome della policy.<br><br>Lunghezza max: 128, min.: 1<br><br>modello: [w+=,.@-]+                         |
| marker     | Stringa | Contrassegno usato per ottenere il successivo set di risultati.<br><br>Modello: [A-Z a-z 0-9 +/]++={0,2} |

| Nome     | Tipo                                     | Descrizione                                          |
|----------|------------------------------------------|------------------------------------------------------|
| pageSize | intero<br>Intervallo – Max: 250, min.: 1 | Numero massimo di risultati da restituire per volta. |

#### Output

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

#### Campi di output dell'interfaccia a riga di comando

| Nome       | Tipo                                                          | Descrizione                                                     |
|------------|---------------------------------------------------------------|-----------------------------------------------------------------|
| targets    | elenco<br>Membro: PolicyTarget<br>Classe Java: java.util.List | Target della policy.                                            |
| nextMarker | Stringa<br>Modello: [A–Z a–z 0–9 +/]+={0,2}                   | Contrassegno usato per ottenere il successivo set di risultati. |

#### Errori

##### ResourceNotFoundException

La risorsa specificata non esiste.

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

##### InternalFailureException

Si è verificato un errore imprevisto.

##### LimitExceededException

È stato superato un limite.

## ListTargetsForSecurityProfile

Elenca i target (gruppi di oggetti) associati a un determinato profilo di sicurezza di Device Defender.

## Riepilogo

```
aws iot list-targets-for-security-profile \
--security-profile-name <value> \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "securityProfileName": "string",
 "nextToken": "string",
 "maxResults": "integer"
}
```

## Campi di cli-input-json

| Nome                | Tipo                                                                          | Descrizione                                          |
|---------------------|-------------------------------------------------------------------------------|------------------------------------------------------|
| securityProfileName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Profilo di sicurezza.                                |
| nextToken           | Stringa                                                                       | Token per il set di risultati successivo.            |
| maxResults          | intero<br><br>Intervallo – Max: 250, min.: 1                                  | Numero massimo di risultati da restituire per volta. |

## Output

```
{
 "securityProfileTargets": [
 {
 "arn": "string"
 }
],
 "nextToken": "string"
}
```

## Campi di output dell'interfaccia a riga di comando

| Nome                   | Tipo                                                                           | Descrizione                                                    |
|------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------------|
| securityProfileTargets | elenco<br><br>membro: SecurityProfileTarget<br><br>Classe Java: java.util.List | Gruppi di oggetti a cui è collegato il profilo di sicurezza.   |
| arn                    | Stringa                                                                        | ARN del profilo di sicurezza.                                  |
| nextToken              | Stringa                                                                        | Token che è possibile usare per recuperare il set di risultati |

| Nome | Tipo | Descrizione                                                              |
|------|------|--------------------------------------------------------------------------|
|      |      | successivo oppure <code>null</code> se non ci sono risultati aggiuntivi. |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

## ListThingGroups

Elenca i gruppi di oggetti nell'account.

#### Riepilogo

```
aws iot list-thing-groups \
[--next-token <value>] \
[--max-results <value>] \
[--parent-group <value>] \
[--name-prefix-filter <value>] \
[--recursive | --no-recursive] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di `cli-input-json`

```
{
 "nextToken": "string",
 "maxResults": "integer",
 "parentGroup": "string",
 "namePrefixFilter": "string",
 "recursive": "boolean"
}
```

#### Campi di `cli-input-json`

| Nome                    | Tipo    | Descrizione                                                |
|-------------------------|---------|------------------------------------------------------------|
| <code>nextToken</code>  | Stringa | Token usato per recuperare il successivo set di risultati. |
| <code>maxResults</code> | intero  | Numero massimo di risultati da restituire per volta.       |

| Nome             | Tipo                                                                  | Descrizione                                                                 |
|------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------|
|                  | Intervallo – Max: 250, min.: 1                                        |                                                                             |
| parentGroup      | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+ | Filtro che limita i risultati a quelli con il gruppo padre specificato.     |
| namePrefixFilter | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+ | Filtro che limita i risultati a quelli con il prefisso di nome specificato. |
| recursive        | booleano                                                              | Se è true, restituisce anche i gruppi figlio.                               |

#### Output

```
{
 "thingGroups": [
 {
 "groupName": "string",
 "groupArn": "string"
 }
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome        | Tipo                                                                  | Descrizione                                                                                              |
|-------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| thingGroups | elenco<br>Membro: GroupNameAndArn<br>Classe Java: java.util.List      | Gruppi di oggetti.                                                                                       |
| groupName   | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+ | Nome del gruppo.                                                                                         |
| groupArn    | Stringa                                                               | ARN del gruppo.                                                                                          |
| nextToken   | Stringa                                                               | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

#### InternalFailureException

Si è verificato un errore imprevisto.

#### ResourceNotFoundException

La risorsa specificata non esiste.

## ListThingGroupsForThing

Elenca i gruppi di oggetti cui appartiene l'oggetto specificato.

### Riepilogo

```
aws iot list-thing-groups-for-thing \
--thing-name <value> \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "thingName": "string",
 "nextToken": "string",
 "maxResults": "integer"
}
```

### Campi di **cli-input-json**

| Nome       | Tipo    | Descrizione                                                                                |
|------------|---------|--------------------------------------------------------------------------------------------|
| thingName  | Stringa | Nome dell'oggetto.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_]+    |
| nextToken  | Stringa | Token usato per recuperare il successivo set di risultati.                                 |
| maxResults | intero  | Numero massimo di risultati da restituire per volta.<br><br>Intervallo – Max: 250, min.: 1 |

### Output

```
{
 "thingGroups": [
 {
 "groupName": "string",
 "groupArn": "string"
 }
],
 "nextToken": "string"
```

}

Campi di output dell'interfaccia a riga di comando

| Nome        | Tipo                                                                       | Descrizione                                                                                              |
|-------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| thingGroups | elenco<br><br>Membro: GroupNameAndArn<br><br>Classe Java: java.util.List   | Gruppi di oggetti.                                                                                       |
| groupName   | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z0-9:_-]+ | Nome del gruppo.                                                                                         |
| groupArn    | Stringa                                                                    | ARN del gruppo.                                                                                          |
| nextToken   | Stringa                                                                    | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ResourceNotFoundException**

La risorsa specificata non esiste.

## ListThingPrincipals

Elenca le entità principali associate all'oggetto specificato. Un principale può essere certificati X.509, utenti IAM, gruppi e ruoli, identità Amazon Cognito o identità federate.

Riepilogo

```
aws iot list-thing-principals \
--thing-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "thingName": "string"
}
```

### Campi di **cli-input-json**

| Nome      | Tipo                                                                          | Descrizione        |
|-----------|-------------------------------------------------------------------------------|--------------------|
| thingName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto. |

### Output

```
{
 " principals": [
 "string"
]
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome       | Tipo                                                                  | Descrizione                              |
|------------|-----------------------------------------------------------------------|------------------------------------------|
| principals | elenco<br><br>Membro: PrincipalArn<br><br>Classe Java: java.util.List | Entità principali associate all'oggetto. |

### Errori

#### `InvalidRequestException`

I contenuti della richiesta non sono validi.

#### `ThrottlingException`

La velocità supera il limite.

#### `UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

#### `InternalFailureException`

Si è verificato un errore imprevisto.

#### `ResourceNotFoundException`

La risorsa specificata non esiste.

## ListThingRegistrationTaskReports

Informazioni sulle attività di registrazione di oggetti.

### Riepilogo

```
aws iot list-thing-registration-task-reports \
--task-id <value> \
--report-type <value> \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "taskId": "string",
 "reportType": "string",
 "nextToken": "string",
 "maxResults": "integer"
}
```

Campi di **cli-input-json**

| Nome       | Tipo                                     | Descrizione                                                     |
|------------|------------------------------------------|-----------------------------------------------------------------|
| taskId     | Stringa<br>Lunghezza max: 40             | ID dell'attività.                                               |
| reportType | Stringa                                  | Tipo di report dell'attività.<br>Enumerazione: ERRORS   RESULTS |
| nextToken  | Stringa                                  | Token usato per recuperare il successivo set di risultati.      |
| maxResults | intero<br>Intervallo – Max: 250, min.: 1 | Numero massimo di risultati da restituire per ogni richiesta.   |

Output

```
{
 "resourceLinks": [
 "string"
],
 "reportType": "string",
 "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome          | Tipo                        | Descrizione                                                     |
|---------------|-----------------------------|-----------------------------------------------------------------|
| resourceLinks | elenco<br>Membro: S3FileUrl | Collegamenti alle risorse dell'attività.                        |
| reportType    | Stringa                     | Tipo di report dell'attività.<br>Enumerazione: ERRORS   RESULTS |

| Nome      | Tipo    | Descrizione                                                                                              |
|-----------|---------|----------------------------------------------------------------------------------------------------------|
| nextToken | Stringa | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**InternalFailureException**

Si è verificato un errore imprevisto.

## ListThingRegistrationTasks

Elenca le attività di provisioning in blocco di oggetti.

#### Riepilogo

```
aws iot list-thing-registration-tasks \
[--next-token <value>] \
[--max-results <value>] \
[--status <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "nextToken": "string",
 "maxResults": "integer",
 "status": "string"
}
```

#### Campi di cli-input-json

| Nome       | Tipo    | Descrizione                                                                            |
|------------|---------|----------------------------------------------------------------------------------------|
| nextToken  | Stringa | Token usato per recuperare il successivo set di risultati.                             |
| maxResults | intero  | Numero massimo di risultati da restituire per volta.<br>Intervallo – Max: 250, min.: 1 |

| Nome  | Tipo    | Descrizione                                                                                                                             |
|-------|---------|-----------------------------------------------------------------------------------------------------------------------------------------|
| stato | Stringa | Stato dell'attività di provisioning in blocco di oggetti.<br><br>Enumerazione: InProgress   Completed   Failed   Cancelled   Cancelling |

#### Output

```
{
 "taskIds": [
 "string"
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome      | Tipo                     | Descrizione                                                                                              |
|-----------|--------------------------|----------------------------------------------------------------------------------------------------------|
| taskIds   | elenco<br>Membro: TaskId | Elenco di ID attività di provisioning in blocco di oggetti.                                              |
| nextToken | Stringa                  | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### InternalFailureException

Si è verificato un errore imprevisto.

## ListThingTypes

Elenca i tipi di oggetto esistenti.

#### Riepilogo

```
aws iot list-thing-types \
```

```
[--next-token <value>] \
[--max-results <value>] \
[--thing-type-name <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "nextToken": "string",
 "maxResults": "integer",
 "thingTypeName": "string"
}
```

Campi di **cli-input-json**

| Nome          | Tipo    | Descrizione                                                                                       |
|---------------|---------|---------------------------------------------------------------------------------------------------|
| nextToken     | Stringa | Token usato per recuperare il successivo set di risultati.                                        |
| maxResults    | intero  | Numero massimo di risultati da restituire in questa operazione.<br>Intervallo – Max: 250, min.: 1 |
| thingTypeName | Stringa | Nome del tipo di oggetto.<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+           |

Output

```
{
 "thingTypes": [
 {
 "thingTypeName": "string",
 "thingTypeArn": "string",
 "thingTypeProperties": {
 "thingTypeDescription": "string",
 "searchableAttributes": [
 "string"
]
 },
 "thingTypeMetadata": {
 "deprecated": "boolean",
 "deprecationDate": "timestamp",
 "creationDate": "timestamp"
 }
 }
],
 "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome       | Tipo   | Descrizione      |
|------------|--------|------------------|
| thingTypes | elenco | Tipi di oggetto. |

| Nome                 | Tipo                                                                         | Descrizione                                                                                                                                                                                                    |
|----------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | Membro: ThingTypeDefinition<br><br>Classe Java: java.util.List               |                                                                                                                                                                                                                |
| thingTypeName        | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_]+ | Nome del tipo di oggetto.                                                                                                                                                                                      |
| thingTypeArn         | Stringa                                                                      | ARN del tipo di oggetto.                                                                                                                                                                                       |
| thingTypeProperties  | ThingTypeProperties                                                          | ThingTypeProperties per il tipo di oggetto.                                                                                                                                                                    |
| thingTypeDescription | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [\p{Graph}]*              | Descrizione del tipo di oggetto.                                                                                                                                                                               |
| searchableAttributes | elenco<br><br>Membro: AttributeName<br><br>Classe Java: java.util.List       | Elenco di nomi di attributi dell'oggetto che è possibile cercare.                                                                                                                                              |
| thingTypeMetadata    | ThingTypeMetadata                                                            | ThingTypeMetadata contiene informazioni aggiuntive sul tipo di oggetto, tra cui data e ora di creazione, un valore indicante se il tipo di oggetto è obsoleto e data e ora in cui è stato dichiarato obsoleto. |
| deprecated           | booleano                                                                     | Specifica se il tipo di oggetto è obsoleto. Se è true, a questo tipo non possono essere associati nuovi oggetti.                                                                                               |
| deprecationDate      | Timestamp                                                                    | Data e ora in cui il tipo di oggetto è stato dichiarato obsoleto.                                                                                                                                              |
| creationDate         | Timestamp                                                                    | Data e ora di creazione del tipo di oggetto.                                                                                                                                                                   |
| nextToken            | Stringa                                                                      | Token per il successivo set di risultati oppure null se non ci sono risultati aggiuntivi.                                                                                                                      |

## Errori

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ThrottlingException

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## ListThings

Elenca gli oggetti. Usa i parametri attributeName e attributeValue per filtrare gli oggetti. Ad esempio, chiamando `ListThings` con attributeName =Color e attributeValue=Red, potrai recuperare tutti gli oggetti presenti nel registro che contengono un attributo Color con il valore Red.

### Riepilogo

```
aws iot list-things \
[--next-token <value>] \
[--max-results <value>] \
[--attribute-name <value>] \
[--attribute-value <value>] \
[--thing-type-name <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di `cli-input-json`

```
{
 "nextToken": "string",
 "maxResults": "integer",
 "attributeName": "string",
 "attributeValue": "string",
 "thingTypeName": "string"
}
```

### Campi di `cli-input-json`

| Nome           | Tipo                                                                      | Descrizione                                                                                       |
|----------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| nextToken      | Stringa                                                                   | Token usato per recuperare il successivo set di risultati.                                        |
| maxResults     | intero                                                                    | Numero massimo di risultati da restituire in questa operazione.<br>Intervallo – Max: 250, min.: 1 |
| attributeName  | Stringa<br><br>Lunghezza max: 128<br><br>Modello: [a-z A-Z 0-9 _.,@/:#-]+ | Nome di attributo usato per cercare oggetti.                                                      |
| attributeValue | Stringa                                                                   | Valore di attributo usato per cercare oggetti.                                                    |

| Nome          | Tipo                                                                  | Descrizione                                         |
|---------------|-----------------------------------------------------------------------|-----------------------------------------------------|
|               | Lunghezza max: 800<br>Modello: [a-z A-Z 0-9 _.,@/:#-]*                |                                                     |
| thingTypeName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del tipo di oggetto usato per cercare oggetti. |

#### Output

```
{
 "things": [
 {
 "thingName": "string",
 "thingTypeArn": "string",
 "thingArn": "string",
 "attributes": {
 "string": "string"
 },
 "version": "long"
 }
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome         | Tipo                                                                  | Descrizione                                                         |
|--------------|-----------------------------------------------------------------------|---------------------------------------------------------------------|
| things       | elenco<br>Membro: ThingAttribute<br>Classe Java: java.util.List       | Oggetti.                                                            |
| thingName    | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto.                                                  |
| thingTypeArn | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del tipo di oggetto, se l'oggetto è stato associato a un tipo. |
| version      | Long                                                                  | Versione del record dell'oggetto nel registro.                      |
| nextToken    | Stringa                                                               | Token usato per ottenere il successivo set di risultati oppure      |

| Nome | Tipo | Descrizione                               |
|------|------|-------------------------------------------|
|      |      | null se non ci sono risultati aggiuntivi. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ThrottlingException

La velocità supera il limite.

##### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

##### InternalFailureException

Si è verificato un errore imprevisto.

## ListThingsInBillingGroup

Elenca gli oggetti che hai aggiunto al gruppo di fatturazione specificato.

#### Riepilogo

```
aws iot list-things-in-billing-group \
--billing-group-name <value> \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "billingGroupName": "string",
 "nextToken": "string",
 "maxResults": "integer"
}
```

#### Campi di cli-input-json

| Nome             | Tipo    | Descrizione                                                                                      |
|------------------|---------|--------------------------------------------------------------------------------------------------|
| billingGroupName | Stringa | Il nome del gruppo di fatturazione.<br>Lunghezza max: 128, min.: 1<br>Modello: [a-zA-Z 0-9 :_-]+ |
| nextToken        | Stringa | Token usato per recuperare il successivo set di risultati.                                       |

| Nome       | Tipo                                     | Descrizione                                                   |
|------------|------------------------------------------|---------------------------------------------------------------|
| maxResults | intero<br>Intervallo – Max: 250, min.: 1 | Numero massimo di risultati da restituire per ogni richiesta. |

#### Output

```
{
 "things": [
 "string"
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome      | Tipo                        | Descrizione                                                                                              |
|-----------|-----------------------------|----------------------------------------------------------------------------------------------------------|
| things    | elenco<br>Membro: ThingName | Un elenco di oggetti nel gruppo di fatturazione.                                                         |
| nextToken | Stringa                     | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### InternalFailureException

Si è verificato un errore imprevisto.

##### ResourceNotFoundException

La risorsa specificata non esiste.

##### ThrottlingException

La velocità supera il limite.

## ListThingsInThingGroup

Elenca gli oggetti nel gruppo specificato.

#### Riepilogo

```
aws iot list-things-in-thing-group \
--thing-group-name <value> \
[--recursive | --no-recursive] \
[--next-token <value>] \
```

```
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "thingGroupName": "string",
 "recursive": "boolean",
 "nextToken": "string",
 "maxResults": "integer"
}
```

#### Campi di cli-input-json

| Nome           | Tipo                                                                          | Descrizione                                                                                 |
|----------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| thingGroupName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome del gruppo di oggetti.                                                                 |
| recursive      | booleano                                                                      | Se è true, elenca gli oggetti in questo gruppo di oggetti e anche in tutti i gruppi figlio. |
| nextToken      | Stringa                                                                       | Token usato per recuperare il successivo set di risultati.                                  |
| maxResults     | intero<br><br>Intervallo – Max: 250, min.: 1                                  | Numero massimo di risultati da restituire per volta.                                        |

#### Output

```
{
 "things": [
 "string"
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome      | Tipo                            | Descrizione                                                                                              |
|-----------|---------------------------------|----------------------------------------------------------------------------------------------------------|
| things    | elenco<br><br>Membro: ThingName | Oggetti nel gruppo di oggetti specificato.                                                               |
| nextToken | Stringa                         | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### InternalFailureException

Si è verificato un errore imprevisto.

#### ResourceNotFoundException

La risorsa specificata non esiste.

## ListTopicRules

Elenca le regole per l'argomento specifico.

### Riepilogo

```
aws iot list-topic-rules \
[--topic <value>] \
[--max-results <value>] \
[--next-token <value>] \
[--rule-disabled | --no-rule-disabled] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "topic": "string",
 "maxResults": "integer",
 "nextToken": "string",
 "ruleDisabled": "boolean"
}
```

### Campi di cli-input-json

| Nome         | Tipo     | Descrizione                                                                    |
|--------------|----------|--------------------------------------------------------------------------------|
| argomento    | Stringa  | Argomento.                                                                     |
| maxResults   | intero   | Numero massimo di risultati da restituire.<br>Intervallo – Max: 10000, min.: 1 |
| nextToken    | Stringa  | Token usato per recuperare il valore successivo.                               |
| ruleDisabled | booleano | Specifica se la regola è disabilitata.                                         |

### Output

```
{
 "rules": [
 {
 "ruleArn": "string",
 "ruleName": "string",
 "topicPattern": "string",
```

```

 "createdAt": "timestamp",
 "ruleDisabled": "boolean"
}
],
"nextToken": "string"
}

```

Campi di output dell'interfaccia a riga di comando

| Nome         | Tipo                      | Descrizione                                                                               |
|--------------|---------------------------|-------------------------------------------------------------------------------------------|
| rules        | elenco                    | Regole.                                                                                   |
|              | Membro: TopicRuleListItem |                                                                                           |
| ruleArn      | Stringa                   | ARN della regola.                                                                         |
| ruleName     | Stringa                   | Nome della regola.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: ^[a-z A-Z 0-9 _]+\$ |
| topicPattern | Stringa                   | Modello per i nomi di argomento validi.                                                   |
| createdAt    | Timestamp                 | Data e ora di creazione della regola.                                                     |
| ruleDisabled | booleano                  | Specifica se la regola è disabilitata.                                                    |
| nextToken    | Stringa                   | Token usato per recuperare il valore successivo.                                          |

Errori

**InternalException**

Si è verificato un errore imprevisto.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

## ListV2LoggingLevels

Elenca i livelli di logging.

Riepilogo

```

aws iot list-v2-logging-levels \
[--target-type <value>] \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \

```

[--generate-cli-skeleton]

#### Formato di cli-input-json

```
{
 "targetType": "string",
 "nextToken": "string",
 "maxResults": "integer"
}
```

#### Campi di cli-input-json

| Nome       | Tipo                                         | Descrizione                                                                                                               |
|------------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| targetType | Stringa                                      | Tipo di risorsa per cui stai configurando il logging. Deve essere THING_Group.<br><br>Enumerazione: DEFAULT   THING_GROUP |
| nextToken  | Stringa                                      | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi.                  |
| maxResults | intero<br><br>Intervallo – Max: 250, min.: 1 | Numero massimo di risultati da restituire per volta.                                                                      |

#### Output

```
{
 "logTargetConfigurations": [
 {
 "logTarget": {
 "targetType": "string",
 "targetName": "string"
 },
 "logLevel": "string"
 }
],
 "nextToken": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome                    | Tipo                                         | Descrizione                                                         |
|-------------------------|----------------------------------------------|---------------------------------------------------------------------|
| logTargetConfigurations | elenco<br><br>Membro: LogTargetConfiguration | Configurazione di logging per un target.                            |
| logTarget               | LogTarget                                    | Target di log.                                                      |
| targetType              | Stringa                                      | Il tipo di destinazione.<br><br>Enumerazione: DEFAULT   THING_GROUP |

| Nome       | Tipo    | Descrizione                                                                                              |
|------------|---------|----------------------------------------------------------------------------------------------------------|
| targetName | Stringa | Nome del target.                                                                                         |
| logLevel   | Stringa | Livello di logging.<br>Enumerazione: DEBUG   INFO   ERROR   WARN   DISABLED                              |
| nextToken  | Stringa | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |

#### Errori

##### **InternalException**

Si è verificato un errore imprevisto.

##### **NotConfiguredException**

La risorsa non è configurata.

##### **InvalidRequestException**

I contenuti della richiesta non sono validi.

##### **ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

## ListViolationEvents

Elenca le violazioni dei profili di sicurezza di Device Defender rilevate durante il periodo di tempo specificato. Puoi usare i filtri per limitare i risultati solo agli avvisi creati per un determinato profilo di sicurezza, comportamento o oggetto (dispositivo).

#### Riepilogo

```
aws iot list-violation-events \
--start-time <value> \
--end-time <value> \
[--thing-name <value>] \
[--security-profile-name <value>] \
[--next-token <value>] \
[--max-results <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "startTime": "timestamp",
 "endTime": "timestamp",
 "thingName": "string",
 "securityProfileName": "string",
```

```

 "nextToken": "string",
 "maxResults": "integer"
}

```

#### Campi di **cli-input-json**

| Nome                | Tipo                                                                  | Descrizione                                                                              |
|---------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| startTime           | timestamp                                                             | Ora di inizio degli avvisi da elencare.                                                  |
| endTime             | timestamp                                                             | Ora di fine degli avvisi da elencare.                                                    |
| thingName           | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Filtro che limita i risultati agli avvisi causati dall'oggetto specificato.              |
| securityProfileName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Filtro che limita i risultati agli avvisi generati dal profilo di sicurezza specificato. |
| nextToken           | Stringa                                                               | Token per il set di risultati successivo.                                                |
| maxResults          | intero<br>Intervallo – Max: 250, min.: 1                              | Numero massimo di risultati da restituire per volta.                                     |

#### Output

```
{
 "violationEvents": [
 {
 "violationId": "string",
 "thingName": "string",
 "securityProfileName": "string",
 "behavior": {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 }
 },
 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "statistic": "string"
 }
 }
 }
]
}
```

```

},
"metricValue": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
},
"violationEventType": "string",
"violationEventTime": "timestamp"
}
],
"nextToken": "string"
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome                | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                            |
|---------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| violationEvents     | elenco<br>membro: ViolationEvent                                             | Avvisi di violazione dei profili di sicurezza creati per l'account durante l'intervallo di tempo specificato, che possono essere filtrati in base a profilo di sicurezza, comportamento violato o oggetto (dispositivo) responsabile della violazione. |
| violationId         | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :-]+ | ID dell'evento di violazione.                                                                                                                                                                                                                          |
| thingName           | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :-]+ | Nome dell'oggetto responsabile dell'evento di violazione.                                                                                                                                                                                              |
| securityProfileName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :-]+ | Nome del profilo di sicurezza il cui comportamento è stato violato.                                                                                                                                                                                    |
| behavior            | Behavior                                                                     | Comportamento che è stato violato.                                                                                                                                                                                                                     |
| name                | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :-]+ | Nome assegnato al comportamento.                                                                                                                                                                                                                       |
| metric              | Stringa                                                                      | Valore misurato dal comportamento.                                                                                                                                                                                                                     |
| criteria            | BehaviorCriteria                                                             | Criteri che determinano se un dispositivo presenta un                                                                                                                                                                                                  |

| Nome               | Tipo                             | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    |                                  | comportamento normale in relazione a <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| comparisonOperator | Stringa                          | Operatore che mette in correlazione l'oggetto misurato ( <code>metric</code> ) e i criteri (contenenti un <code>value</code> o <code>statisticalThreshold</code> ).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set                                                                                                                                                                                                                                                            |
| value              | MetricValue                      | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count              | Long<br><br>Intervallo - min.: 0 | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cidrs              | elenco<br><br>membro: Cidr       | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports              | elenco<br><br>membro: Port       | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds    | intero                           | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |

| Nome                         | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| consecutiveDatapointsToAlarm | intero<br><br>Intervallo – Max: 10, min.: 1                                  | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| consecutiveDatapointsToClear | intero<br><br>Intervallo – Max: 10, min.: 1                                  | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| statisticalThreshold         | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistic                    | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato ( <code>durationSeconds</code> ) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto ( <code>comparisonOperator</code> ) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario si verifica una violazione. |
| metricValue                  | MetricValue                                                                  | Valore del parametro (misurazione).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| count                        | Long<br><br>Intervallo - min.: 0                                             | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Nome               | Tipo                   | Descrizione                                                                                                                                       |
|--------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| cids               | elenco<br>membro: Cidr | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .  |
| ports              | elenco<br>membro: Port | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> . |
| violationEventType | Stringa                | Tipo di evento di violazione.<br>enumerazione: in-alarm   alarm-cleared   alarm-invalidated                                                       |
| violationEventTime | timestamp              | Ora in cui si è verificato l'evento di violazione.                                                                                                |
| nextToken          | Stringa                | Token che è possibile usare per recuperare il set di risultati successivo oppure <code>null</code> se non ci sono risultati aggiuntivi.           |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

## Publish

Pubblica le informazioni sullo stato.

Per ulteriori informazioni, consulta la pagina relativa al [protocollo HTTP](#) nella Guida per lo sviluppatore di AWS IoT.

#### Riepilogo

```
aws iot-data publish \
[--topic <value>] \
[--qos <value>] \
[--payload <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "topic": "string",
 "qos": "integer",
 "payload": "blob"
}
```

#### Campi di **cli-input-json**

| Nome      | Tipo    | Descrizione                                                      |
|-----------|---------|------------------------------------------------------------------|
| argomento | Stringa | Nome dell'argomento MQTT.                                        |
| qos       | intero  | Livello di qualità del servizio.<br>Intervallo – Max: 1, min.: 0 |
| payload   | blob    | Informazioni sullo stato, in formato JSON.                       |

#### Output

Nessuna

#### Errori

**InternalFailureException**

Si è verificato un errore imprevisto.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**MethodNotAllowedException**

La combinazione specificata di verbo HTTP e URI non è supportata.

## RegisterCACertificate

Registra un certificato CA con AWS IoT. Questo certificato CA può quindi essere usato per firmare certificati dei dispositivi, che possono essere registrati con AWS IoT. Puoi registrare fino a dieci certificati CA per ogni account AWS con lo stesso campo dell'oggetto. In questo modo, potrai avere fino a 10 autorità di certificazione per firmare i certificati dei dispositivi. Se hai più di un certificato CA registrato, assicurati di passare il certificato CA quando registri i certificati dei dispositivi con l'API RegisterCertificate.

#### Riepilogo

```
aws iot register-ca-certificate \
 --ca-certificate <value> \
 --verification-certificate <value> \
 [--set-as-active | --no-set-as-active] \
 [--allow-auto-registration | --no-allow-auto-registration] \
 [--registration-config <value>] \

```

```
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di **cli-input-json**

```
{
 "caCertificate": "string",
 "verificationCertificate": "string",
 "setAsActive": "boolean",
 "allowAutoRegistration": "boolean",
 "registrationConfig": {
 "templateBody": "string",
 "roleArn": "string"
 }
}
```

#### Campi di **cli-input-json**

| Nome                    | Tipo               | Descrizione                                                                                              |
|-------------------------|--------------------|----------------------------------------------------------------------------------------------------------|
| caCertificate           | Stringa            | Certificato CA.<br><br>Lunghezza max: 65536, min.: 1                                                     |
| verificationCertificate | Stringa            | Certificato di verifica della chiave privata.<br><br>Lunghezza max: 65536, min.: 1                       |
| setAsActive             | booleano           | Valore booleano che specifica se il certificato CA è impostato come attivo.                              |
| allowAutoRegistration   | booleano           | Permette l'uso di questo certificato CA per la registrazione automatica dei certificati dei dispositivi. |
| registrationConfig      | RegistrationConfig | Informazioni sulla configurazione della registrazione.                                                   |
| templateBody            | Stringa            | Corpo del modello.                                                                                       |
| roleArn                 | Stringa            | ARN del ruolo.<br><br>Lunghezza max: 2048, min.: 20                                                      |

#### Output

```
{
 "certificateArn": "string",
 "certificateId": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo    | Descrizione             |
|----------------|---------|-------------------------|
| certificateArn | Stringa | ARN del certificato CA. |

| Nome          | Tipo                                                                   | Descrizione                        |
|---------------|------------------------------------------------------------------------|------------------------------------|
| certificateId | Stringa<br>Lunghezza max: 64, min.: 64<br>Modello: (0x)?[a-f A-F 0-9]+ | Identificatore del certificato CA. |

#### Errori

**ResourceAlreadyExistsException**

La risorsa esiste già.

**RegistrationCodeValidationException**

Il codice di registrazione non è valido.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**CertificateValidationException**

Il certificato non è valido.

**ThrottlingException**

La velocità supera il limite.

**LimitExceededException**

È stato superato un limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## RegisterCertificate

Registra un certificato del dispositivo con AWS IoT. Se esistono più certificati CA con lo stesso campo dell'oggetto, devi specificare il certificato CA usato per firmare il certificato del dispositivo.

#### Riepilogo

```
aws iot register-certificate \
--certificate-pem <value> \
[--ca-certificate-pem <value>] \
[--set-as-active | --no-set-as-active] \
[--status <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "certificatePem": "string",
```

```
{
 "caCertificatePem": "string",
 "status": "string"
}
```

#### Campi di **cli-input-json**

| Nome             | Tipo                                     | Descrizione                                                                                                                                                          |
|------------------|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| certificatePem   | Stringa<br>Lunghezza max: 65536, min.: 1 | Dati del certificato, in formato PEM.                                                                                                                                |
| caCertificatePem | Stringa<br>Lunghezza max: 65536, min.: 1 | Certificato CA usato per firmare il certificato del dispositivo registrato.                                                                                          |
| status           | Stringa                                  | Stato della richiesta di registrazione del certificato.<br><br>Enumerazione: ACTIVE   INACTIVE   REVOKED   PENDING_TRANSFER   REGISTER_INACTIVE   PENDING_ACTIVATION |

#### Output

```
{
 "certificateArn": "string",
 "certificateId": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo                                                                   | Descrizione                     |
|----------------|------------------------------------------------------------------------|---------------------------------|
| certificateArn | Stringa                                                                | ARN del certificato.            |
| certificateId  | Stringa<br>Lunghezza max: 64, min.: 64<br>Modello: (0x)?[a-f A-F 0-9]+ | Identificatore del certificato. |

#### Errori

**ResourceAlreadyExistsException**

La risorsa esiste già.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**CertificateValidationException**

Il certificato non è valido.

**CertificateStateException**

L'operazione del certificato non è consentita.

#### CertificateConflictException

Non è possibile verificare il certificato CA usato per firmare il certificato del dispositivo che stai tentando di registrare. Questo problema si verifica quando hai registrato più di un certificato CA che ha lo stesso campo dell'oggetto e la stessa chiave pubblica.

#### ThrottlingException

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## RegisterThing

Effettua il provisioning di un oggetto.

### Riepilogo

```
aws iot register-thing \
 --template-body <value> \
 [--parameters <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "templateBody": "string",
 "parameters": {
 "string": "string"
 }
}
```

### Campi di cli-input-json

| Nome         | Tipo    | Descrizione                                                                                                                              |
|--------------|---------|------------------------------------------------------------------------------------------------------------------------------------------|
| templateBody | Stringa | Modello di provisioning. Per ulteriori informazioni, consulta la pagina <a href="#">Provisioning programmatico</a> .                     |
| parameters   | mappa   | Parametri per il provisioning di un oggetto. Per ulteriori informazioni, consulta la pagina <a href="#">Provisioning programmatico</a> . |

### Output

```
{
 "certificatePem": "string",
```

```

 "resourceArns": {
 "string": "string"
 }
}

```

Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo    | Descrizione                   |
|----------------|---------|-------------------------------|
| certificatePem | Stringa | .                             |
|                |         | Lunghezza max: 65536, min.: 1 |
| resourceArns   | mappa   | ARN per le risorse generate.  |

Errori

**InternalFailureException**

Si è verificato un errore imprevisto.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ThrottlingException**

La velocità supera il limite.

**ConflictingResourceUpdateException**

Eccezione relativa ad aggiornamenti in conflitto della risorsa. Questa eccezione viene generata quando due aggiornamenti in sospeso causano un conflitto.

**ResourceRegistrationFailureException**

La registrazione della risorsa non è riuscita.

## RejectCertificateTransfer

Rifiuta un trasferimento in sospeso del certificato. Dopo che AWS IoT rifiuta un trasferimento del certificato, lo stato del certificato passa da PENDING\_TRANSFER a INACTIVE.

Per verificare i trasferimenti di certificati in sospeso, chiama ListCertificates per enumerare i certificati.

Questa operazione può essere chiamata solo dalla destinazione del trasferimento. Dopo la chiamata, il certificato viene restituito all'account dell'origine con stato INACTIVE.

Riepilogo

```

aws iot reject-certificate-transfer \
--certificate-id <value> \
[--reject-reason <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]

```

Formato di **cli-input-json**

```
{
 "certificateId": "string",
 "rejectReason": "string"
}
```

Campi di **cli-input-json**

| Nome          | Tipo                                                                   | Descrizione                                                                            |
|---------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| certificateId | Stringa<br>Lunghezza max: 64, min.: 64<br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato. L'ultima parte dell'ARN del certificato contiene l'ID certificato. |
| rejectReason  | Stringa<br>Lunghezza max: 128                                          | Motivo per cui il trasferimento del certificato è stato rifiutato.                     |

Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**TransferAlreadyCompletedException**

Non puoi annullare il trasferimento del certificato perché è già stato completato.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## RemoveThingFromBillingGroup

Rimuove l'oggetto specificato dal gruppo di fatturazione.

Riepilogo

```
aws iot remove-thing-from-billing-group \
[--billing-group-name <value>] \
```

```
[--billing-group-arn <value>] \
[--thing-name <value>] \
[--thing-arn <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "billingGroupName": "string",
 "billingGroupArn": "string",
 "thingName": "string",
 "thingArn": "string"
}
```

Campi di **cli-input-json**

| Nome             | Tipo    | Descrizione                                                                                                                 |
|------------------|---------|-----------------------------------------------------------------------------------------------------------------------------|
| billingGroupName | Stringa | Il nome del gruppo di fatturazione.<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+                           |
| billingGroupArn  | Stringa | L'ARN del gruppo di fatturazione.                                                                                           |
| thingName        | Stringa | Il nome dell'oggetto da rimuovere dal gruppo di fatturazione.<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ |
| thingArn         | Stringa | L'ARN dell'oggetto da rimuovere dal gruppo di fatturazione.                                                                 |

Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ResourceNotFoundException**

La risorsa specificata non esiste.

## RemoveThingFromThingGroup

Rimuove l'oggetto specificato dal gruppo specificato.

## Riepilogo

```
aws iot remove-thing-from-thing-group \
[--thing-group-name <value>] \
[--thing-group-arn <value>] \
[--thing-name <value>] \
[--thing-arn <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "thingGroupName": "string",
 "thingGroupArn": "string",
 "thingName": "string",
 "thingArn": "string"
}
```

## Campi di cli-input-json

| Nome           | Tipo    | Descrizione                                                                                                      |
|----------------|---------|------------------------------------------------------------------------------------------------------------------|
| thingGroupName | Stringa | Nome del gruppo.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+                           |
| thingGroupArn  | Stringa | ARN del gruppo.                                                                                                  |
| thingName      | Stringa | Nome dell'oggetto da rimuovere dal gruppo.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ |
| thingArn       | Stringa | ARN dell'oggetto da rimuovere dal gruppo.                                                                        |

## Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ResourceNotFoundException**

La risorsa specificata non esiste.

# ReplaceTopicRule

Sostituisce la regola. Devi specificare tutti i parametri per la nuova regola. La creazione di regole è un'operazione a livello di amministratore. Qualsiasi utente che ha l'autorizzazione necessaria per creare regole potrà accedere ai dati elaborati dalla regola.

## Riepilogo

```
aws iot replace-topic-rule \
--rule-name <value> \
--topic-rule-payload <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "ruleName": "string",
 "topicRulePayload": {
 "sql": "string",
 "description": "string",
 "actions": [
 {
 "dynamoDB": {
 "tableName": "string",
 "roleArn": "string",
 "operation": "string",
 "hashKeyField": "string",
 "hashKeyValue": "string",
 "hashKeyType": "string",
 "rangeKeyField": "string",
 "rangeKeyValue": "string",
 "rangeKeyType": "string",
 "payloadField": "string"
 },
 "dynamoDBv2": {
 "roleArn": "string",
 "putItem": {
 "tableName": "string"
 }
 },
 "lambda": {
 "functionArn": "string"
 },
 "sns": {
 "targetArn": "string",
 "roleArn": "string",
 "messageFormat": "string"
 },
 "sqs": {
 "roleArn": "string",
 "queueUrl": "string",
 "useBase64": "boolean"
 },
 "kinesis": {
 "roleArn": "string",
 "streamName": "string",
 "partitionKey": "string"
 },
 "republish": {
 "roleArn": "string",
 "topic": "string"
 }
 }
]
 }
}
```

```
 },
 "s3": {
 "roleArn": "string",
 "bucketName": "string",
 "key": "string",
 "cannedAcl": "string"
 },
 "firehose": {
 "roleArn": "string",
 "deliveryStreamName": "string",
 "separator": "string"
 },
 "cloudwatchMetric": {
 "roleArn": "string",
 "metricNamespace": "string",
 "metricName": "string",
 "metricValue": "string",
 "metricUnit": "string",
 "metricTimestamp": "string"
 },
 "cloudwatchAlarm": {
 "roleArn": "string",
 "alarmName": "string",
 "stateReason": "string",
 "stateValue": "string"
 },
 "elasticsearch": {
 "roleArn": "string",
 "endpoint": "string",
 "index": "string",
 "type": "string",
 "id": "string"
 },
 "salesforce": {
 "token": "string",
 "url": "string"
 },
 "iotAnalytics": {
 "channelArn": "string",
 "channelName": "string",
 "roleArn": "string"
 },
 "iotEvents": {
 "inputName": "string",
 "messageId": "string",
 "roleArn": "string"
 },
 "stepFunctions": {
 "executionNamePrefix": "string",
 "stateMachineName": "string",
 "roleArn": "string"
 }
 }
},
"ruleDisabled": "boolean",
"awsIotSqlVersion": "string",
"errorAction": {
 "dynamodb": {
 "tableName": "string",
 "roleArn": "string",
 "operation": "string",
 "hashKeyField": "string",
 "hashKeyValue": "string",
 "hashKeyType": "string",
 "rangeKeyField": "string",
 "rangeKeyValue": "string"
 }
}
],
```

```
 "rangeKeyType": "string",
 "payloadField": "string"
 },
 "dynamoDBv2": {
 "roleArn": "string",
 "putItem": {
 "tableName": "string"
 }
 },
 "lambda": {
 "functionArn": "string"
 },
 "sns": {
 "targetArn": "string",
 "roleArn": "string",
 "messageFormat": "string"
 },
 "sqs": {
 "roleArn": "string",
 "queueUrl": "string",
 "useBase64": "boolean"
 },
 "kinesis": {
 "roleArn": "string",
 "streamName": "string",
 "partitionKey": "string"
 },
 "republish": {
 "roleArn": "string",
 "topic": "string"
 },
 "s3": {
 "roleArn": "string",
 "bucketName": "string",
 "key": "string",
 "cannedAcl": "string"
 },
 "firehose": {
 "roleArn": "string",
 "deliveryStreamName": "string",
 "separator": "string"
 },
 "cloudwatchMetric": {
 "roleArn": "string",
 "metricNamespace": "string",
 "metricName": "string",
 "metricValue": "string",
 "metricUnit": "string",
 "metricTimestamp": "string"
 },
 "cloudwatchAlarm": {
 "roleArn": "string",
 "alarmName": "string",
 "stateReason": "string",
 "stateValue": "string"
 },
 "elasticsearch": {
 "roleArn": "string",
 "endpoint": "string",
 "index": "string",
 "type": "string",
 "id": "string"
 },
 "salesforce": {
 "token": "string",
 "url": "string"
 }
```

```
 },
 "iotAnalytics": {
 "channelArn": "string",
 "channelName": "string",
 "roleArn": "string"
 },
 "iotEvents": {
 "inputName": "string",
 "messageId": "string",
 "roleArn": "string"
 },
 "stepFunctions": {
 "executionNamePrefix": "string",
 "stateMachineName": "string",
 "roleArn": "string"
 }
 }
}
```

#### Campi di **cli-input-json**

| Nome             | Tipo                                                                   | Descrizione                                                                                                                                                                                          |
|------------------|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ruleName         | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: ^[a-z A-Z 0-9 _]+\$ | Nome della regola.                                                                                                                                                                                   |
| topicRulePayload | TopicRulePayload                                                       | Payload della regola.                                                                                                                                                                                |
| sql              | Stringa                                                                | Istruzione SQL usata per eseguire query sull'argomento. Per ulteriori informazioni, consulta le <a href="#">informazioni di riferimento su SQL per AWS IoT</a> nella Guida per sviluppatori AWS IoT. |
| description      | Stringa                                                                | Descrizione della regola.                                                                                                                                                                            |
| actions          | elenco<br>Membro: Action                                               | Operazioni associate alla regola.                                                                                                                                                                    |
| dynamoDB         | DynamoDBAction                                                         | Scrive in una tabella DynamoDB.                                                                                                                                                                      |
| tableName        | Stringa                                                                | Nome della tabella DynamoDB.                                                                                                                                                                         |
| roleArn          | Stringa                                                                | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                       |
| operation        | Stringa                                                                | Tipo di operazione da eseguire. Segue il modello di sostituzione, per cui può essere \$ <b>operation</b> , ma la sostituzione deve restituire uno dei risultati seguenti: INSERT, UPDATE o DELETE.   |
| hashKeyField     | Stringa                                                                | Nome della chiave hash.                                                                                                                                                                              |

| Nome          | Tipo             | Descrizione                                                                                                                                                                                                                                                                                                        |
|---------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hashKeyValue  | Stringa          | Valore della chiave hash.                                                                                                                                                                                                                                                                                          |
| hashKeyType   | Stringa          | Tipo di chiave hash. I valori validi sono "STRING" e "NUMBER"<br><br>Enumerazione: STRING   NUMBER                                                                                                                                                                                                                 |
| rangeKeyField | Stringa          | Nome della chiave di intervallo.                                                                                                                                                                                                                                                                                   |
| rangeKeyValue | Stringa          | Valore della chiave di intervallo.                                                                                                                                                                                                                                                                                 |
| rangeKeyType  | Stringa          | Tipo di chiave di intervallo. I valori validi sono "STRING" e "NUMBER"<br><br>Enumerazione: STRING   NUMBER                                                                                                                                                                                                        |
| payloadField  | Stringa          | Payload dell'operazione. Questo nome può essere personalizzato.                                                                                                                                                                                                                                                    |
| dynamoDBv2    | DynamoDBv2Action | Scrive in una tabella DynamoDB. Questa è una nuova versione dell'operazione DynamoDB. Permette di scrivere ogni attributo incluso nel payload di un messaggio MQTT in una colonna DynamoDB separata.                                                                                                               |
| roleArn       | Stringa          | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                                                                                                                                     |
| putItem       | PutItemInput     | Specifica la tabella DynamoDB in cui verranno scritti i dati del messaggio. Ad esempio:<br><br><pre>{ "dynamoDBv2": { "roleArn": "aws:iam:12341251:my-role" "putItem": { "tableName": "my-table" } } }</pre> Ogni attributo nel payload del messaggio verrà scritto in una colonna separata del database DynamoDB. |
| tableName     | Stringa          | Tabella in cui verranno scritti i dati del messaggio.                                                                                                                                                                                                                                                              |
| lambda        | LambdaAction     | Richiama una funzione Lambda.                                                                                                                                                                                                                                                                                      |
| functionArn   | Stringa          | ARN della funzione Lambda.                                                                                                                                                                                                                                                                                         |
| sns           | SnsAction        | Pubblica in un argomento Amazon SNS.                                                                                                                                                                                                                                                                               |

| Nome          | Tipo            | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| targetArn     | Stringa         | ARN dell'argomento SNS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| messageFormat | Stringa         | (Opzionale) Formato del messaggio da pubblicare. I valori accettati sono "JSON" e "RAW". Il valore predefinito dell'attributo è "RAW". SNS usa questa impostazione per determinare se il payload deve essere analizzato e se devono essere estratti i bit specifici della piattaforma rilevanti del payload. Per ulteriori informazioni sui formati di messaggio SNS, consulta la pagina <a href="https://docs.aws.amazon.com/sns/latest/dg/json-formats.html">https://docs.aws.amazon.com/sns/latest/dg/json-formats.html</a> e fai riferimento alla documentazione ufficiale.<br><br>Enumerazione: RAW   JSON |
| sqs           | SqsAction       | Pubblica in una coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| queueUrl      | Stringa         | URL della coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| useBase64     | booleano        | Specifica se usare la codifica Base64.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| kinesis       | KinesisAction   | Scrive i dati in un flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso al flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| streamName    | Stringa         | Nome del flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| partitionKey  | Stringa         | Chiave di partizione.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| republish     | RepublishAction | Pubblica in un altro argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| roleArn       | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| argomento     | Stringa         | Nome dell'argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| s3            | S3Action        | Scrive in un bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Nome               | Tipo                               | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn            | Stringa                            | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                         |
| bucketName         | Stringa                            | Bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| key                | Stringa                            | Chiave dell'oggetto.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| cannedAcl          | Stringa                            | <p>Lista di controllo degli accessi predefinita Amazon S3 che controlla l'accesso all'oggetto identificato dalla chiave dell'oggetto. Per ulteriori informazioni, consulta la pagina relativa alle <a href="#">liste di controllo degli accessi predefinite S3</a>.</p> <p>Enumerazione: private   public-read   public-read-write   aws-exec-read   authenticated-read   bucket-owner-read   bucket-owner-full-control   log-delivery-write</p> |
| firehose           | FirehoseAction                     | Scrive in un flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                                                     |
| roleArn            | Stringa                            | Ruolo IAM che concede l'accesso al flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                               |
| deliveryStreamName | Stringa                            | Nome del flusso di distribuzione.                                                                                                                                                                                                                                                                                                                                                                                                                |
| separator          | Stringa<br>Modello: ([ ]) (  ) (.) | Separatore di caratteri che verrà usato per separare i record scritti nel flusso Firehose. I valori validi sono: '\n' (nuova riga), '\t' (tabulazione), '\r\n' (nuova riga Windows), ',' (virgola).                                                                                                                                                                                                                                              |
| cloudwatchMetric   | CloudwatchMetricAction             | Acquisisce un parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                              |
| roleArn            | Stringa                            | Ruolo IAM che permette l'accesso al parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                        |
| metricNamespace    | Stringa                            | Namespace dei nomi del parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                     |
| metricName         | Stringa                            | Nome parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| metricValue        | Stringa                            | Valore del parametro CloudWatch.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| metricUnit         | Stringa                            | <a href="#">Unità di misura del parametro supportata da CloudWatch</a> .                                                                                                                                                                                                                                                                                                                                                                         |
| metricTimestamp    | Stringa                            | Uno <a href="#">Timestamp Unix</a> opzionale.                                                                                                                                                                                                                                                                                                                                                                                                    |

| Nome            | Tipo                                                                                                                                                                       | Descrizione                                                                                                                                                                         |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cloudwatchAlarm | CloudwatchAlarmAction                                                                                                                                                      | Modifica lo stato di un allarme CloudWatch.                                                                                                                                         |
| roleArn         | Stringa                                                                                                                                                                    | Ruolo IAM che permette l'accesso all'allarme CloudWatch.                                                                                                                            |
| alarmName       | Stringa                                                                                                                                                                    | Nome dell'allarme CloudWatch.                                                                                                                                                       |
| stateReason     | Stringa                                                                                                                                                                    | Motivo della modifica dell'allarme.                                                                                                                                                 |
| stateValue      | Stringa                                                                                                                                                                    | Valore dello stato dell'allarme. I valori accettabili sono: OK, ALARM, INSUFFICIENT_DATA.                                                                                           |
| elasticsearch   | ElasticsearchAction                                                                                                                                                        | Scrive dati in un dominio Amazon Elasticsearch Service.                                                                                                                             |
| roleArn         | Stringa                                                                                                                                                                    | ARN del ruolo IAM che ha accesso a Elasticsearch.                                                                                                                                   |
| endpoint        | Stringa<br>modello: https?://.*                                                                                                                                            | Endpoint del dominio Elasticsearch.                                                                                                                                                 |
| index           | Stringa                                                                                                                                                                    | Indice Elasticsearch in cui vuoi archiviare i dati.                                                                                                                                 |
| type            | Stringa                                                                                                                                                                    | Tipo di documento che stai archiviando.                                                                                                                                             |
| id              | Stringa                                                                                                                                                                    | Identificatore univoco per il documento che stai archiviando.                                                                                                                       |
| salesforce      | SalesforceAction                                                                                                                                                           | Invia un messaggio a un flusso di input Salesforce IoT Cloud.                                                                                                                       |
| token           | Stringa<br>Lunghezza min.: 40                                                                                                                                              | Token usato per autenticare l'accesso al flusso di input Salesforce IoT Cloud. Il token è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input. |
| url             | Stringa<br>Lunghezza max: 2000<br>modello: https://ingestion-[a-zA-Z0-9]{1,12}.[a-zA-Z0-9]+.((sfdc-matrix.net) (sfdcnow.com))/streams/w <b>1,20</b> /w <b>1,20</b> /evento | URL esposto dal flusso di input Salesforce IoT Cloud. L'URL è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input.                             |
| iotAnalytics    | iotAnalyticsAction                                                                                                                                                         | Invia i dati del messaggio a un canale AWS IoT Analytics.                                                                                                                           |
| channelArn      | Stringa                                                                                                                                                                    | (obsoleto) L'ARN del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                               |

| Nome                | Tipo                                       | Descrizione                                                                                                                                                                                                                                             |
|---------------------|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| channelName         | Stringa                                    | Il nome del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                                                                                                            |
| roleArn             | Stringa                                    | L'ARN del ruolo con una policy che concede a IoT Analytics l'autorizzazione per l'invio di dati di messaggi tramite IoT Analytics (iotanalytics:BatchPutMessage).                                                                                       |
| iotEvents           | IoTEventsAction                            | Invia un input a un rilevatore AWS IoT Events.                                                                                                                                                                                                          |
| inputName           | Stringa<br><br>Lunghezza max: 128, min.: 1 | Il nome dell'input AWS IoT Events.                                                                                                                                                                                                                      |
| messageId           | Stringa<br><br>Lunghezza max: 128          | [Opzionale] Da utilizzare per essere certi che il rilevatore AWS IoT Events elaborerà solo un messaggio di input con un determinato messageId.                                                                                                          |
| roleArn             | Stringa                                    | L'ARN del ruolo che concede l'autorizzazione AWS IoT per inviare un messaggio di input a un rilevatore AWS IoT Events. ("Action":"iotevents:BatchPutMessage").                                                                                          |
| stepFunctions       | StepFunctionsAction                        | Avvia l'esecuzione di una macchina a stati Step Functions.                                                                                                                                                                                              |
| executionNamePrefix | Stringa                                    | (Opzionale) All'esecuzione della macchina a stati verrà assegnato un nome costituito da questo prefisso seguito da un UUID. Step Functions crea automaticamente un nome univoco per ogni esecuzione della macchina a stati se non ne viene fornito uno. |
| stateMachineName    | Stringa                                    | Il nome della macchina a stati Step Functions di cui verrà avviata l'esecuzione.                                                                                                                                                                        |
| roleArn             | Stringa                                    | L'ARN del ruolo che concede a IoT l'autorizzazione per avviare l'esecuzione di una macchina a stati ("Action":"states:StartExecution").                                                                                                                 |
| ruleDisabled        | booleano                                   | Specifica se la regola è disabilitata.                                                                                                                                                                                                                  |

| Nome             | Tipo             | Descrizione                                                                                                                                                                                                                                       |
|------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| awsIotSqlVersion | Stringa          | Versione del motore di regole SQL da usare durante la valutazione della regola.                                                                                                                                                                   |
| errorAction      | Action           | Operazione da eseguire quando si verifica un errore.                                                                                                                                                                                              |
| dynamoDB         | DynamoDBAction   | Scrive in una tabella DynamoDB.                                                                                                                                                                                                                   |
| tableName        | Stringa          | Nome della tabella DynamoDB.                                                                                                                                                                                                                      |
| roleArn          | Stringa          | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                                                                    |
| operation        | Stringa          | Tipo di operazione da eseguire. Segue il modello di sostituzione, per cui può essere <code>\$ operation</code> , ma la sostituzione deve restituire uno dei risultati seguenti: <code>INSERT</code> , <code>UPDATE</code> o <code>DELETE</code> . |
| hashKeyField     | Stringa          | Nome della chiave hash.                                                                                                                                                                                                                           |
| hashKeyValue     | Stringa          | Valore della chiave hash.                                                                                                                                                                                                                         |
| hashKeyType      | Stringa          | Tipo di chiave hash. I valori validi sono "STRING" e "NUMBER"<br><br>Enumerazione: STRING   NUMBER                                                                                                                                                |
| rangeKeyField    | Stringa          | Nome della chiave di intervallo.                                                                                                                                                                                                                  |
| rangeKeyValue    | Stringa          | Valore della chiave di intervallo.                                                                                                                                                                                                                |
| rangeKeyType     | Stringa          | Tipo di chiave di intervallo. I valori validi sono "STRING" e "NUMBER"<br><br>Enumerazione: STRING   NUMBER                                                                                                                                       |
| payloadField     | Stringa          | Payload dell'operazione. Questo nome può essere personalizzato.                                                                                                                                                                                   |
| dynamoDBv2       | DynamoDBv2Action | Scrive in una tabella DynamoDB. Questa è una nuova versione dell'operazione DynamoDB. Permette di scrivere ogni attributo incluso nel payload di un messaggio MQTT in una colonna DynamoDB separata.                                              |
| roleArn          | Stringa          | ARN del ruolo IAM che concede l'accesso alla tabella DynamoDB.                                                                                                                                                                                    |

| Nome          | Tipo         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| putItem       | PutItemInput | <p>Specifica la tabella DynamoDB in cui verranno scritti i dati del messaggio. Ad esempio:</p> <pre>{ "dynamoDBv2": { "roleArn": "aws:iam:12341251:my-role" "putItem": { "tableName": "my-table" } } }</pre> <p>Ogni attributo nel payload del messaggio verrà scritto in una colonna separata del database DynamoDB.</p>                                                                                                                                                                                                                                                                                              |
| tableName     | Stringa      | Tabella in cui verranno scritti i dati del messaggio.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| lambda        | LambdaAction | Richiama una funzione Lambda.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| functionArn   | Stringa      | ARN della funzione Lambda.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| sns           | SnsAction    | Pubblica in un argomento Amazon SNS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| targetArn     | Stringa      | ARN dell'argomento SNS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| roleArn       | Stringa      | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| messageFormat | Stringa      | <p>(Opzionale) Formato del messaggio da pubblicare. I valori accettati sono "JSON" e "RAW". Il valore predefinito dell'attributo è "RAW". SNS usa questa impostazione per determinare se il payload deve essere analizzato e se devono essere estratti i bit specifici della piattaforma rilevanti del payload. Per ulteriori informazioni sui formati di messaggio SNS, consulta la pagina <a href="https://docs.aws.amazon.com/sns/latest/dg/json-formats.html">https://docs.aws.amazon.com/sns/latest/dg/json-formats.html</a> e fai riferimento alla documentazione ufficiale.</p> <p>Enumerazione: RAW   JSON</p> |
| sqs           | SqsAction    | Pubblica in una coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| roleArn       | Stringa      | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Nome               | Tipo            | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| queueUrl           | Stringa         | URL della coda Amazon SQS.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| useBase64          | booleano        | Specifica se usare la codifica Base64.                                                                                                                                                                                                                                                                                                                                                                                                           |
| kinesis            | KinesisAction   | Scrive i dati in un flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                       |
| roleArn            | Stringa         | ARN del ruolo IAM che concede l'accesso al flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                |
| streamName         | Stringa         | Nome del flusso Amazon Kinesis.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| partitionKey       | Stringa         | Chiave di partizione.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| republish          | RepublishAction | Pubblica in un altro argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                             |
| roleArn            | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                         |
| argomento          | Stringa         | Nome dell'argomento MQTT.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| s3                 | S3Action        | Scrive in un bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| roleArn            | Stringa         | ARN del ruolo IAM che concede l'accesso.                                                                                                                                                                                                                                                                                                                                                                                                         |
| bucketName         | Stringa         | Bucket Amazon S3.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| key                | Stringa         | Chiave dell'oggetto.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| cannedAcl          | Stringa         | <p>Lista di controllo degli accessi predefinita Amazon S3 che controlla l'accesso all'oggetto identificato dalla chiave dell'oggetto. Per ulteriori informazioni, consulta la pagina relativa alle <a href="#">liste di controllo degli accessi predefinite S3</a>.</p> <p>Enumerazione: private   public-read   public-read-write   aws-exec-read   authenticated-read   bucket-owner-read   bucket-owner-full-control   log-delivery-write</p> |
| firehose           | FirehoseAction  | Scrive in un flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                                                     |
| roleArn            | Stringa         | Ruolo IAM che concede l'accesso al flusso Amazon Kinesis Firehose.                                                                                                                                                                                                                                                                                                                                                                               |
| deliveryStreamName | Stringa         | Nome del flusso di distribuzione.                                                                                                                                                                                                                                                                                                                                                                                                                |

| Nome             | Tipo                               | Descrizione                                                                                                                                                                                         |
|------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| separator        | Stringa<br>Modello: ([ ] (  ) (),) | Separatore di caratteri che verrà usato per separare i record scritti nel flusso Firehose. I valori validi sono: '\n' (nuova riga), '\t' (tabulazione), '\r\n' (nuova riga Windows), ',' (virgola). |
| cloudwatchMetric | CloudwatchMetricAction             | Acquisisce un parametro CloudWatch.                                                                                                                                                                 |
| roleArn          | Stringa                            | Ruolo IAM che permette l'accesso al parametro CloudWatch.                                                                                                                                           |
| metricNamespace  | Stringa                            | Namespace dei nomi del parametro CloudWatch.                                                                                                                                                        |
| metricName       | Stringa                            | Nome parametro CloudWatch.                                                                                                                                                                          |
| metricValue      | Stringa                            | Valore del parametro CloudWatch.                                                                                                                                                                    |
| metricUnit       | Stringa                            | <a href="#">Unità di misura del parametro supportata da CloudWatch</a> .                                                                                                                            |
| metricTimestamp  | Stringa                            | Uno <a href="#">Timestamp Unix</a> opzionale.                                                                                                                                                       |
| cloudwatchAlarm  | CloudwatchAlarmAction              | Modifica lo stato di un allarme CloudWatch.                                                                                                                                                         |
| roleArn          | Stringa                            | Ruolo IAM che permette l'accesso all'allarme CloudWatch.                                                                                                                                            |
| alarmName        | Stringa                            | Nome dell'allarme CloudWatch.                                                                                                                                                                       |
| stateReason      | Stringa                            | Motivo della modifica dell'allarme.                                                                                                                                                                 |
| stateValue       | Stringa                            | Valore dello stato dell'allarme. I valori accettabili sono: OK, ALARM, INSUFFICIENT_DATA.                                                                                                           |
| elasticsearch    | ElasticsearchAction                | Scrive dati in un dominio Amazon Elasticsearch Service.                                                                                                                                             |
| roleArn          | Stringa                            | ARN del ruolo IAM che ha accesso a Elasticsearch.                                                                                                                                                   |
| endpoint         | Stringa<br>modello: https?://.*    | Endpoint del dominio Elasticsearch.                                                                                                                                                                 |
| index            | Stringa                            | Indice Elasticsearch in cui vuoi archiviare i dati.                                                                                                                                                 |
| type             | Stringa                            | Tipo di documento che stai archiviando.                                                                                                                                                             |
| id               | Stringa                            | Identificatore univoco per il documento che stai archiviando.                                                                                                                                       |

| Nome         | Tipo                                                                                                                                                                                           | Descrizione                                                                                                                                                                         |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| salesforce   | SalesforceAction                                                                                                                                                                               | Invia un messaggio a un flusso di input Salesforce IoT Cloud.                                                                                                                       |
| token        | Stringa<br>Lunghezza min.: 40                                                                                                                                                                  | Token usato per autenticare l'accesso al flusso di input Salesforce IoT Cloud. Il token è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input. |
| url          | Stringa<br>Lunghezza max: 2000<br>modello: https://ingestion-[a-zA-Z0-9]{1,12}.[a-zA-Z0-9]+.((sfdc-matrix.net) (sfdcnow.com))/streams/w <a href="#">1, 20</a> /w <a href="#">1, 20</a> /evento | URL esposto dal flusso di input Salesforce IoT Cloud. L'URL è disponibile dalla piattaforma Salesforce IoT Cloud dopo la creazione del flusso di input.                             |
| iotAnalytics | IotAnalyticsAction                                                                                                                                                                             | Invia i dati del messaggio a un canale AWS IoT Analytics.                                                                                                                           |
| channelArn   | Stringa                                                                                                                                                                                        | (obsoleto) L'ARN del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                               |
| channelName  | Stringa                                                                                                                                                                                        | Il nome del canale IoT Analytics a cui saranno inviati i dati del messaggio.                                                                                                        |
| roleArn      | Stringa                                                                                                                                                                                        | L'ARN del ruolo con una policy che concede a IoT Analytics l'autorizzazione per l'invio di dati di messaggi tramite IoT Analytics (iotanalytics:BatchPutMessage).                   |
| iotEvents    | IotEventsAction                                                                                                                                                                                | Invia un input a un rilevatore AWS IoT Events.                                                                                                                                      |
| inputName    | Stringa<br>Lunghezza max: 128, min.: 1                                                                                                                                                         | Il nome dell'input AWS IoT Events.                                                                                                                                                  |
| messageId    | Stringa<br>Lunghezza max: 128                                                                                                                                                                  | [Opzionale] Da utilizzare per essere certi che il rilevatore AWS IoT Events elaborerà solo un messaggio di input con un determinato messageId.                                      |
| roleArn      | Stringa                                                                                                                                                                                        | L'ARN del ruolo che concede l'autorizzazione AWS IoT per inviare un messaggio di input a un rilevatore AWS IoT Events. ("Action":"iotevents:BatchPutMessage").                      |

| Nome                | Tipo                | Descrizione                                                                                                                                                                                                                                             |
|---------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| stepFunctions       | StepFunctionsAction | Avvia l'esecuzione di una macchina a stati Step Functions.                                                                                                                                                                                              |
| executionNamePrefix | Stringa             | (Opzionale) All'esecuzione della macchina a stati verrà assegnato un nome costituito da questo prefisso seguito da un UUID. Step Functions crea automaticamente un nome univoco per ogni esecuzione della macchina a stati se non ne viene fornito uno. |
| stateMachineName    | Stringa             | Il nome della macchina a stati Step Functions di cui verrà avviata l'esecuzione.                                                                                                                                                                        |
| roleArn             | Stringa             | L'ARN del ruolo che concede a IoT l'autorizzazione per avviare l'esecuzione di una macchina a stati ("Action":"states:StartExecution").                                                                                                                 |

#### Output

Nessuna

#### Errori

##### `SqlParseException`

L'espressione SQL della regola non può essere analizzata correttamente.

##### `InternalException`

Si è verificato un errore imprevisto.

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

##### `UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### `ConflictingResourceUpdateException`

Eccezione relativa ad aggiornamenti in conflitto della risorsa. Questa eccezione viene generata quando due aggiornamenti in sospeso causano un conflitto.

## SearchIndex

Indice di ricerca della query.

Riepilogo

```
aws iot search-index \
[--index-name <value>] \
--query-string <value> \
[--next-token <value>] \
[--max-results <value>] \
[--query-version <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "indexName": "string",
 "queryString": "string",
 "nextToken": "string",
 "maxResults": "integer",
 "queryVersion": "string"
}
```

### Campi di **cli-input-json**

| Nome         | Tipo                                                                          | Descrizione                                                                                              |
|--------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| indexName    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'indice di ricerca.                                                                             |
| queryString  | Stringa<br><br>Lunghezza min.: 1                                              | Stringa della query di ricerca.                                                                          |
| nextToken    | Stringa                                                                       | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |
| maxResults   | intero<br><br>Intervallo – Max: 500, min.: 1                                  | Numero massimo di risultati da restituire per volta.                                                     |
| queryVersion | Stringa                                                                       | Versione della query.                                                                                    |

### Output

```
{
 "nextToken": "string",
 "things": [
 {
 "thingName": "string",
 "thingId": "string",
 "thingTypeName": "string",
 "thingGroupNames": [
 "string"
],
 "attributes": {
 "string": "string"
 },
 }
]
}
```

```

 "shadow": "string",
 "connectivity": {
 "connected": "boolean",
 "timestamp": "long"
 }
],
 "thingGroups": [
 {
 "thingGroupName": "string",
 "thingGroupId": "string",
 "thingGroupDescription": "string",
 "attributes": {
 "string": "string"
 },
 "parentGroupNames": [
 "string"
]
 }
]
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome            | Tipo                                                                          | Descrizione                                                                                              |
|-----------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| nextToken       | Stringa                                                                       | Token usato per ottenere il successivo set di risultati oppure null se non ci sono risultati aggiuntivi. |
| things          | elenco<br>Membro: ThingDocument<br>Classe Java: java.util.List                | Oggetti che corrispondono alla query di ricerca.                                                         |
| thingName       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto.                                                                                       |
| thingId         | Stringa                                                                       | ID oggetto.                                                                                              |
| thingTypeName   | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del tipo di oggetto.                                                                                |
| thingGroupNames | elenco<br>Membro: ThingGroupName<br>Classe Java: java.util.List               | Nomi dei gruppi di oggetti.                                                                              |
| attributes      | mappa                                                                         | Attributi.                                                                                               |
| shadow          | Stringa                                                                       | La copia shadow.                                                                                         |
| connectivity    | ThingConnectivity                                                             | Indica se l'oggetto è connesso o al servizio AWS IoT.                                                    |

| Nome                  | Tipo                                                                  | Descrizione                                                                                                                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| connected             | booleano                                                              | True se l'oggetto è connesso al servizio AWS IoT, false se non lo è.                                                                                                                                                              |
| timestamp             | Long                                                                  | L'ora nel formato epoca (in millisecondi) in cui l'oggetto è stato collegato o scollegato per l'ultima volta. Se l'oggetto è stato disconnesso per più di qualche settimana, il valore temporale potrebbe non essere specificato. |
| thingGroups           | elenco<br>Membro: ThingGroupDocument<br>Classe Java: java.util.List   | Gruppi di oggetti che corrispondono alla query di ricerca.                                                                                                                                                                        |
| thingGroupName        | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del gruppo di oggetti.                                                                                                                                                                                                       |
| thingGroupId          | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9 -]+   | ID gruppo di oggetti.                                                                                                                                                                                                             |
| thingGroupDescription | Stringa<br>Lunghezza max: 2028<br>Modello: [\p{Graph}]*               | Descrizione del gruppo di oggetti.                                                                                                                                                                                                |
| attributes            | mappa                                                                 | Attributi del gruppo di oggetti.                                                                                                                                                                                                  |
| parentGroupNames      | elenco<br>Membro: ThingGroupName<br>Classe Java: java.util.List       | Nomi dei gruppi padre.                                                                                                                                                                                                            |

## Errori

### InvalidRequestException

I contenuti della richiesta non sono validi.

### ThrottlingException

La velocità supera il limite.

### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

### ServiceUnavailableException

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

#### ResourceNotFoundException

La risorsa specificata non esiste.

#### InvalidQueryException

La query non è valida.

#### IndexNotReadyException

L'indice non è pronto.

## SetDefaultAuthorizer

Imposta l'autorizzazione predefinita. Questa verrà usata se viene stabilita una connessione WebSocket senza specificare alcuna autorizzazione.

### Riepilogo

```
aws iot set-default-authorizer \
 --authorizer-name <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "authorizerName": "string"
}
```

### Campi di cli-input-json

| Nome           | Tipo                                                                | Descrizione               |
|----------------|---------------------------------------------------------------------|---------------------------|
| authorizerName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=,@-]+ | Nome dell'autorizzazione. |

### Output

```
{
 "authorizerName": "string",
 "authorizerArn": "string"
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo    | Descrizione               |
|----------------|---------|---------------------------|
| authorizerName | Stringa | Nome dell'autorizzazione. |

| Nome          | Tipo                                             | Descrizione              |
|---------------|--------------------------------------------------|--------------------------|
|               | Lunghezza max: 128, min.: 1<br>Modello: [w=,@-]+ |                          |
| authorizerArn | Stringa                                          | ARN dell'autorizzazione. |

#### Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ResourceAlreadyExistsException**

La risorsa esiste già.

## SetDefaultPolicyVersion

Imposta la versione indicata della policy specificata come versione predefinita (operativa) della policy. Questa operazione influisce su tutti i certificati cui è collegata la policy. Per elencare le entità principali cui è collegata la policy, usa l'API ListPrincipalPolicy.

#### Riepilogo

```
aws iot set-default-policy-version \
--policy-name <value> \
--policy-version-id <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "policyName": "string",
 "policyVersionId": "string"
}
```

### Campi di **cli-input-json**

| Nome            | Tipo                                                          | Descrizione               |
|-----------------|---------------------------------------------------------------|---------------------------|
| policyName      | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [w+=,.@-]+ | Nome della policy.        |
| policyVersionId | Stringa<br>Modello: [0-9]+                                    | ID versione della policy. |

### Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## SetLoggingOptions

Imposta le opzioni di logging.

NOTA: l'utilizzo di questo comando non è consigliato. Usa invece **SetV2LoggingOptions**.

Riepilogo

```
aws iot set-logging-options \
--logging-options-payload <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
```

```

 "loggingOptionsPayload": {
 "roleArn": "string",
 "logLevel": "string"
 }
}

```

#### Campi di **cli-input-json**

| Nome                  | Tipo                  | Descrizione                                                             |
|-----------------------|-----------------------|-------------------------------------------------------------------------|
| loggingOptionsPayload | LoggingOptionsPayload | Payload delle opzioni di logging.                                       |
| roleArn               | Stringa               | ARN del ruolo IAM che concede l'accesso.                                |
| logLevel              | Stringa               | Livello di log.<br>Enumerazione: DEBUG   INFO   ERROR   WARN   DISABLED |

#### Output

Nessuna

Errori

**InternalException**

Si è verificato un errore imprevisto.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

## SetV2LogLevel

Imposta il livello di logging.

Riepilogo

```

aws iot set-v2-logging-level \
--log-target <value> \
--log-level <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]

```

#### Formato di **cli-input-json**

```

{
 "logTarget": {
 "targetType": "string",
 "targetName": "string"
 },
 "logLevel": "string"
}

```

}

#### Campi di **cli-input-json**

| Nome       | Tipo      | Descrizione                                                             |
|------------|-----------|-------------------------------------------------------------------------|
| logTarget  | LogTarget | Target del log.                                                         |
| targetType | Stringa   | Il tipo di destinazione.<br>Enumerazione: DEFAULT   THING_GROUP         |
| targetName | Stringa   | Nome del target.                                                        |
| logLevel   | Stringa   | Livello di log.<br>Enumerazione: DEBUG   INFO   ERROR   WARN   DISABLED |

#### Output

Nessuna

Errori

**InternalException**

Si è verificato un errore imprevisto.

**NotConfiguredException**

La risorsa non è configurata.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

## SetV2LoggingOptions

Imposta le opzioni di logging per il servizio di logging V2.

#### Riepilogo

```
aws iot set-v2-logging-options \
[--role-arn <value>] \
[--default-log-level <value>] \
[--disable-all-logs | --no-disable-all-logs] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di **cli-input-json**

```
{
 "roleArn": "string",
```

```
 "defaultLogLevel": "string",
 "disableAllLogs": "boolean"
}
```

#### Campi di **cli-input-json**

| Nome            | Tipo     | Descrizione                                                                             |
|-----------------|----------|-----------------------------------------------------------------------------------------|
| roleArn         | Stringa  | L'ARN del ruolo che permette a IoT di scrivere nei log di CloudWatch.                   |
| defaultLogLevel | Stringa  | Livello di logging predefinito.<br>Enumerazione: DEBUG   INFO   ERROR   WARN   DISABLED |
| disableAllLogs  | booleano | Se il valore è true, tutti i log vengono disabilitati. Il valore predefinito è false.   |

#### Output

Nessuna

Errori

**InternalException**

Si è verificato un errore imprevisto.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

## StartNextPendingJobExecution

Ottiene e avvia l'esecuzione del processo in sospeso successiva (stato IN\_PROGRESS o QUEUED) per un oggetto.

#### Riepilogo

```
aws iot-jobs-data start-next-pending-job-execution \
 --thing-name <value> \
 [--status-details <value>] \
 [--step-timeout-in-minutes <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

#### Formato di **cli-input-json**

```
{
 "thingName": "string",
 "statusDetails": {
```

```

 "string": "string"
},
"stepTimeoutInMinutes": "long"
}

```

### Campi di **cli-input-json**

| Nome                 | Tipo                                                                          | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingName            | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 :_–]+ | Nome dell'oggetto associato al dispositivo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| statusDetails        | mappa                                                                         | Raccolta di coppie nome/valore che descrivono lo stato dell'esecuzione del processo. Se non è specificato, statusDetails resta invariato.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| stepTimeoutInMinutes | Long                                                                          | Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Se lo stato di esecuzione del processo non è impostato su uno stato terminale prima del timeout o prima della reimpostazione del timer (chiamando <code>UpdateJobExecution</code> , impostando lo stato su <code>IN_PROGRESS</code> e specificando un nuovo valore di timeout nel campo <code>stepTimeoutInMinutes</code> ), lo stato di esecuzione del processo verrà impostato automaticamente su <code>TIMED_OUT</code> . L'impostazione del timeout della fase non ha alcun effetto su quello dell'avanzamento che potresti avere specificato al momento della creazione del processo ( <code>CreateJob</code> utilizzando il campo <code>timeoutConfig</code> ).<br><br>I valori validi di questo parametro variano da 1 a 10080 (da 1 minuto a 7 giorni). |

### Output

```
{
"execution": {
"jobId": "string",
"thingName": "string",
"status": "string",

```

```

 "statusDetails": {
 "string": "string"
 },
 "queuedAt": "long",
 "startedAt": "long",
 "lastUpdatedAt": "long",
 "approximateSecondsBeforeTimedOut": "long",
 "versionNumber": "long",
 "executionNumber": "long",
 "jobDocument": "string"
}
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome          | Tipo                                                                                                                                                                                                                                                                    | Descrizione                                                                                                                                                                                                                                              |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| execution     | JobExecution                                                                                                                                                                                                                                                            | Oggetto JobExecution.                                                                                                                                                                                                                                    |
| jobId         | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+                                                                                                                                                                                              | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                                                                                 |
| thingName     | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+                                                                                                                                                                                           | Nome dell'oggetto che sta eseguendo il processo.                                                                                                                                                                                                         |
| stato         | Stringa<br><br>Stato dell'esecuzione del processo. Può essere "QUEUED", "IN_PROGRESS", "FAILED", "SUCCESS", "CANCELED", "TIMED_OUT", "REJECTED" o "REMOVED".<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED | Stato dell'esecuzione del processo. Può essere "QUEUED", "IN_PROGRESS", "FAILED", "SUCCESS", "CANCELED", "TIMED_OUT", "REJECTED" o "REMOVED".<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED |
| statusDetails | mappa                                                                                                                                                                                                                                                                   | Raccolta di coppie nome/valore che descrivono lo stato dell'esecuzione del processo.                                                                                                                                                                     |
| queuedAt      | Long                                                                                                                                                                                                                                                                    | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'aggiunta dell'esecuzione del processo alla coda.                                                                                                                                               |
| startedAt     | Long                                                                                                                                                                                                                                                                    | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'avvio dell'esecuzione del processo.                                                                                                                                                            |
| lastUpdatedAt | Long                                                                                                                                                                                                                                                                    | Periodo di tempo, in secondi, dall'epoca (Unix epoch) all'ultimo aggiornamento dell'esecuzione del processo.                                                                                                                                             |

| Nome                             | Tipo                            | Descrizione                                                                                                                                                                                                                               |
|----------------------------------|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| approximateSecondsBeforeTimedOut | Long                            | Il numero stimato di secondi che rimangono prima che lo stato di esecuzione del processo venga modificato in <code>TIMED_OUT</code> . L'effettivo timeout dell'esecuzione del processo può verificarsi 60 secondi dopo la durata stimata. |
| versionNumber                    | Long                            | Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che vengono aggiornate da un dispositivo.                                                                                |
| executionNumber                  | Long                            | Numero che identifica una determinata esecuzione di un processo in un dispositivo specifico. Può essere usato successivamente in comandi che restituiscono o aggiornano le informazioni sull'esecuzione del processo.                     |
| jobDocument                      | Stringa<br>Lunghezza max: 32768 | Contenuto del documento del processo.                                                                                                                                                                                                     |

#### Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceNotFoundException`

La risorsa specificata non esiste.

`ThrottlingException`

La velocità supera il limite.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

`CertificateValidationException`

Il certificato non è valido.

## StartOnDemandAuditTask

Avvia un audit di Device Defender on demand.

Riepilogo

```
aws iot start-on-demand-audit-task \
--target-check-names <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "targetCheckNames": [
 "string"
]
}
```

Campi di **cli-input-json**

| Nome             | Tipo                             | Descrizione                                                                                                                                                                                                                                                                                                                                                      |
|------------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| targetCheckNames | elenco<br>membro: AuditCheckName | Controlli eseguiti durante l'audit. I controlli specificati devono essere abilitati per l'account, altrimenti si verifica un'eccezione. Usa <a href="#">DescribeAccountAuditConfiguration</a> per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati, o <a href="#">UpdateAccountAuditConfiguration</a> per selezionare i controlli abilitati. |

Output

```
{
 "taskId": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome   | Tipo                                                               | Descrizione                      |
|--------|--------------------------------------------------------------------|----------------------------------|
| taskId | Stringa<br>Lunghezza max: 40, min.: 1<br>Modello: [a-z A-Z 0-9 -]+ | ID dell'audit on demand avviato. |

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

#### LimitExceeded**Exception**

È stato superato un limite.

## StartThingRegistrationTask

Crea un'attività di provisioning in blocco di oggetti.

### Riepilogo

```
aws iot start-thing-registration-task \
--template-body <value> \
--input-file-bucket <value> \
--input-file-key <value> \
--role-arn <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di **cli-input-json**

```
{
 "templateBody": "string",
 "inputFileBucket": "string",
 "inputFileKey": "string",
 "roleArn": "string"
}
```

### Campi di **cli-input-json**

| Nome            | Tipo                                                                              | Descrizione                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| templateBody    | Stringa                                                                           | Modello di provisioning.                                                                                                                                                                        |
| inputFileBucket | Stringa<br><br>Lunghezza max: 256, min.: 3<br><br>modello: [a-zA-Z0-9._-]+        | Bucket S3 che contiene il file di input.                                                                                                                                                        |
| inputFileKey    | Stringa<br><br>Lunghezza max: 1024, min.: 1<br><br>modello: [a-zA-Z0-9!_.*'()-/]+ | Nome del file di input all'interno del bucket S3. Il file contiene un file JSON delimitato da righe. Ogni riga contiene i valori dei parametri per il provisioning di un dispositivo (oggetto). |
| roleArn         | Stringa<br><br>Lunghezza max: 2048, min.: 20                                      | ARN del ruolo IAM, che concede l'autorizzazione al file di input.                                                                                                                               |

### Output

```
{
 "taskId": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome   | Tipo                         | Descrizione                                       |
|--------|------------------------------|---------------------------------------------------|
| taskId | Stringa<br>Lunghezza max: 40 | ID attività di provisioning in blocco di oggetti. |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ThrottlingException`

La velocità supera il limite.

##### `UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

## StopThingRegistrationTask

Annulla un'attività di provisioning in blocco di oggetti.

#### Riepilogo

```
aws iot stop-thing-registration-task \
 --task-id <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

#### Formato di `cli-input-json`

```
{
 "taskId": "string"
}
```

#### Campi di `cli-input-json`

| Nome   | Tipo                         | Descrizione                                       |
|--------|------------------------------|---------------------------------------------------|
| taskId | Stringa<br>Lunghezza max: 40 | ID attività di provisioning in blocco di oggetti. |

#### Output

Nessuna

#### Errori

#### InvalidRequestException

I contenuti della richiesta non sono validi.

#### ThrottlingException

La velocità supera il limite.

#### UnauthorizedException

Non hai le autorizzazioni necessarie per eseguire questa operazione.

#### InternalFailureException

Si è verificato un errore imprevisto.

#### ResourceNotFoundException

La risorsa specificata non esiste.

## TagResource

Aggiunge o modifica i tag di una determinata risorsa. I tag sono metadati che possono essere utilizzati per gestire una risorsa.

### Riepilogo

```
aws iot tag-resource \
--resource-arn <value> \
--tags <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "resourceArn": "string",
 "tags": [
 {
 "Key": "string",
 "Value": "string"
 }
]
}
```

### Campi di cli-input-json

| Nome        | Tipo                                                     | Descrizione                               |
|-------------|----------------------------------------------------------|-------------------------------------------|
| resourceArn | Stringa                                                  | L'ARN della risorsa.                      |
| tags        | elenco<br>member: Tag<br><br>Classe Java: java.util.List | I tag (nuovi o modificati) della risorsa. |
| Chiave      | Stringa                                                  | La chiave del tag.                        |
| Valore      | Stringa                                                  | Il valore del tag.                        |

Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**LimitExceededException**

È stato superato un limite.

## TestAuthorization

Verifica se un'entità principale specificata è autorizzata a eseguire un'operazione AWS IoT su una risorsa specificata. Utilizzare questo parametro per eseguire il test e il debugging del comportamento delle autorizzazioni dei dispositivi che si connettono al gateway di dispositivo AWS IoT.

Riepilogo

```
aws iot test-authorization \
[--principal <value>] \
[--cognito-identity-pool-id <value>] \
--auth-infos <value> \
[--client-id <value>] \
[--policy-names-to-add <value>] \
[--policy-names-to-skip <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di cli-input-json

```
{
 "principal": "string",
 "cognitoIdentityPoolId": "string",
 "authInfos": [
 {
 "actionType": "string",
 "resources": [
 "string"
]
 }
],
 "clientId": "string",
 "policyNamesToAdd": [
 "string"
],
 "policyNamesToSkip": [
 "string"
]
}
```

}

### Campi di **cli-input-json**

| Nome                  | Tipo                                                        | Descrizione                                                                                                                                        |
|-----------------------|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| principal             | Stringa                                                     | Entità principale.                                                                                                                                 |
| cognitoidentityPoolId | Stringa                                                     | ID pool di identità di Cognito.                                                                                                                    |
| authInfos             | elenco<br>Membro: AuthInfo                                  | Elenco di oggetti di informazioni sull'autorizzazione. La simulazione dell'autorizzazione crea una risposta per ogni oggetto authInfo nell'elenco. |
| actionType            | Stringa                                                     | Tipo di operazione per cui l'entità principale viene autorizzata.<br><br>Enumerazione: PUBLISH   SUBSCRIBE   RECEIVE   CONNECT                     |
| resources             | elenco<br>Membro: Resource                                  | Risorse per cui l'entità principale viene autorizzata a eseguire l'operazione specificata.                                                         |
| clientId              | Stringa                                                     | ID client MQTT.                                                                                                                                    |
| policyNamesToAdd      | elenco<br>Membro: PolicyName<br>Classe Java: java.util.List | Durante i test dell'autorizzazione personalizzata, le policy specificate qui vengono considerate collegate all'entità principale autorizzata.      |
| policyNamesToSkip     | elenco<br>Membro: PolicyName<br>Classe Java: java.util.List | Durante i test dell'autorizzazione personalizzata, le policy specificate qui vengono considerate non collegate all'entità principale autorizzata.  |

### Output

```
{
 "authResults": [
 {
 "authInfo": {
 "actionType": "string",
 "resources": [
 "string"
]
 },
 "allowed": {
 "policies": [
 {
 "policyName": "string",
 "policyArn": "string"
 }
]
 }
 }
]
}
```

```
"denied": {
 "implicitDeny": {
 "policies": [
 {
 "policyName": "string",
 "policyArn": "string"
 }
]
 },
 "explicitDeny": {
 "policies": [
 {
 "policyName": "string",
 "policyArn": "string"
 }
]
 }
},
"authDecision": "string",
"missingContextValues": [
 "string"
]
}
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome        | Tipo                                                          | Descrizione                                                                                                                           |
|-------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| authResults | elenco<br>Membro: AuthResult                                  | Risultati dell'autenticazione.                                                                                                        |
| authInfo    | AuthInfo                                                      | Informazioni sull'autorizzazione.                                                                                                     |
| actionType  | Stringa                                                       | <p>Tipo di operazione per cui l'entità principale viene autorizzata.</p> <p>Enumerazione: PUBLISH   SUBSCRIBE   RECEIVE   CONNECT</p> |
| resources   | elenco<br>Membro: Resource                                    | Risorse per cui l'entità principale viene autorizzata a eseguire l'operazione specificata.                                            |
| allowed     | Allowed                                                       | Policy e istruzioni che hanno permesso l'operazione specificata.                                                                      |
| policies    | elenco<br>Membro: Policy<br>Classe Java: java.util.List       | Elenco di policy che hanno permesso l'autenticazione.                                                                                 |
| policyName  | Stringa<br>Lunghezza max: 128, min.: 1<br>modello: [w+=,.@-]+ | Nome della policy.                                                                                                                    |

| Nome         | Tipo                                                          | Descrizione                                                                                                                                                                                                                                                                                                               |
|--------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| policyArn    | Stringa                                                       | ARN della policy.                                                                                                                                                                                                                                                                                                         |
| denied       | Denied                                                        | Policy e istruzioni che hanno negato l'operazione specificata.                                                                                                                                                                                                                                                            |
| implicitDeny | ImplicitDeny                                                  | Informazioni che negano implicitamente l'autorizzazione. Quando una policy non nega esplicitamente o non permette un'operazione su una risorsa, questo comportamento è considerato una negazione隐式.                                                                                                                       |
| policies     | elenco<br>Membro: Policy<br>Classe Java: java.util.List       | Policy che non contengono un'istruzione di rifiuto o concessione corrispondente per l'operazione specificata nella risorsa specificata.                                                                                                                                                                                   |
| policyName   | Stringa<br>Lunghezza max: 128, min.: 1<br>modello: [w+=,.@-]+ | Nome della policy.                                                                                                                                                                                                                                                                                                        |
| policyArn    | Stringa                                                       | ARN della policy.                                                                                                                                                                                                                                                                                                         |
| explicitDeny | ExplicitDeny                                                  | Informazioni che negano esplicitamente l'autorizzazione.                                                                                                                                                                                                                                                                  |
| policies     | elenco<br>Membro: Policy<br>Classe Java: java.util.List       | Policy che hanno negato l'autorizzazione.                                                                                                                                                                                                                                                                                 |
| policyName   | Stringa<br>Lunghezza max: 128, min.: 1<br>modello: [w+=,.@-]+ | Nome della policy.                                                                                                                                                                                                                                                                                                        |
| policyArn    | Stringa                                                       | ARN della policy.                                                                                                                                                                                                                                                                                                         |
| authDecision | Stringa                                                       | Decisione finale relativa all'autorizzazione per questo scenario. Per determinare la decisione relativa all'autorizzazione, vengono prese in considerazione più istruzioni. Un'istruzione di rifiuto esplicito può sostituire più istruzioni di concessione.<br><br>Enumerazione: ALLOWED   EXPLICIT_DENY   IMPLICIT_DENY |

| Nome                 | Tipo                                                                 | Descrizione                                                                               |
|----------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| missingContextValues | elenco<br>Membro: MissingContextValue<br>Classe Java: java.util.List | Contiene tutti i valori di contesto mancanti trovati durante la valutazione della policy. |

#### Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

**LimitExceededException**

È stato superato un limite.

## TestInvokeAuthorizer

Esegue il test di un comportamento delle autorizzazioni personalizzato richiamando delle autorizzazioni ad hoc specificate. Utilizzare questo parametro per eseguire il test e il debugging del comportamento delle autorizzazioni personalizzato dei dispositivi che si connettono al gateway di dispositivo AWS IoT.

#### Riepilogo

```
aws iot test-invoke-authorizer \
--authorizer-name <value> \
--token <value> \
--token-signature <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "authorizerName": "string",
 "token": "string",
 "tokenSignature": "string"
```

}

### Campi di **cli-input-json**

| Nome           | Tipo                                                                        | Descrizione                                                                                  |
|----------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| authorizerName | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [w=,@-]+                 | Nome dell'autorizzazione ad hoc.                                                             |
| token          | Stringa<br>Lunghezza max: 6144, min.: 1                                     | Token restituito dal servizio di autenticazione personalizzato.                              |
| tokenSignature | Stringa<br>Lunghezza max: 2560, min.: 1<br>Modello: [A-Z a-z 0-9 +/]++{0,2} | Firma creata con il token e la chiave privata del servizio di autenticazione personalizzato. |

### Output

```
{
 "isAuthenticated": "boolean",
 "principalId": "string",
 "policyDocuments": [
 "string"
],
 "refreshAfterInSeconds": "integer",
 "disconnectAfterInSeconds": "integer"
}
```

### Campi di output dell'interfaccia a riga di comando

| Nome                     | Tipo                                                              | Descrizione                                                                  |
|--------------------------|-------------------------------------------------------------------|------------------------------------------------------------------------------|
| isAuthenticated          | booleano                                                          | True se il token è autenticato; in caso contrario, false.                    |
| principalId              | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-z A-Z 0-9]+ | ID entità principale.                                                        |
| policyDocuments          | elenco<br>Membro: PolicyDocument                                  | Documenti delle policy IAM.                                                  |
| refreshAfterInSeconds    | intero                                                            | Numero di secondi dopo i quali le credenziali temporanee vengono aggiornate. |
| disconnectAfterInSeconds | intero                                                            | Numero di secondi dopo i quali la connessione viene terminata.               |

### Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

**InvalidResponseException**

La risposta non è valida.

## TransferCertificate

Trasferisce il certificato indicato nell'account AWS specificato.

Puoi annullare il trasferimento finché non viene riconosciuto dal destinatario.

All'account della destinazione di trasferimento non viene inviata alcuna notifica. Sarà il chiamante a inviare una notifica al target di trasferimento.

Il certificato trasferito non deve avere lo stato ACTIVE. Puoi usare l'API UpdateCertificate per disattivarlo:

Al certificato non devono essere collegate policy. Puoi usare l'API DetachPrincipalPolicy per scollarle.

**Riepilogo**

```
aws iot transfer-certificate \
 --certificate-id <value> \
 --target-aws-account <value> \
 [--transfer-message <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

**Formato di cli-input-json**

```
{
 "certificateId": "string",
 "targetAwsAccount": "string",
 "transferMessage": "string"
}
```

**Campi di cli-input-json**

| Nome          | Tipo    | Descrizione                                                                                                           |
|---------------|---------|-----------------------------------------------------------------------------------------------------------------------|
| certificateId | Stringa | ID del certificato. L'ultima parte dell'ARN del certificato contiene l'ID certificato.<br>Lunghezza max: 64, min.: 64 |

| Nome             | Tipo                                                              | Descrizione                 |
|------------------|-------------------------------------------------------------------|-----------------------------|
|                  | Modello: (0x)?[a-f A-F 0-9]+                                      |                             |
| targetAwsAccount | Stringa<br><br>Lunghezza max: 12, min.: 12<br><br>Modello: [0-9]+ | Account AWS.                |
| transferMessage  | Stringa<br><br>Lunghezza max: 128                                 | Messaggio di trasferimento. |

#### Output

```
{
 "transferredCertificateArn": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome                      | Tipo    | Descrizione          |
|---------------------------|---------|----------------------|
| transferredCertificateArn | Stringa | ARN del certificato. |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `CertificateStateException`

L'operazione del certificato non è consentita.

##### `TransferConflictException`

Non puoi trasferire il certificato perché sono ancora collegate policy di autorizzazione.

##### `ThrottlingException`

La velocità supera il limite.

##### `UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

##### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

## UntagResource

Rimuove determinati tag (metadati) dalla risorsa.

## Riepilogo

```
aws iot untag-resource \
 --resource-arn <value> \
 --tag-keys <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "resourceArn": "string",
 "tagKeys": [
 "string"
]
}
```

## Campi di cli-input-json

| Nome        | Tipo                                                    | Descrizione                                             |
|-------------|---------------------------------------------------------|---------------------------------------------------------|
| resourceArn | Stringa                                                 | L'ARN della risorsa.                                    |
| tagKeys     | elenco<br>member: TagKey<br>Classe Java: java.util.List | Un elenco di chiavi dei tag da rimuovere dalla risorsa. |

## Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

# UpdateAccountAuditConfiguration

Configura o riconfigura le impostazioni di auditing di Device Defender per l'account. Le impostazioni includono la modalità di invio delle notifiche degli audit e i controlli di auditing abilitati o disabilitati.

## Riepilogo

```
aws iot update-account-audit-configuration \
 [--role-arn <value>] \
```

```
[--audit-notification-target-configurations <value>] \
[--audit-check-configurations <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "roleArn": "string",
 "auditNotificationTargetConfigurations": {
 "string": {
 "targetArn": "string",
 "roleArn": "string",
 "enabled": "boolean"
 }
 },
 "auditCheckConfigurations": {
 "string": {
 "enabled": "boolean"
 }
 }
}
```

#### Campi di cli-input-json

| Nome                                  | Tipo                                     | Descrizione                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn                               | Stringa<br>Lunghezza max: 2048, min.: 20 | ARN del ruolo che concede ad AWS IoT l'autorizzazione per accedere alle informazioni su dispositivi, policy, certificati e altri elementi necessari per eseguire un audit.                                                                                                                                                    |
| auditNotificationTargetConfigurations | mappa                                    | Informazioni sui target a cui vengono inviate le notifiche di auditing.                                                                                                                                                                                                                                                       |
| targetArn                             | Stringa                                  | ARN del target (argomento SNS) a cui vengono inviate le notifiche di auditing.                                                                                                                                                                                                                                                |
| roleArn                               | Stringa<br>Lunghezza max: 2048, min.: 20 | ARN del ruolo che concede l'autorizzazione per l'invio delle notifiche ai target.                                                                                                                                                                                                                                             |
| enabled                               | booleano                                 | True se le notifiche per il target sono abilitate.                                                                                                                                                                                                                                                                            |
| auditCheckConfigurations              | mappa                                    | Specifica i controlli di auditing abilitati e disabilitati per l'account. Usa <a href="#">DescribeAccountAuditConfiguration</a> per visualizzare l'elenco di tutti i controlli, inclusi quelli attualmente abilitati.<br><br>La raccolta di alcuni dati potrebbe iniziare immediatamente quando determinati controlli vengono |

| Nome                 | Tipo     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |          | <p>abilitati. Quando un controllo viene disabilitato, i dati raccolti fino a quel momento in relazione al controllo vengono eliminati.</p> <p>Non è possibile disabilitare un controllo se viene usato da un audit pianificato. È prima necessario eliminare il controllo dall'audit pianificato oppure eliminare l'audit pianificato stesso.</p> <p>Nella prima chiamata a <code>UpdateAccountAuditConfiguration</code> questo parametro è obbligatorio e deve specificare almeno un controllo abilitato.</p> |
| <code>enabled</code> | booleano | True se il controllo di auditing è abilitato per l'account.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

#### Output

Nessuna

#### Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

## UpdateAuthorizer

Aggiorna un'autorizzazione.

#### Riepilogo

```
aws iot update-authorizer \
--authorizer-name <value> \
[--authorizer-function-arn <value>] \
[--token-key-name <value>] \
[--token-signing-public-keys <value>] \
[--status <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di `cli-input-json`

```
{
 "authorizerName": "string",
 "authorizerFunctionArn": "string",
 "tokenKeyName": "string",
 "tokenSigningPublicKeys": {
 "string": "string"
 },
 "status": "string"
}
```

#### Campi di `cli-input-json`

| Nome                   | Tipo    | Descrizione                                                                                                                      |
|------------------------|---------|----------------------------------------------------------------------------------------------------------------------------------|
| authorizerName         | Stringa | Nome dell'autorizzazione.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=,@-]+                                            |
| authorizerFunctionArn  | Stringa | ARN della funzione Lambda dell'autorizzazione.                                                                                   |
| tokenKeyName           | Stringa | Chiave usata per estrarre il token dalle intestazioni HTTP.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ |
| tokenSigningPublicKeys | mappa   | Chiavi pubbliche usate per verificare la firma del token.                                                                        |
| stato                  | Stringa | Stato della richiesta di autorizzazione di aggiornamento.<br><br>Enumerazione: ACTIVE   INACTIVE                                 |

#### Output

```
{
 "authorizerName": "string",
 "authorizerArn": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo    | Descrizione                                                                           |
|----------------|---------|---------------------------------------------------------------------------------------|
| authorizerName | Stringa | Nome dell'autorizzazione.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=,@-]+ |
| authorizerArn  | Stringa | ARN dell'autorizzazione.                                                              |

## Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**LimitExceededException**

È stato superato un limite.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

# UpdateBillingGroup

Aggiorna le informazioni sul gruppo di fatturazione.

## Riepilogo

```
aws iot update-billing-group \
 --billing-group-name <value> \
 --billing-group-properties <value> \
 [--expected-version <value>] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "billingGroupName": "string",
 "billingGroupProperties": {
 "billingGroupDescription": "string"
 },
 "expectedVersion": "long"
}
```

## Campi di **cli-input-json**

| Nome             | Tipo    | Descrizione                         |
|------------------|---------|-------------------------------------|
| billingGroupName | Stringa | Il nome del gruppo di fatturazione. |

| Nome                    | Tipo                                                     | Descrizione                                                                                                                                                                                                                                                             |
|-------------------------|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | Lunghezza max: 128, min.: 1<br>Modello: [a-zA-Z0-9:_-]+  |                                                                                                                                                                                                                                                                         |
| billingGroupProperties  | BillingGroupProperties                                   | Le proprietà del gruppo di fatturazione.                                                                                                                                                                                                                                |
| billingGroupDescription | Stringa<br>Lunghezza max: 2028<br>Modello: [\p{Graph}]^* | La descrizione del gruppo di fatturazione.                                                                                                                                                                                                                              |
| expectedVersion         | Long                                                     | La versione prevista del gruppo di fatturazione. Se la versione del gruppo di fatturazione non corrisponde alla versione prevista specificata nella richiesta, la richiesta <code>DeleteBillingGroup</code> viene rifiutata con <code>VersionConflictException</code> . |

#### Output

```
{
 "version": "long"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome     | Tipo | Descrizione                                   |
|----------|------|-----------------------------------------------|
| versione | Long | L'ultima versione del gruppo di fatturazione. |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `VersionConflictException`

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

# UpdateCACertificate

Aggiorna un certificato CA registrato.

Riepilogo

```
aws iot update-ca-certificate \
 --certificate-id <value> \
 [--new-status <value>] \
 [--new-auto-registration-status <value>] \
 [--registration-config <value>] \
 [--remove-auto-registration | --no-remove-auto-registration] \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "certificateId": "string",
 "newStatus": "string",
 "newAutoRegistrationStatus": "string",
 "registrationConfig": {
 "templateBody": "string",
 "roleArn": "string"
 },
 "removeAutoRegistration": "boolean"
}
```

Campi di `cli-input-json`

| Nome                                   | Tipo                                                                                                                                                    | Descrizione                                                                                        |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <code>certificateId</code>             | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+                                                                          | Identificatore del certificato CA.                                                                 |
| <code>newStatus</code>                 | Stringa<br><br>Nota: il valore di stato REGISTER_INACTIVE è obsoleto e non deve essere usato.<br><br>Enumerazione: ACTIVE   INACTIVE                    | Stato di aggiornamento del certificato CA.                                                         |
| <code>newAutoRegistrationStatus</code> | Stringa<br><br>Nuovo valore per lo stato di registrazione automatica. I valori validi sono: "ENABLE" e "DISABLE".<br><br>Enumerazione: ENABLE   DISABLE | Nuovo valore per lo stato di registrazione automatica. I valori validi sono: "ENABLE" e "DISABLE". |
| <code>registrationConfig</code>        | <code>RegistrationConfig</code>                                                                                                                         | Informazioni sulla configurazione della registrazione.                                             |

| Nome                   | Tipo     | Descrizione                                     |
|------------------------|----------|-------------------------------------------------|
| templateBody           | Stringa  | Corpo del modello.                              |
| roleArn                | Stringa  | ARN del ruolo.<br>Lunghezza max: 2048, min.: 20 |
| removeAutoRegistration | booleano | Se è true, rimuove la registrazione automatica. |

#### Output

Nessuna

#### Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## UpdateCertificate

Aggiorna lo stato del certificato specificato. Questa operazione è idempotente.

Il passaggio di un certificato dallo stato ACTIVE (incluso REVOKED) non disconnette i dispositivi attualmente connessi, ma questi dispositivi non saranno più in grado di riconnettersi.

Lo stato ACTIVE è necessario per autenticare i dispositivi che si connettono ad AWS IoT usando un certificato.

#### Riepilogo

```
aws iot update-certificate \
--certificate-id <value> \
--new-status <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di cli-input-json

```
{
 "certificateId": "string",
```

```
 "newStatus": "string"
}
```

#### Campi di **cli-input-json**

| Nome          | Tipo                                                                           | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| certificateId | Stringa<br><br>Lunghezza max: 64, min.: 64<br><br>Modello: (0x)?[a-f A-F 0-9]+ | ID del certificato. L'ultima parte dell'ARN del certificato contiene l'ID certificato.                                                                                                                                                                                                                                                                                                                                                              |
| newStatus     | Stringa                                                                        | Nuovo stato.<br><br>Nota: l'impostazione dello stato su PENDING_TRANSFER comporta la generazione di un'eccezione.<br>PENDING_TRANSFER è uno stato usato internamente da AWS IoT. Questo stato non è destinato a essere usato dagli sviluppatori.<br><br>Nota: il valore di stato REGISTER_INACTIVE è obsoleto e non deve essere usato.<br><br>Enumerazione: ACTIVE   INACTIVE   REVOKED   PENDING_TRANSFER   REGISTER_INACTIVE   PENDING_ACTIVATION |

#### Output

Nessuna

Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**CertificateStateException**

L'operazione del certificato non è consentita.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

#### InternalFailureException

Si è verificato un errore imprevisto.

## UpdateDynamicThingGroup

Aggiorna un gruppo di oggetti dinamico.

### Riepilogo

```
aws iot update-dynamic-thing-group \
--thing-group-name <value> \
--thing-group-properties <value> \
[--expected-version <value>] \
[--index-name <value>] \
[--query-string <value>] \
[--query-version <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "thingGroupName": "string",
 "thingGroupProperties": {
 "thingGroupDescription": "string",
 "attributePayload": {
 "attributes": {
 "string": "string"
 },
 "merge": "boolean"
 }
 },
 "expectedVersion": "long",
 "indexName": "string",
 "queryString": "string",
 "queryVersion": "string"
}
```

### Campi di **cli-input-json**

| Nome                  | Tipo                                                                  | Descrizione                                                |
|-----------------------|-----------------------------------------------------------------------|------------------------------------------------------------|
| thingGroupName        | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a–z A–Z 0–9 :_–]+ | Il nome del gruppo di oggetti dinamico da aggiornare.      |
| thingGroupProperties  | ThingGroupProperties                                                  | Le proprietà del gruppo di oggetti dinamico da aggiornare. |
| thingGroupDescription | Stringa<br>Lunghezza max: 2028<br>Modello: [\p{Graph}]*               | Descrizione del gruppo di oggetti.                         |
| attributePayload      | AttributePayload                                                      | Attributi del gruppo di oggetti in formato JSON.           |

| Nome            | Tipo                                                                                 | Descrizione                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| attributes      | mappa                                                                                | <p>Stringa JSON contenente fino a tre coppie chiave/valore in formato JSON. Ad esempio:</p> <pre>\"attributes\": {\\"string1\\\":  \\"string2\\\"}</pre>                                                                                                                                                                                                                    |
| merge           | booleano                                                                             | <p>Specifica se l'elenco di attributi fornito in AttributePayload deve essere unito agli attributi archiviati nel registro, anziché sovrascrivere questi ultimi.</p> <p>Per rimuovere un attributo, chiama UpdateThing con un valore di attributo vuoto.</p> <p><b>Note</b></p> <p>L'attributo <code>merge</code> è valido solo quando chiavi <code>UpdateThing</code>.</p> |
| expectedVersion | Long                                                                                 | <p>La versione prevista del gruppo di oggetti dinamico da aggiornare.</p>                                                                                                                                                                                                                                                                                                   |
| indexName       | <p>Stringa</p> <p>Lunghezza max: 128, min.: 1</p> <p>Modello: [a-z A-Z 0-9 :_-]+</p> | <p>L'indice del gruppo di oggetti dinamico da aggiornare.</p> <p><b>Note</b></p> <p>Attualmente è supportato un indice: "AWS_Things".</p>                                                                                                                                                                                                                                   |
| queryString     | <p>Stringa</p> <p>Lunghezza min.: 1</p>                                              | <p>La stringa di query per la ricerca del gruppo di oggetti dinamico da aggiornare.</p>                                                                                                                                                                                                                                                                                     |
| queryVersion    | Stringa                                                                              | <p>La versione di query del gruppo di oggetti dinamico da aggiornare.</p> <p><b>Note</b></p> <p>Attualmente è supportata una versione di query: "2017-09-30". Se non viene specificata, la versione di query è impostata in modo predefinito su questo valore.</p>                                                                                                          |

## Output

```
{
 "version": "long"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome     | Tipo | Descrizione                                 |
|----------|------|---------------------------------------------|
| versione | Long | La versione del gruppo di oggetti dinamico. |

## Errori

### InvalidRequestException

I contenuti della richiesta non sono validi.

### VersionConflictException

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

### ThrottlingException

La velocità supera il limite.

### InternalFailureException

Si è verificato un errore imprevisto.

### ResourceNotFoundException

La risorsa specificata non esiste.

### InvalidQueryException

La query non è valida.

# UpdateEventConfigurations

Aggiorna le configurazioni dell'evento.

## Riepilogo

```
aws iot update-event-configurations \
[--event-configurations <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "eventConfigurations": {
 "string": {
```

```
 "Enabled": "boolean"
 }
}
```

#### Campi di **cli-input-json**

| Nome                | Tipo     | Descrizione                                 |
|---------------------|----------|---------------------------------------------|
| eventConfigurations | mappa    | Nuovi valori di configurazione dell'evento. |
| Enabled             | booleano | True per abilitare la configurazione.       |

#### Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ThrottlingException**

La velocità supera il limite.

## UpdateIndexingConfiguration

Aggiorna la configurazione della ricerca.

#### Riepilogo

```
aws iot update-indexing-configuration \
[--thing-indexing-configuration <value>] \
[--thing-group-indexing-configuration <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di **cli-input-json**

```
{
 "thingIndexingConfiguration": {
 "thingIndexingMode": "string",
 "thingConnectivityIndexingMode": "string"
 },
 "thingGroupIndexingConfiguration": {
 "thingGroupIndexingMode": "string"
 }
}
```

### Campi di `cli-input-json`

| Nome                            | Tipo                            | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingIndexingConfiguration      | ThingIndexingConfiguration      | Configurazione dell'indicizzazione di oggetti.                                                                                                                                                                                                                                                                                                                                                                                                  |
| thingIndexingMode               | Stringa                         | <p>Modalità di indicizzazione di oggetti. I valori validi sono:</p> <ul style="list-style-type: none"> <li>• REGISTRY – L'indice dell'oggetto contiene solo dati del registro.</li> <li>• REGISTRY_AND_SHADOW – L'indice dell'oggetto contiene i dati shadow e del registro.</li> <li>• OFF – L'indicizzazione di oggetti è disabilitata.</li> </ul> <p>Enumerazione: OFF   REGISTRY   REGISTRY_AND_SHADOW</p>                                  |
| thingConnectivityIndexingMode   | Stringa                         | <p>La modalità di indicizzazione della connettività. I valori validi sono:</p> <ul style="list-style-type: none"> <li>• STATUS – L'indice dell'oggetto contiene lo stato di connettività. Per abilitare l'indicizzazione della connettività degli oggetti, thingIndexMode non deve essere impostato su OFF.</li> <li>• OFF – L'indicizzazione dello stato della connettività degli oggetti è disabilitato.</li> </ul> <p>enum: OFF   STATUS</p> |
| thingGroupIndexingConfiguration | ThingGroupIndexingConfiguration | Configurazione dell'indicizzazione di gruppi di oggetti.                                                                                                                                                                                                                                                                                                                                                                                        |
| thingGroupIndexingMode          | Stringa                         | <p>Modalità di indicizzazione di gruppi di oggetti.</p> <p>enumerazione: OFF   ON</p>                                                                                                                                                                                                                                                                                                                                                           |

### Output

Nessuna

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## UpdateJob

Aggiorna i campi supportati del processo specificato.

Riepilogo

```
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]
```

Formato di cli-input-json

```
{
 "jobId": "string",
 "description": "string",
 "presignedUrlConfig": {
 "roleArn": "string",
 "expiresInSec": "long"
 },
 "jobExecutionsRolloutConfig": {
 "maximumPerMinute": "integer",
 "exponentialRate": {
 "baseRatePerMinute": "integer",
 "incrementFactor": "double",
 "rateIncreaseCriteria": {
 "numberOfNotifiedThings": "integer",
 "numberOfSucceededThings": "integer"
 }
 }
 },
 "abortConfig": {
 "criteriaList": [
 {
 "failureType": "string",
 "action": "string",
 "thresholdPercentage": "double",
 "minNumberOfExecutedThings": "integer"
 }
]
 },
 "timeoutConfig": {
 "inProgressTimeoutInMinutes": "long"
```

```
}
```

#### Campi di **cli-input-json**

| Nome                       | Tipo                                                               | Descrizione                                                                                                                                                                                                                                                     |
|----------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId                      | Stringa<br>Lunghezza max: 64, min.: 1<br>Modello: [a-z A-Z 0-9 _]+ | L'ID del processo da aggiornare.                                                                                                                                                                                                                                |
| description                | Stringa<br>Lunghezza max: 2028<br>Modello: [^\p{C}]+               | Breve descrizione di testo del processo.                                                                                                                                                                                                                        |
| presignedUrlConfig         | PresignedUrlConfig                                                 | Informazioni di configurazione per URL S3 prefissati.                                                                                                                                                                                                           |
| roleArn                    | Stringa<br>Lunghezza max: 2048, min.: 20                           | L'ARN di un ruolo IAM che concede l'autorizzazione per scaricare file dal bucket S3 in cui vengono archiviati i dati e gli aggiornamenti del processo. Il ruolo deve anche concedere l'autorizzazione per IoT per il download dei file.                         |
| expiresInSec               | Long<br>Intervallo – Max: 3600, min.: 60                           | Periodo di validità (in secondi) degli URL prefissati. I valori validi sono compresi tra 60 e 3600 e il valore predefinito è 3600 secondi. Gli URL prefissati vengono generati quando il servizio Jobs riceve una richiesta MQTT per il documento del processo. |
| jobExecutionsRolloutConfig | JobExecutionsRolloutConfig                                         | Permette di creare un'implementazione per fasi del processo.                                                                                                                                                                                                    |
| maximumPerMinute           | intero<br>Intervallo - min.: 1                                     | Numero massimo di oggetti che riceveranno una notifica di un processo in sospeso, ogni minuto. Questo parametro permette di creare un'implementazione per fasi.                                                                                                 |
| exponentialRate            | ExponentialRolloutRate                                             | La velocità di aumento di un rollout di processo. Questo parametro consente di definire una velocità esponenziale per un rollout di processo.                                                                                                                   |
| baseRatePerMinute          | intero                                                             | Il numero minimo di oggetti che riceveranno una notifica di un                                                                                                                                                                                                  |

| Nome                      | Tipo                                                                   | Descrizione                                                                                                                                                         |
|---------------------------|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | Intervallo – Max: 1000, min.: 1                                        | processo in sospeso, ogni minuto all'inizio del rollout di processo. Questo parametro consente di definire la velocità iniziale di un rollout.                      |
| rateIncreaseCriteria      | RateIncreaseCriteria                                                   | I criteri per avviare l'aumento della velocità di rollout per un processo.<br><br>AWS IoT supporta fino a una cifra dopo il decimale (ad esempio, 1,5 ma non 1,55). |
| numberOfNotifiedThings    | intero<br><br>Intervallo - min.: 1                                     | La soglia per il numero di oggetti notificati che avvierà l'aumento della velocità di rollout.                                                                      |
| numberOfSucceededThings   | intero<br><br>Intervallo - min.: 1                                     | La soglia per il numero di oggetti completati che avvierà l'aumento della velocità di rollout.                                                                      |
| abortConfig               | AbortConfig                                                            | Consente di creare criteri per interrompere un processo.                                                                                                            |
| criteriaList              | elenco<br><br>member: AbortCriteria<br><br>Classe Java: java.util.List | L'elenco dei criteri di eliminazione per definire regole per interrompere il processo.                                                                              |
| failureType               | Stringa                                                                | Il tipo di errore di esecuzione di processo per definire una regola di avvio dell'interruzione di un processo.<br><br>enum: FAILED   REJECTED   TIMED_OUT   ALL     |
| action                    | Stringa                                                                | Il tipo di operazione di eliminazione per avviare l'interruzione di un processo.<br><br>enum: CANCEL                                                                |
| minNumberOfExecutedThings | intero<br><br>Intervallo - min.: 1                                     | Il numero minimo di oggetti eseguiti prima della valutazione della regola di interruzione.                                                                          |

| Nome                       | Tipo          | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| timeoutConfig              | TimeoutConfig | Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione del processo. Il timer viene avviato quando imposta lo stato di esecuzione del processo su <code>IN_PROGRESS</code> . Se lo stato di esecuzione del processo non è impostato su un altro stato terminale prima della scadenza del tempo a disposizione, verrà automaticamente impostato su <code>TIMED_OUT</code> .                                                                                                                                                                      |
| inProgressTimeoutInMinutes | Long          | Specifica l'intervallo di tempo, in minuti, a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. L'intervallo di timeout può essere compreso fra 1 minuto e 7 giorni (da 1 a 10080 minuti). Il timer in corso non può essere aggiornato e verrà applicato a tutte le esecuzioni del processo. Se l'esecuzione del processo resta nello stato <code>IN_PROGRESS</code> per un periodo di tempo superiore a quello consentito dall'intervallo, l'esecuzione del processo non andrà a buon fine e verrà impostato lo stato <code>TIMED_OUT</code> terminale. |

#### Output

Nessuna

#### Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

# UpdateJobExecution

Aggiorna lo stato dell'esecuzione di un processo.

Riepilogo

```
aws iot-jobs-data update-job-execution \
--job-id <value> \
--thing-name <value> \
--status <value> \
[--status-details <value>] \
[--step-timeout-in-minutes <value>] \
[--expected-version <value>] \
[--include-job-execution-state | --no-include-job-execution-state] \
[--include-job-document | --no-include-job-document] \
[--execution-number <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "jobId": "string",
 "thingName": "string",
 "status": "string",
 "statusDetails": {
 "string": "string"
 },
 "stepTimeoutInMinutes": "long",
 "expectedVersion": "long",
 "includeJobExecutionState": "boolean",
 "includeJobDocument": "boolean",
 "executionNumber": "long"
}
```

Campi di **cli-input-json**

| Nome      | Tipo                                                                                                                                                                                                                    | Descrizione                                                                                                                                                                                              |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| jobId     | Stringa<br><br>Lunghezza max: 64, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+                                                                                                                                             | Identificatore univoco assegnato al processo al momento della creazione.                                                                                                                                 |
| thingName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+                                                                                                                                           | Nome dell'oggetto associato al dispositivo.                                                                                                                                                              |
| stato     | Stringa<br><br>Nuovo stato per l'esecuzione del processo (IN_PROGRESS, FAILED, SUCCESS o REJECTED). Questo valore deve essere specificato per ogni aggiornamento.<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED | Nuovo stato per l'esecuzione del processo (IN_PROGRESS, FAILED, SUCCESS o REJECTED). Questo valore deve essere specificato per ogni aggiornamento.<br><br>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED |

| Nome                 | Tipo  | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |       | FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| statusDetails        | mappa | Opzionale. Raccolta di coppie nome/valore che descrivono lo stato dell'esecuzione del processo. Se non è specificato, statusDetails resta invariato.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| stepTimeoutInMinutes | Long  | <p>Specifica l'intervallo di tempo a disposizione di ciascun dispositivo per terminare l'esecuzione di questo processo. Se lo stato di esecuzione del processo non è impostato su uno stato terminale prima del timeout o prima della reimpostazione del timer (chiamando nuovamente <code>UpdateJobExecution</code>, impostando lo stato su <code>IN_PROGRESS</code> e specificando un nuovo valore di timeout in questo campo), lo stato di esecuzione del processo verrà impostato automaticamente su <code>TIMED_OUT</code>. L'impostazione o la reimpostazione del timeout della fase non ha alcun effetto su quello dell'avanzamento che potresti avere specificato al momento della creazione del processo (<code>CreateJob</code> utilizzando il campo <code>timeoutConfig</code>).</p> <p>I valori validi di questo parametro variano da 1 a 10080 (da 1 minuto a 7 giorni). Il valore -1 è valido e annullerà il timer della fase corrente (creato tramite un precedente utilizzo di <code>UpdateJobExecutionRequest</code>).</p> |

| Nome                     | Tipo    | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| expectedVersion          | Long    | Opzionale. Versione corrente prevista dell'esecuzione del processo. Ogni volta che aggiorni l'esecuzione del processo, la versione viene incrementata. Se la versione dell'esecuzione del processo archiviata in Jobs non corrisponde, l'aggiornamento viene rifiutato con errore VersionMismatch e viene restituita una risposta ErrorResponse che contiene i dati sullo stato di esecuzione del processo corrente. Questo comportamento rende superfluo eseguire una richiesta DescribeJobExecution separata per ottenere i dati sullo stato dell'esecuzione del processo. |
| includeJobExecutionState | boolean | Opzionale. Quando è incluso e impostato su true, la risposta contiene i dati JobExecutionState. Il valore predefinito è false.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| includeJobDocument       | boolean | Opzionale. Se è impostato su true, la risposta contiene il documento del processo. Il valore predefinito è false.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| executionNumber          | Long    | Opzionale. Numero che identifica una determinata esecuzione di un processo in un dispositivo specifico.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

#### Output

```
{
 "executionState": {
 "status": "string",
 "statusDetails": {
 "string": "string"
 },
 "versionNumber": "long"
 },
 "jobDocument": "string"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome           | Tipo              | Descrizione                |
|----------------|-------------------|----------------------------|
| executionState | JobExecutionState | Oggetto JobExecutionState. |

| Nome          | Tipo                            | Descrizione                                                                                                                                                                                                                                                     |
|---------------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| stato         | Stringa                         | <p>Stato dell'esecuzione del processo. Può essere "QUEUED", "IN_PROGRESS", "FAILED", "SUCCESS", "CANCELED", "TIMED_OUT", "REJECTED" o "REMOVED".</p> <p>Enumerazione: QUEUED   IN_PROGRESS   SUCCEEDED   FAILED   TIMED_OUT   REJECTED   REMOVED   CANCELED</p> |
| statusDetails | mappa                           | Raccolta di coppie nome/valore che descrivono lo stato dell'esecuzione del processo.                                                                                                                                                                            |
| versionNumber | Long                            | Versione dell'esecuzione del processo. Le versioni delle esecuzioni dei processi vengono incrementate ogni volta che vengono aggiornate da un dispositivo.                                                                                                      |
| jobDocument   | Stringa<br>Lunghezza max: 32768 | Contenuto dei documenti dei processi.                                                                                                                                                                                                                           |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `ResourceNotFoundException`

La risorsa specificata non esiste.

##### `ThrottlingException`

La velocità supera il limite.

##### `ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

##### `CertificateValidationException`

Il certificato non è valido.

##### `InvalidStateTransitionException`

Un aggiornamento ha tentato di modificare l'esecuzione del processo impostando uno stato non valido in base allo stato corrente dell'esecuzione del processo (ad esempio, un tentativo di modificare una richiesta con stato SUCCESS impostando lo stato IN\_PROGRESS). In questo caso, il corpo del messaggio di errore contiene anche il campo executionState.

# UpdateRoleAlias

Aggiorna un alias del ruolo.

Riepilogo

```
aws iot update-role-alias \
--role-alias <value> \
[--role-arn <value>] \
[--credential-duration-seconds <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di **cli-input-json**

```
{
 "roleAlias": "string",
 "roleArn": "string",
 "credentialDurationSeconds": "integer"
}
```

Campi di **cli-input-json**

| Nome                      | Tipo                                                               | Descrizione                                      |
|---------------------------|--------------------------------------------------------------------|--------------------------------------------------|
| roleAlias                 | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=@-]+ | Alias del ruolo da aggiornare.                   |
| roleArn                   | Stringa<br><br>Lunghezza max: 2048, min.: 20                       | ARN del ruolo.                                   |
| credentialDurationSeconds | intero<br><br>Intervallo – Max: 3600, min.: 900                    | Numero di secondi di validità della credenziale. |

Output

```
{
 "roleAlias": "string",
 "roleAliasArn": "string"
}
```

Campi di output dell'interfaccia a riga di comando

| Nome         | Tipo                                                               | Descrizione               |
|--------------|--------------------------------------------------------------------|---------------------------|
| roleAlias    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [w=@-]+ | Alias del ruolo.          |
| roleAliasArn | Stringa                                                            | ARN dell'alias del ruolo. |

## Errori

**ResourceNotFoundException**

La risorsa specificata non esiste.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

## UpdateScheduledAudit

Aggiorna un audit pianificato, inclusi i controlli eseguiti e la frequenza di esecuzione dell'audit.

### Riepilogo

```
aws iot update-scheduled-audit \
[--frequency <value>] \
[--day-of-month <value>] \
[--day-of-week <value>] \
[--target-check-names <value>] \
--scheduled-audit-name <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "frequency": "string",
 "dayOfMonth": "string",
 "dayOfWeek": "string",
 "targetCheckNames": [
 "string"
],
 "scheduledAuditName": "string"
}
```

### Campi di cli-input-json

| Nome      | Tipo    | Descrizione                                                                                                                                                               |
|-----------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| frequenza | Stringa | Frequenza di esecuzione dell'audit. I valori possibili sono "DAILY", "WEEKLY", "BIWEEKLY" o "MONTHLY". L'ora di inizio effettiva di ogni audit è determinata dal sistema. |

| Nome               | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                       |
|--------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    |                                                                              | enumerazione: DAILY   WEEKLY   BIWEEKLY   MONTHLY                                                                                                                                                                                                                                                                                                 |
| dayOfMonth         | Stringa<br><br>modello: ^([1-9] [12][0-9] 3[01])\$ ^LAST\$                   | Giorno del mese in cui viene eseguito l'audit pianificato. Il valore può essere compreso tra "1" e "31" oppure può essere "LAST". Questo campo è obbligatorio se il parametro "frequency" è impostato su "MONTHLY". Se vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese. |
| dayOfWeek          | Stringa                                                                      | Giorno della settimana in cui viene eseguito l'audit pianificato. I valori possibili sono "SUN", "MON", "TUE", "WED", "THU", "FRI" o "SAT". Questo campo è obbligatorio se il parametro "frequency" è impostato su "WEEKLY" o "BIWEEKLY".<br><br>enumerazione: SUN   MON   TUE   WED   THU   FRI   SAT                                            |
| targetCheckNames   | elenco<br><br>membro: AuditCheckName                                         | Controlli eseguiti durante l'audit pianificato. I controlli devono essere abilitati per l'account. Usa <a href="#">DescribeAccountAuditConfiguration</a> per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati, o <a href="#">UpdateAccountAuditConfiguration</a> per selezionare i controlli abilitati.                       |
| scheduledAuditName | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _-]+ | Nome dell'audit pianificato. Massimo 128 caratteri.                                                                                                                                                                                                                                                                                               |

## Output

```
{
 "scheduledAuditArn": "string"
}
```

## Campi di output dell'interfaccia a riga di comando

| Nome              | Tipo    | Descrizione                 |
|-------------------|---------|-----------------------------|
| scheduledAuditArn | Stringa | ARN dell'audit pianificato. |

## Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ResourceNotFoundException**

La risorsa specificata non esiste.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

# UpdateSecurityProfile

Aggiorna un profilo di sicurezza di Device Defender.

## Riepilogo

```
aws iot update-security-profile \
--security-profile-name <value> \
[--security-profile-description <value>] \
[--behaviors <value>] \
[--alert-targets <value>] \
[--additional-metrics-to-retain <value>] \
[--delete-behaviors | --no-delete-behaviors] \
[--delete-alert-targets | --no-delete-alert-targets] \
[--delete-additional-metrics-to-retain | --no-delete-additional-metrics-to-retain] \
[--expected-version <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "securityProfileName": "string",
 "securityProfileDescription": "string",
 "behaviors": [
 {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 },
 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "statistic": "string"
 }
 }
 }
}
```

```

 },
],
 "alertTargets": {
 "string": {
 "alertTargetArn": "string",
 "roleArn": "string"
 }
 },
 "additionalMetricsToRetain": [
 "string"
],
 "deleteBehaviors": "boolean",
 "deleteAlertTargets": "boolean",
 "deleteAdditionalMetricsToRetain": "boolean",
 "expectedVersion": "long"
 }
}

```

### Campi di **cli-input-json**

| Nome                       | Tipo                                                                       | Descrizione                                                                                                                                                                                                                    |
|----------------------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| securityProfileName        | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z0-9:_-]+ | Nome del profilo di sicurezza da aggiornare.                                                                                                                                                                                   |
| securityProfileDescription | Stringa<br><br>Lunghezza max: 1000<br><br>Modello: [\p{Graph}]*            | Descrizione del profilo di sicurezza.                                                                                                                                                                                          |
| behaviors                  | elenco<br><br>membro: Behavior                                             | Specifica i comportamenti che, quando violati da un dispositivo (oggetto), causano la generazione di un avviso.                                                                                                                |
| name                       | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z0-9:_-]+ | Nome assegnato al comportamento.                                                                                                                                                                                               |
| metric                     | Stringa                                                                    | Valore misurato dal comportamento.                                                                                                                                                                                             |
| criteria                   | BehaviorCriteria                                                           | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a metric.                                                                                                                             |
| comparisonOperator         | Stringa                                                                    | Operatore che mette in correlazione l'oggetto misurato (metric) e i criteri (contenenti un value o statisticalThreshold).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set |

| Nome                         | Tipo                                    | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              |                                         | not-in-cidr-set   in-port-set   not-in-port-set                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| value                        | MetricValue                             | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count                        | Long<br>Intervallo - min.: 0            | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cids                         | elenco<br>membro: Cidr                  | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports                        | elenco<br>membro: Port                  | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds              | intero                                  | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |
| consecutiveDatapointsToAlarm | intero<br>Intervallo – Max: 10, min.: 1 | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                      |

| Nome                         | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| consecutiveDatapointsToClear | intero<br><br>Intervallo – Max: 10, min.: 1                                  | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| statisticalThreshold         | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistic                    | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato ( <code>durationSeconds</code> ) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto ( <code>comparisonOperator</code> ) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario si verifica una violazione. |
| alertTargets                 | mappa                                                                        | Destinazione di invio degli avvisi. Gli avvisi vengono sempre inviati alla console.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| alertTargetArn               | Stringa                                                                      | ARN del target di notifica a cui vengono inviati gli avvisi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| roleArn                      | Stringa<br><br>Lunghezza max: 2048, min.: 20                                 | ARN del ruolo che concede l'autorizzazione per l'invio degli avvisi al target di notifica.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Nome                            | Tipo                             | Descrizione                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| additionalMetricsToRetain       | elenco<br>membro: BehaviorMetric | Un elenco di parametri i cui dati vengono conservati (archiviati). Per impostazione predefinita, i dati vengono conservati per qualsiasi parametro utilizzato nel behaviors del profilo ma vengono anche conservati per qualsiasi parametro specificato qui. |
| deleteBehaviors                 | booleano                         | Se true, elimina tutti i behaviors definiti per questo profilo di sicurezza. Se esistono behaviors definiti nell'invocazione corrente, si verifica un'eccezione.                                                                                             |
| deleteAlertTargets              | booleano                         | Se true, elimina tutti i alertTargets definiti per questo profilo di sicurezza. Se esistono alertTargets definiti nell'invocazione corrente, si verifica un'eccezione.                                                                                       |
| deleteAdditionalMetricsToRetain | booleano                         | Se true, elimina tutti i additionalMetricsToRetain definiti per questo profilo di sicurezza. Se esistono additionalMetricsToRetain definiti nell'invocazione corrente, si verifica un'eccezione.                                                             |
| expectedVersion                 | Long                             | Versione prevista del profilo di sicurezza. Viene generata una nuova versione ogni volta che il profilo di sicurezza viene aggiornato. Se specifichi un valore diverso dalla versione effettiva, viene generata un'eccezione VersionConflictException.       |

## Output

```
{
 "securityProfileName": "string",
 "securityProfileArn": "string",
 "securityProfileDescription": "string",
 "behaviors": [
 {
 "name": "string",
 "metric": "string",
 "criteria": {
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "unit": "string"
 }
 }
 }
]
}
```

```

 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
},
"durationSeconds": "integer",
"consecutiveDatapointsToAlarm": "integer",
"consecutiveDatapointsToClear": "integer",
"statisticalThreshold": {
 "statistic": "string"
}
}
],
"alertTargets": {
 "string": {
 "alertTargetArn": "string",
 "roleArn": "string"
 }
},
"additionalMetricsToRetain": [
 "string"
],
"version": "long",
"creationDate": "timestamp",
"lastModifiedDate": "timestamp"
}

```

#### Campi di output dell'interfaccia a riga di comando

| Nome                       | Tipo                                                               | Descrizione                                                                                                     |
|----------------------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| securityProfileName        | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-zA-Z0-9:_-]+ | Nome del profilo di sicurezza aggiornato.                                                                       |
| securityProfileArn         | Stringa                                                            | ARN del profilo di sicurezza aggiornato.                                                                        |
| securityProfileDescription | Stringa<br>Lunghezza max: 1000<br>Modello: [\p{Graph}]*            | Descrizione del profilo di sicurezza.                                                                           |
| behaviors                  | elenco<br>membro: Behavior                                         | Specifica i comportamenti che, quando violati da un dispositivo (oggetto), causano la generazione di un avviso. |
| name                       | Stringa<br>Lunghezza max: 128, min.: 1<br>Modello: [a-zA-Z0-9:_-]+ | Nome assegnato al comportamento.                                                                                |
| metric                     | Stringa                                                            | Valore misurato dal comportamento.                                                                              |

| Nome               | Tipo                             | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| criteria           | BehaviorCriteria                 | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| comparisonOperator | Stringa                          | Operatore che mette in correlazione l'oggetto misurato ( <code>metric</code> ) e i criteri (contenenti un <code>value</code> o <code>statisticalThreshold</code> ).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set                                                                                                                                                                                                                                                            |
| value              | MetricValue                      | Valore da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| count              | Long<br><br>Intervallo - min.: 0 | Se <code>comparisonOperator</code> richiede un valore numerico, usa questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cidrs              | elenco<br><br>membro: Cidr       | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports              | elenco<br><br>membro: Port       | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds    | intero                           | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |

| Nome                         | Tipo                                                                         | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| consecutiveDatapointsToAlarm | intero<br><br>Intervallo – Max: 10, min.: 1                                  | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| consecutiveDatapointsToClear | intero<br><br>Intervallo – Max: 10, min.: 1                                  | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| statisticalThreshold         | StatisticalThreshold                                                         | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistic                    | Stringa<br><br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato ( <code>durationSeconds</code> ) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto ( <code>comparisonOperator</code> ) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario si verifica una violazione. |
| alertTargets                 | mappa                                                                        | Destinazione di invio degli avvisi. Gli avvisi vengono sempre inviati alla console.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| alertTargetArn               | Stringa                                                                      | ARN del target di notifica a cui vengono inviati gli avvisi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Nome                      | Tipo                                     | Descrizione                                                                                                                                                                                                                                                               |
|---------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| roleArn                   | Stringa<br>Lunghezza max: 2048, min.: 20 | ARN del ruolo che concede l'autorizzazione per l'invio degli avvisi al target di notifica.                                                                                                                                                                                |
| additionalMetricsToRetain | elenco<br>membro: BehaviorMetric         | Un elenco di parametri i cui dati vengono conservati (archiviati). Per impostazione predefinita, i dati vengono conservati per qualsiasi parametro utilizzato nei behaviors del profilo di sicurezza ma vengono anche conservati per qualsiasi parametro specificato qui. |
| versione                  | Long                                     | Versione aggiornata del profilo di sicurezza.                                                                                                                                                                                                                             |
| creationDate              | timestamp                                | Ora della creazione del profilo di sicurezza.                                                                                                                                                                                                                             |
| lastModifiedDate          | timestamp                                | Ora dell'ultima modifica del profilo di sicurezza.                                                                                                                                                                                                                        |

#### Errori

##### InvalidRequestException

I contenuti della richiesta non sono validi.

##### ResourceNotFoundException

La risorsa specificata non esiste.

##### VersionConflictException

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

##### ThrottlingException

La velocità supera il limite.

##### InternalFailureException

Si è verificato un errore imprevisto.

## UpdateStream

Aggiorna un flusso esistente. La versione del flusso verrà incrementata di uno.

#### Riepilogo

```
aws iot update-stream \
--stream-id <value> \
[--description <value>] \
[--files <value>] \
```

```
[--role-arn <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

#### Formato di cli-input-json

```
{
 "streamId": "string",
 "description": "string",
 "files": [
 {
 "fileId": "integer",
 "s3Location": {
 "bucket": "string",
 "key": "string",
 "version": "string"
 }
 }
],
 "roleArn": "string"
}
```

#### Campi di **cli-input-json**

| Nome        | Tipo                                                                        | Descrizione                                                                              |
|-------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| streamId    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 _]+ | ID flusso.                                                                               |
| description | Stringa<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+                | Descrizione del flusso.                                                                  |
| files       | elenco<br><br>Membro: StreamFile                                            | File associati al flusso.                                                                |
| fileId      | intero<br><br>Intervallo – Max: 255, min.: 0                                | ID file.                                                                                 |
| s3Location  | S3Location                                                                  | Posizione del file in S3.                                                                |
| bucket      | Stringa<br><br>Lunghezza min.: 1                                            | Bucket S3.                                                                               |
| key         | Stringa<br><br>Lunghezza min.: 1                                            | La chiave S3.                                                                            |
| versione    | Stringa                                                                     | Versione del bucket S3                                                                   |
| roleArn     | Stringa<br><br>Lunghezza max: 2048, min.: 20                                | Ruolo IAM che l'entità principale del servizio IoT può assumere per accedere ai file S3. |

## Output

```
{
 "streamId": "string",
 "streamArn": "string",
 "description": "string",
 "streamVersion": "integer"
}
```

## Campi di output dell'interfaccia a riga di comando

| Nome          | Tipo    | Descrizione                                                                    |
|---------------|---------|--------------------------------------------------------------------------------|
| streamId      | Stringa | ID flusso.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a–z A–Z 0–9 _]+ |
| streamArn     | Stringa | ARN del flusso.                                                                |
| description   | Stringa | Descrizione del flusso.<br><br>Lunghezza max: 2028<br><br>Modello: [^\p{C}]+   |
| streamVersion | intero  | Versione del flusso.<br><br>Intervallo – Max: 65535, min.: 0                   |

## Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceNotFoundException`

La risorsa specificata non esiste.

`ThrottlingException`

La velocità supera il limite.

`UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

`InternalFailureException`

Si è verificato un errore imprevisto.

# UpdateThing

Aggiorna i dati per un oggetto.

## Riepilogo

```
aws iot update-thing \
--thing-name <value> \
[--thing-type-name <value>] \
[--attribute-payload <value>] \
[--expected-version <value>] \
[--remove-thing-type | --no-remove-thing-type] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

## Formato di cli-input-json

```
{
 "thingName": "string",
 "thingTypeName": "string",
 "attributePayload": {
 "attributes": {
 "string": "string"
 },
 "merge": "boolean"
 },
 "expectedVersion": "long",
 "removeThingType": "boolean"
}
```

## Campi di **cli-input-json**

| Nome             | Tipo                                                                          | Descrizione                                                                                                                                                                                                                                               |
|------------------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingName        | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome dell'oggetto da aggiornare.                                                                                                                                                                                                                          |
| thingTypeName    | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome del tipo di oggetto.                                                                                                                                                                                                                                 |
| attributePayload | AttributePayload                                                              | Elenco di attributi dell'oggetto in una stringa JSON che contiene coppie nome/valore. Ad esempio:<br><br><b>\"attributes\": {\"name1\": \"value2\"}</b><br><br>Questi dati vengono usati per aggiungere nuovi attributi o aggiornare attributi esistenti. |
| attributes       | mappa                                                                         | Stringa JSON contenente fino a tre coppie chiave/valore in formato JSON. Ad esempio:<br><br><b>\"attributes\": {\"string1\": \"string2\"}</b>                                                                                                             |

| Nome            | Tipo     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| merge           | booleano | <p>Specifica se l'elenco di attributi fornito in <code>AttributePayload</code> deve essere unito agli attributi archiviati nel registro, anziché sovrascrivere questi ultimi.</p> <p>Per rimuovere un attributo, chiama <code>UpdateThing</code> con un valore di attributo vuoto.</p> <p><b>Note</b></p> <p>L'attributo <code>merge</code> è valido solo quando chiavi <code>UpdateThing</code>.</p> |
| expectedVersion | Long     | Versione prevista del record dell'oggetto nel registro. Se la versione del record nel registro non corrisponde alla versione prevista specificata nella richiesta, la richiesta <code>UpdateThing</code> viene rifiutata con <code>VersionConflictException</code> .                                                                                                                                  |
| removeThingType | booleano | Rimuove l'associazione a un tipo di oggetto. Se è true, l'associazione viene rimossa.                                                                                                                                                                                                                                                                                                                 |

#### Output

Nessuna

#### Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`VersionConflictException`

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro --version.

`ThrottlingException`

La velocità supera il limite.

`UnauthorizedException`

Non hai le autorizzazioni necessarie per eseguire questa operazione.

`ServiceUnavailableException`

Il servizio è temporaneamente non disponibile.

`InternalFailureException`

Si è verificato un errore imprevisto.

**ResourceNotFoundException**

La risorsa specificata non esiste.

## UpdateThingGroup

Aggiorna un gruppo di oggetti.

### Riepilogo

```
aws iot update-thing-group \
--thing-group-name <value> \
--thing-group-properties <value> \
[--expected-version <value>] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di `cli-input-json`

```
{
 "thingGroupName": "string",
 "thingGroupProperties": {
 "thingGroupDescription": "string",
 "attributePayload": {
 "attributes": {
 "string": "string"
 },
 "merge": "boolean"
 }
 },
 "expectedVersion": "long"
}
```

### Campi di `cli-input-json`

| Nome                  | Tipo                 | Descrizione                                                                                         |
|-----------------------|----------------------|-----------------------------------------------------------------------------------------------------|
| thingGroupName        | Stringa              | Gruppo di oggetti da aggiornare.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z0-9:_-]+ |
| thingGroupProperties  | ThingGroupProperties | Proprietà del gruppo di oggetti.                                                                    |
| thingGroupDescription | Stringa              | Descrizione del gruppo di oggetti.<br><br>Lunghezza max: 2028<br><br>Modello: [\p{Graph}]*          |
| attributePayload      | AttributePayload     | Attributi del gruppo di oggetti in formato JSON.                                                    |
| attributes            | mappa                | Stringa JSON contenente fino a tre coppie chiave/valore in formato JSON. Ad esempio:                |

| Nome            | Tipo     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |          | <pre>\\"attributes\\":\n{\\"string1\\":\n\\"string2\\\"}</pre>                                                                                                                                                                                                                                                                                                                                        |
| merge           | booleano | <p>Specifica se l'elenco di attributi fornito in <code>AttributePayload</code> deve essere unito agli attributi archiviati nel registro, anziché sovrascrivere questi ultimi.</p> <p>Per rimuovere un attributo, chiama <code>UpdateThing</code> con un valore di attributo vuoto.</p> <p><b>Note</b></p> <p>L'attributo <code>merge</code> è valido solo quando chiavi <code>UpdateThing</code>.</p> |
| expectedVersion | Long     | Versione prevista del gruppo di oggetti. Se non corrisponde alla versione del gruppo di oggetti in fase di aggiornamento, l'aggiornamento non riesce.                                                                                                                                                                                                                                                 |

#### Output

```
{
 "version": "long"
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome     | Tipo | Descrizione                                |
|----------|------|--------------------------------------------|
| versione | Long | Versione del gruppo di oggetti aggiornato. |

#### Errori

##### `InvalidRequestException`

I contenuti della richiesta non sono validi.

##### `VersionConflictException`

Eccezione generata quando la versione di un oggetto passato a un comando è diversa dalla versione specificata con il parametro `--version`.

##### `ThrottlingException`

La velocità supera il limite.

##### `InternalFailureException`

Si è verificato un errore imprevisto.

ResourceNotFoundException

La risorsa specificata non esiste.

## UpdateThingGroupsForThing

Aggiorna i gruppi cui appartiene l'oggetto.

### Riepilogo

```
aws iot update-thing-groups-for-thing \
[--thing-name <value>] \
[--thing-groups-to-add <value>] \
[--thing-groups-to-remove <value>] \
[--override-dynamic-groups | --no-override-dynamic-groups] \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

### Formato di cli-input-json

```
{
 "thingName": "string",
 "thingGroupsToAdd": [
 "string"
],
 "thingGroupsToRemove": [
 "string"
],
 "overrideDynamicGroups": "boolean"
}
```

### Campi di **cli-input-json**

| Nome                  | Tipo    | Descrizione                                                                                                                                                                                                                                                                                                                       |
|-----------------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| thingName             | Stringa | Oggetto le cui appartenenze ai gruppi verranno aggiornate.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+                                                                                                                                                                                                  |
| thingGroupsToAdd      | elenco  | Gruppi cui verrà aggiunto l'oggetto.<br><br>Membro: ThingGroupName                                                                                                                                                                                                                                                                |
| thingGroupsToRemove   | elenco  | Gruppi da cui verrà rimosso l'oggetto.<br><br>Membro: ThingGroupName                                                                                                                                                                                                                                                              |
| overrideDynamicGroups | boolean | Sostituisce i gruppi di oggetti dinamici con gruppi di oggetti statici quando viene raggiunto il limite di 10 oggetti per gruppo. Se un oggetto appartiene a gruppi di 10 oggetti e uno o più gruppi sono gruppi di oggetti dinamici, l'aggiunta di un oggetto a un gruppo statico rimuove l'oggetto dall'ultimo gruppo dinamico. |

Output

Nessuna

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.

**ResourceNotFoundException**

La risorsa specificata non esiste.

## UpdateThingShadow

Aggiorna la copia shadow per l'oggetto specificato.

Per ulteriori informazioni, consulta [UpdateThingShadow](#) nella Guida per lo sviluppatore di AWS IoT.

Riepilogo

```
aws iot-data update-thing-shadow \
 --thing-name <value> \
 --payload <value> \
 [--cli-input-json <value>] \
 [--generate-cli-skeleton]
```

Formato di `cli-input-json`

```
{
 "thingName": "string",
 "payload": "blob"
}
```

Campi di `cli-input-json`

| Nome      | Tipo    | Descrizione                                                                           |
|-----------|---------|---------------------------------------------------------------------------------------|
| thingName | Stringa | Nome dell'oggetto.<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-zA-Z0-9:_-]+ |
| payload   | blob    | Informazioni sullo stato, in formato JSON.                                            |

Output

```
{
 "payload": "blob"
```

}

Campi di output dell'interfaccia a riga di comando

| Nome    | Tipo | Descrizione                                |
|---------|------|--------------------------------------------|
| payload | blob | Informazioni sullo stato, in formato JSON. |

Errori

**ConflictException**

La versione specificata non corrisponde alla versione del documento.

**RequestEntityTooLargeException**

Il payload supera le dimensioni massime permesse.

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**UnauthorizedException**

Non hai le autorizzazioni necessarie per eseguire questa operazione.

**ServiceUnavailableException**

Il servizio è temporaneamente non disponibile.

**InternalFailureException**

Si è verificato un errore imprevisto.

**MethodNotAllowedException**

La combinazione specificata di verbo HTTP e URI non è supportata.

**UnsupportedDocumentEncodingException**

La codifica non è supportata.

## ValidateSecurityProfileBehaviors

Convalida la specifica dei comportamenti dei profili di sicurezza di Device Defender.

Riepilogo

```
aws iot validate-security-profile-behaviors \
--behaviors <value> \
[--cli-input-json <value>] \
[--generate-cli-skeleton]
```

Formato di cli-input-json

```
{
 "behaviors": [
 {
 "name": "string",
 "metric": "string",
```

```

 "criteria": [
 "comparisonOperator": "string",
 "value": {
 "count": "long",
 "cidrs": [
 "string"
],
 "ports": [
 "integer"
]
 },
 "durationSeconds": "integer",
 "consecutiveDatapointsToAlarm": "integer",
 "consecutiveDatapointsToClear": "integer",
 "statisticalThreshold": {
 "statistic": "string"
 }
 }
]
}

```

#### Campi di **cli-input-json**

| Nome               | Tipo                                                                          | Descrizione                                                                                                                                                                                                                                                                                              |
|--------------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| behaviors          | elenco<br><br>membro: Behavior                                                | Specifica i comportamenti che, quando violati da un dispositivo (oggetto), causano la generazione di un avviso.                                                                                                                                                                                          |
| name               | Stringa<br><br>Lunghezza max: 128, min.: 1<br><br>Modello: [a-z A-Z 0-9 :_-]+ | Nome assegnato al comportamento.                                                                                                                                                                                                                                                                         |
| metric             | Stringa                                                                       | Valore misurato dal comportamento.                                                                                                                                                                                                                                                                       |
| criteria           | BehaviorCriteria                                                              | Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a <b>metric</b> .                                                                                                                                                                                               |
| comparisonOperator | Stringa                                                                       | Operatore che mette in correlazione l'oggetto misurato ( <b>metric</b> ) e i criteri (contenenti un <b>value</b> o <b>statisticalThreshold</b> ).<br><br>enumerazione: less-than   less-than-equals   greater-than   greater-than-equals   in-cidr-set   not-in-cidr-set   in-port-set   not-in-port-set |
| value              | MetricValue                                                                   | Valore da confrontare con <b>metric</b> .                                                                                                                                                                                                                                                                |
| count              | Long                                                                          | Se <b>comparisonOperator</b> richiede un valore numerico, usa                                                                                                                                                                                                                                            |

| Nome                         | Tipo                                    | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | Intervallo - min.: 0                    | questo parametro per specificare il valore numerico da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| cidrs                        | elenco<br>membro: Cidr                  | Se <code>comparisonOperator</code> richiede un set di CIDR, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ports                        | elenco<br>membro: Port                  | Se <code>comparisonOperator</code> richiede un set di porte, usa questo parametro per specificare il set da confrontare con <code>metric</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| durationSeconds              | intero                                  | Usa questo parametro per specificare il periodo di tempo durante il quale viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, <code>NUM_MESSAGES_SENT</code> ). Per un confronto di parametri <code>statisticalThreshold</code> , le misurazioni da tutti i dispositivi vengono accumulate nell'arco di questa durata prima di essere utilizzate per calcolare percentili e in seguito, misurazioni da un singolo dispositivo vengono pure accumulate nell'arco di questa durata prima che venga assegnata una classificazione percentile. |
| consecutiveDatapointsToAlarm | intero<br>Intervallo – Max: 10, min.: 1 | Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                                                                      |
| consecutiveDatapointsToClear | intero<br>Intervallo – Max: 10, min.: 1 | Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.                                                                                                                                                                                                                                                                                                                                   |

| Nome                 | Tipo                                                                     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| statisticalThreshold | StatisticalThreshold                                                     | Una classificazione statistica (percentile) che indica un valore di soglia in base al quale un comportamento viene considerato conforme al comportamento o in violazione dello stesso.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistic            | Stringa<br>modello: (p0 p0.1 p0.01 p1 p10 p50 p90 p99 p99.9 p99.99 p100) | Il percentile che restituisce un valore di soglia in base al quale viene determinata la conformità con un comportamento. I parametri vengono raccolti nell'arco del periodo specificato ( <code>durationSeconds</code> ) da tutti i dispositivi di segnalazione nell'account e vengono calcolate classificazioni statistiche. Quindi, le misurazioni da un dispositivo vengono raccolte nell'arco dello stesso periodo. Se le misurazioni accumulate dal dispositivo sono sopra o sotto ( <code>comparisonOperator</code> ) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento, in caso contrario si verifica una violazione. |

#### Output

```
{
 "valid": "boolean",
 "validationErrors": [
 {
 "errorMessage": "string"
 }
]
}
```

#### Campi di output dell'interfaccia a riga di comando

| Nome             | Tipo                              | Descrizione                                         |
|------------------|-----------------------------------|-----------------------------------------------------|
| valid            | booleano                          | True se i comportamenti sono validi.                |
| validationErrors | elenco<br>membro: ValidationError | Elenco degli errori trovati nei comportamenti.      |
| errorMessage     | Stringa<br>Lunghezza max: 2048    | Descrizione di un errore trovato nei comportamenti. |

Errori

**InvalidRequestException**

I contenuti della richiesta non sono validi.

**ThrottlingException**

La velocità supera il limite.

**InternalFailureException**

Si è verificato un errore imprevisto.