



Guida per l'utente

# EventBridge Pianificatore



# EventBridge Pianificatore: Guida per l'utente

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

---

# Table of Contents

Che cos'è EventBridge Scheduler? .....	1
Caratteristiche principali di Scheduler EventBridge .....	1
EventBridge Accesso a Scheduler .....	2
Configurazione .....	3
Iscriviti per AWS .....	3
Creazione di un utente IAM .....	3
Utilizza politiche gestite .....	4
Configurare il ruolo di esecuzione .....	5
Configura un bersaglio .....	9
Fasi successive .....	12
Nozioni di base .....	13
Prerequisiti .....	14
Utilizzo della console .....	14
Utilizzando il AWS CLI .....	18
Usando il SDKs .....	18
Fasi successive .....	20
Tipi di pianificazione .....	21
Pianificazioni basate sulle tariffe .....	22
Sintassi .....	22
Esempi .....	22
Pianificazioni basate su CRON .....	23
Sintassi .....	23
Esempi .....	24
Pianificazioni una tantum .....	25
Sintassi .....	25
Esempi .....	25
Fusi orari .....	26
Ora legale .....	26
Gestire una pianificazione .....	28
Modifica dello stato della pianificazione .....	29
Configurazione di finestre temporali flessibili .....	30
Configurazione di un DLQ .....	31
Crea una SQS coda Amazon .....	32
Imposta le autorizzazioni per i ruoli di esecuzione .....	33

Specificate una coda di lettere non scritte .....	33
Recupera l'evento con lettera morta .....	35
Eliminazione di una pianificazione .....	37
Eliminazione dopo il completamento della pianificazione .....	38
Eliminazione manuale .....	39
Fasi successive .....	40
Gestione di un gruppo di pianificazioni .....	41
Creazione di un gruppo di pianificazione .....	42
Fase uno: creare un nuovo gruppo di pianificazioni .....	42
Associazione di una pianificazione .....	44
Eliminazione di un gruppo di pianificazioni .....	45
Risorse correlate .....	47
Gestione degli obiettivi .....	48
Utilizzo di obiettivi basati su modelli .....	49
Amazon SQS SendMessage .....	50
Lambda Invoke .....	52
Step Functions StartExecution .....	54
Utilizzo di obiettivi universali .....	56
Azioni non supportate .....	56
Esempi .....	57
Aggiungere attributi di contesto .....	59
Fasi successive .....	60
Sicurezza .....	61
Gestione dell'accesso .....	61
Destinatari .....	62
Autenticazione con identità .....	63
Gestione dell'accesso con policy .....	66
Integrazione con IAM .....	69
Utilizzo di policy basate su identità .....	76
Prevenzione del "confused deputy" .....	87
Risoluzione dei problemi .....	88
Protezione dei dati .....	90
Crittografia a riposo .....	91
Crittografia in transito .....	100
Convalida della conformità .....	100
Resilienza .....	101

---

Sicurezza dell'infrastruttura .....	102
Monitoraggio e metriche .....	103
Monitoraggio con CloudWatch .....	103
Termini .....	104
Dimensioni .....	104
Accesso ai parametri .....	105
Elenco delle metriche .....	105
Parametri di utilizzo .....	112
Monitoraggio con log CloudTrail .....	114
EventBridge Informazioni sullo scheduler in CloudTrail .....	115
Informazioni sulle voci EventBridge dei file di registro di Scheduler .....	116
Quote .....	117
Risoluzione dei problemi relativi alle quote .....	121
ServiceQuotaExceededException .....	121
Cronologia dei documenti .....	124
.....	cxxvii

# Cos'è Amazon EventBridge Scheduler?

Amazon EventBridge Scheduler è uno strumento di pianificazione senza server che consente di creare, eseguire e gestire attività da un unico servizio gestito centralizzato. Altamente scalabile, EventBridge Scheduler ti consente di pianificare milioni di attività che possono richiamare più di 270 AWS servizi e oltre 6.000 operazioni. API Senza la necessità di fornire e gestire l'infrastruttura o di integrarsi con più servizi, EventBridge Scheduler offre la possibilità di fornire pianificazioni su larga scala e ridurre i costi di manutenzione.

EventBridge Scheduler esegue le attività in modo affidabile, con meccanismi integrati che regolano le pianificazioni in base alla disponibilità degli obiettivi a valle. Con EventBridge Scheduler, puoi creare pianificazioni utilizzando le espressioni cron e rate per schemi ricorrenti o configurare chiamate una tantum. È possibile impostare finestre temporali flessibili per la consegna, definire limiti di nuovi tentativi e impostare il tempo massimo di conservazione per i trigger non riusciti.

## Argomenti

- [Caratteristiche principali di Scheduler EventBridge](#)
- [EventBridge Accesso a Scheduler](#)

## Caratteristiche principali di Scheduler EventBridge

EventBridge Scheduler offre le seguenti funzionalità chiave che è possibile utilizzare per configurare gli obiettivi e scalare le pianificazioni.

- Target basati su modelli: EventBridge Scheduler supporta obiettivi basati su modelli per eseguire operazioni comuni utilizzando Amazon, API SQS Amazon, SNS Lambda e. EventBridge Con obiettivi predefiniti, puoi configurare rapidamente le tue pianificazioni utilizzando la console Scheduler, EventBridge Scheduler o. EventBridge SDK AWS CLI
- Obiettivi universali: EventBridge Scheduler fornisce un parametro di destinazione universale (UTP) che puoi utilizzare per creare trigger personalizzati destinati a più di 270 AWS servizi e oltre API 6.000 operazioni in base a una pianificazione. ConUTP, puoi configurare i tuoi trigger personalizzati utilizzando la console Scheduler, EventBridge Scheduler o. EventBridge SDK AWS CLI
- Finestre temporali flessibili: EventBridge Scheduler supporta finestre temporali flessibili, che consentono di disperdere le pianificazioni e migliorare l'affidabilità dei trigger per i casi d'uso che non richiedono una chiamata programmata precisa degli obiettivi.

- **Tentativi:** EventBridge Scheduler fornisce at-least-once l'invio di eventi agli obiettivi, il che significa che almeno una consegna ha esito positivo con una risposta dalla destinazione. EventBridge Scheduler consente di impostare il numero di nuovi tentativi per la pianificazione di un'attività non riuscita. EventBridge Scheduler riprova le attività non riuscite con tentativi ritardati per migliorare l'affidabilità della pianificazione e garantire la disponibilità degli obiettivi.

## EventBridge Accesso a Scheduler

È possibile utilizzare EventBridge Scheduler tramite la EventBridge console, lo EventBridge SchedulerSDK, il AWS CLI, o utilizzando direttamente lo Scheduler. EventBridge API

# Configurazione di Amazon EventBridge Scheduler

Prima di poter utilizzare EventBridge Scheduler, è necessario completare i seguenti passaggi.

Argomenti

- [Iscriviti per AWS](#)
- [Creazione di un utente IAM](#)
- [Utilizza politiche gestite](#)
- [Configurare il ruolo di esecuzione](#)
- [Configura un bersaglio](#)
- [Fasi successive](#)

## Iscriviti per AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la <https://portal.aws.amazon.com/billing/registrazione>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i AWS servizi nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

## Creazione di un utente IAM

Per creare un utente amministratore, scegli una delle seguenti opzioni.

Scelta di un modo per gestire il tuo amministratore	Per	Come	Puoi anche
In IAM Identity Center  (Consigliato)	Usa credenziali a breve termine per accedere a AWS.  Ciò è in linea con le best practice per la sicurezza . Per informazioni sulle best practice, consulta la sezione <a href="#">Procedure consigliate per la sicurezza IAM nella Guida IAM per l'utente</a> .	Segui le istruzioni riportate in <a href="#">Nozioni di base</a> nella Guida per l'utente di AWS IAM Identity Center .	Configura l'accesso programmatico <a href="#">configurando l'uso AWS IAM Identity Center nella Guida AWS CLI per l'AWS Command Line Interface</a> utente.
In IAM  (Non consigliato)	Usa credenziali a lungo termine per accedere a AWS.	Seguendo le istruzioni riportate nella <a href="#">sezione Creazione del primo utente IAM amministratore e gruppo di utenti</a> nella Guida IAM per l'utente.	Configura l'accesso programmatico <a href="#">gestendo le chiavi di accesso per IAM gli utenti</a> nella Guida per l'IAM utente.

## Utilizza politiche gestite

Nel passaggio precedente, configuri un IAM utente con le credenziali per accedere alle tue AWS risorse. Nella maggior parte dei casi, per utilizzare EventBridge Scheduler in modo sicuro, si consiglia di creare utenti, gruppi o ruoli separati con solo le autorizzazioni necessarie per utilizzare Scheduler. EventBridge EventBridge Scheduler supporta le seguenti politiche gestite per casi d'uso comuni.

- [the section called “AmazonEventBridgeSchedulerFullAccess”](#)— Concede l'accesso completo a EventBridge Scheduler utilizzando la console e il. API
- [the section called “AmazonEventBridgeSchedulerReadOnlyAccess”](#)— Concede l'accesso in sola lettura a Scheduler. EventBridge

È possibile allegare queste politiche gestite ai IAM principali nello stesso modo in cui è stata allegata la AdministratorAccess politica nel passaggio precedente. Per ulteriori informazioni sulla gestione dell'accesso a EventBridge Scheduler utilizzando politiche basate sull'identità, IAM consulta. [the section called “Utilizzo di policy basate su identità”](#)

## Configurare il ruolo di esecuzione

Un ruolo di esecuzione è un IAM ruolo che EventBridge Scheduler assume per interagire con altri per conto dell'utente. AWS servizi A questo ruolo si allegano politiche di autorizzazione per concedere a EventBridge Scheduler l'accesso per richiamare gli obiettivi.

È inoltre possibile creare un nuovo ruolo di esecuzione quando si utilizza la console per [creare una nuova pianificazione](#). Se utilizzi la console, EventBridge Scheduler crea un ruolo per tuo conto con autorizzazioni basate sull'obiettivo scelto. Quando EventBridge Scheduler crea un ruolo per te, la politica di fiducia del ruolo include [chiavi di condizione](#) che limitano i responsabili che possono assumere il ruolo per tuo conto. In questo modo si evita la potenziale [confusione del problema della vice](#) sicurezza.

I passaggi seguenti descrivono come creare un nuovo ruolo di esecuzione e come concedere a EventBridge Scheduler l'accesso per richiamare una destinazione. Questo argomento descrive le autorizzazioni per gli obiettivi basati su modelli più diffusi. Per informazioni sull'aggiunta di autorizzazioni per altre destinazioni, consulta. [the section called “Utilizzo di obiettivi basati su modelli”](#)

Per creare un ruolo di esecuzione utilizzando il AWS CLI

1. Copia la seguente JSON politica di assunzione del ruolo e salvala localmente come Scheduler-Execution-Role.json. Questa politica di fiducia consente a EventBridge Scheduler di assumere il ruolo per tuo conto.

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

```
        "Effect": "Allow",
        "Principal": {
            "Service": "scheduler.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
    }
]
}
```

### Important

Per impostare un ruolo di esecuzione in un ambiente di produzione, consigliamo di implementare misure di protezione aggiuntive per evitare problemi confusi tra gli addetti ai lavori. Per ulteriori informazioni e un esempio di politica, vedere [the section called "Prevenzione del "confused deputy"](#).

2. Da AWS Command Line Interface (AWS CLI), immettete il seguente comando per creare un nuovo ruolo. Sostituiscilo *SchedulerExecutionRole* con il nome che vuoi assegnare a questo ruolo.

```
$ aws iam create-role --role-name SchedulerExecutionRole --assume-role-policy-document file://Scheduler-Execution-Role.json
```

In caso di successo, vedrai il seguente risultato:

```
{
  "Role": {
    "Path": "/",
    "RoleName": "Scheduler-Execution-Role",
    "RoleId": "BR1L2DZK3K4CTL5ZF9EIL",
    "Arn": "arn:aws:iam::123456789012:role/SchedulerExecutionRole",
    "CreateDate": "2022-03-10T18:45:01+00:00",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": "scheduler.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  }
}
```

```
    }
  ]
}
}
```

3. Per creare una nuova politica che consenta a EventBridge Scheduler di richiamare un obiettivo, scegli uno dei seguenti obiettivi comuni. Copia la politica di JSON autorizzazione e salvala localmente come `.json` file.

#### Amazon SQS – SendMessage

Quanto segue consente a EventBridge Scheduler di richiamare l'`sqs:SendMessage` azione su tutte le SQS code Amazon del tuo account.

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

#### Amazon SNS – Publish

Quanto segue consente a EventBridge Scheduler di richiedere l'`sns:Publish` azione su tutti gli SNS argomenti Amazon del tuo account.

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

```

    }
  ]
}

```

## Lambda – Invoke

Quanto segue consente a EventBridge Scheduler di richiamare l'azione `lambda:InvokeFunction` su tutte le funzioni Lambda del tuo account.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}

```

4. Esegui il comando seguente per creare la nuova politica di autorizzazione. Sostituisci *PolicyName* con il nome che desideri assegnare a questa politica.

```

$ aws iam create-policy --policy-name PolicyName --policy-document file://
PermissionPolicy.json

```

In caso di successo, verrà visualizzato il seguente risultato. Nota la politicaARN. Lo usi ARN nel passaggio successivo per collegare la politica al nostro ruolo di esecuzione.

```

{
  "Policy": {
    "PolicyName": "PolicyName",
    "CreateDate": "2022-03-01T19:31:18.620Z",
    "AttachmentCount": 0,
    "IsAttachable": true,
    "PolicyId": "ZXR6A36LTYANPAI7NJ5UV",
    "DefaultVersionId": "v1",
    "Path": "/",
    "Arn": "arn:aws:iam::123456789012:policy/PolicyName",
    "UpdateDate": "2022-03-01T19:31:18.620Z"
  }
}

```

```
}  
}
```

5. Esegui il comando seguente per allegare la policy al tuo ruolo di esecuzione. ARN Sostituiscila *your-policy-arn* con la politica che hai creato nel passaggio precedente. Sostituiscilo *SchedulerExecutionRole* con il nome del tuo ruolo di esecuzione.

```
$ aws iam attach-role-policy --policy-arn your-policy-arn --role-name SchedulerExecutionRole
```

L'attach-role-policy operazione non restituisce una risposta sulla riga di comando.

## Configura un bersaglio

Prima di creare una EventBridge pianificazione di Scheduler, è necessario che la pianificazione richiami almeno un obiettivo. È possibile utilizzare una AWS risorsa esistente o crearne una nuova. I passaggi seguenti mostrano come creare una nuova SQS coda Amazon standard con AWS CloudFormation.

Per creare una nuova SQS coda Amazon

1. Copia il seguente JSON AWS CloudFormation modello e salvalo localmente come `SchedulerTargetSQS.json`.

```
{  
  "AWSTemplateFormatVersion": "2010-09-09",  
  "Resources": {  
    "MyQueue": {  
      "Type": "AWS::SQS::Queue",  
      "Properties": {  
        "QueueName": "MyQueue"  
      }  
    }  
  },  
  "Outputs": {  
    "QueueName": {  
      "Description": "The name of the queue",  
      "Value": {  
        "Fn::GetAtt": [  
          "MyQueue",  

```

```

        "QueueName"
      ]
    }
  },
  "QueueURL": {
    "Description": "The URL of the queue",
    "Value": {
      "Ref": "MyQueue"
    }
  },
  "QueueARN": {
    "Description": "The ARN of the queue",
    "Value": {
      "Fn::GetAtt": [
        "MyQueue",
        "Arn"
      ]
    }
  }
}
}
}

```

- Da AWS CLI, esegui il comando seguente per creare uno AWS CloudFormation stack dal Scheduler-Target-SQS.json modello.

```
$ aws cloudformation create-stack --stack-name Scheduler-Target-SQS --template-body
file://Scheduler-Target-SQS.json
```

In caso di successo, verrà visualizzato il seguente risultato:

```
{
  "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/Scheduler-
Target-SQS/1d2af345-a121-12eb-abc1-012e34567890"
}
```

- Esegui il comando seguente per visualizzare le informazioni di riepilogo relative al tuo AWS CloudFormation stack. Queste informazioni includono lo stato dello stack e gli output specificati nel modello.

```
$ aws cloudformation describe-stacks --stack-name Scheduler-Target-SQS
```

In caso di successo, il comando crea la SQS coda Amazon e restituisce il seguente output:

```
{
  "Stacks": [
    {
      "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/
Scheduler-Target-SQS/1d2af345-a121-12eb-abc1-012e34567890",
      "StackName": "Scheduler-Target-SQS",
      "CreationTime": "2022-03-17T16:21:29.442000+00:00",
      "RollbackConfiguration": {},
      "StackStatus": "CREATE_COMPLETE",
      "DisableRollback": false,
      "NotificationARNs": [],
      "Outputs": [
        {
          "OutputKey": "QueueName",
          "OutputValue": "MyQueue",
          "Description": "The name of the queue"
        },
        {
          "OutputKey": "QueueARN",
          "OutputValue": "arn:aws:sqs:us-west-2:123456789012:MyQueue",
          "Description": "The ARN of the queue"
        },
        {
          "OutputKey": "QueueURL",
          "OutputValue": "https://sqs.us-
west-2.amazonaws.com/123456789012/MyQueue",
          "Description": "The URL of the queue"
        }
      ],
      "Tags": [],
      "EnableTerminationProtection": false,
      "DriftInformation": {
        "StackDriftStatus": "NOT_CHECKED"
      }
    }
  ]
}
```

Più avanti in questa guida, utilizzerai il valore for QueueARN per impostare la coda come destinazione per EventBridge Scheduler.

## Fasi successive

Dopo aver completato la fase di configurazione, usa la guida [introduttiva](#) per creare il tuo primo EventBridge scheduler Scheduler e richiamare un obiettivo.

# Guida introduttiva a EventBridge Scheduler

Questo argomento descrive la creazione di una nuova EventBridge pianificazione Scheduler. Puoi utilizzare la console EventBridge Scheduler, AWS Command Line Interface (AWS CLI) o AWS SDKs per creare una pianificazione con un target Amazon SQS basato su modelli. Quindi, configurerai la registrazione, configurerai i nuovi tentativi e imposterai un tempo massimo di conservazione per le attività non riuscite. Dopo aver creato la pianificazione, verificherai che la pianificazione richiami correttamente la destinazione e invii un messaggio alla coda delle destinazioni.

## Note

Per seguire questa guida, ti consigliamo di configurare IAM gli utenti con le autorizzazioni minime richieste descritte in [the section called “Utilizzo di policy basate su identità”](#). Dopo aver creato e configurato un utente, esegui il comando seguente per impostare le credenziali di accesso. Avrai bisogno dell'ID della chiave di accesso e della chiave di accesso segreta per configurare. AWS CLI

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

Per ulteriori informazioni sui diversi modi in cui è possibile impostare le credenziali, vedere [Impostazioni di configurazione e priorità](#) nella Guida per l'AWS Command Line Interface utente della versione 2.

## Argomenti

- [Prerequisiti](#)
- [Crea una pianificazione utilizzando la console EventBridge Scheduler](#)
- [Crea una pianificazione utilizzando il AWS CLI](#)
- [Crea una pianificazione utilizzando lo Scheduler EventBridge SDKs](#)
- [Fasi successive](#)

## Prerequisiti

Prima di eseguire i passaggi descritti in questa sezione, è necessario effettuare le seguenti operazioni:

- Completare le attività descritte in [Configurazione](#)

## Crea una pianificazione utilizzando la console EventBridge Scheduler

Per creare una nuova pianificazione utilizzando la console

1. [Accedi a AWS Management Console, quindi scegli il seguente link per aprire la sezione EventBridge Scheduler della EventBridge console: https://us-west-2.console.aws.amazon.com/scheduler/home?region=us-west-2#home](https://us-west-2.console.aws.amazon.com/scheduler/home?region=us-west-2#home)

### Note

Puoi cambiare la tua usando il selettore Regione AWS della regione. AWS Management Console

2. Nella pagina Pianificazioni, scegli Crea pianificazione.
3. Nella pagina Specifica i dettagli della pianificazione, nella sezione Nome e descrizione della pianificazione, effettua le seguenti operazioni:
  - a. Per Nome pianificazione, inserisci un nome per la pianificazione. Ad esempio, **MyTestSchedule**.
  - b. Per Descrizione: facoltativo, inserisci una descrizione per il tuo programma. Ad esempio **My first schedule**.
  - c. Per il gruppo di pianificazione, scegli un gruppo di pianificazione dalle opzioni a discesa. Se in precedenza non hai creato alcun gruppo di pianificazione, puoi scegliere il default gruppo per la tua pianificazione. Per creare un nuovo gruppo di pianificazione, scegli il link Crea la tua pianificazione nella descrizione della console. I gruppi di pianificazione vengono utilizzati per aggiungere tag a gruppi di pianificazioni.
4. Nella sezione Schema di pianificazione, procedi come segue:

- a. Per Occorrenza, scegliete una delle seguenti opzioni di pattern. Le opzioni di configurazione cambiano a seconda del pattern selezionato.
  - Pianificazione unica: una pianificazione unica richiama un obiettivo solo una volta alla data e all'ora specificate.

Per Data e ora, inserisci una data valida nel formato. YYYY/MM/DD Quindi, specifica un timestamp in formato 24 ore hh:mm. Infine, scegli un fuso orario dalle opzioni a discesa.

- Pianificazione ricorrente: una pianificazione ricorrente richiama un obiettivo a una frequenza specificata utilizzando un'espressione o un'espressione di frequenza. cron

Scegliete una pianificazione basata su CRON per configurare una pianificazione utilizzando un'espressione. cron Per utilizzare un'espressione di tasso, scegli Pianificazione basata sulla tariffa e inserisci un numero positivo per Valore, quindi scegli un'unità dalle opzioni a discesa.

Per ulteriori informazioni sull'utilizzo delle espressioni cron e rate, consulta. [Tipi di pianificazione](#)

- b. Per Finestra temporale flessibile, scegli Off per disattivare l'opzione o scegli una delle finestre temporali predefinite dall'elenco a discesa. Ad esempio, se scegli 15 minuti e imposti una pianificazione ricorrente per il richiamo della destinazione ogni ora, la pianificazione viene eseguita entro 15 minuti dall'inizio di ogni ora.
5. Se hai scelto Pianificazione ricorrente nel passaggio precedente, nella sezione Intervallo di tempo, specifica un fuso orario e, facoltativamente, imposta una data e un'ora di inizio e una data e ora di fine per la pianificazione. Una pianificazione ricorrente senza una data di inizio avrà inizio non appena verrà creata e sarà disponibile. Una pianificazione ricorrente senza una data di fine continuerà a richiamare il suo obiettivo a tempo indeterminato.
  6. Scegli Next (Successivo).
  7. Nella pagina Seleziona destinazione, procedi come segue:
    - a. Seleziona obiettivi basati su modelli e scegli un obiettivo. API Per questo esempio, sceglieremo il target basato su SQS **SendMessage** modelli Amazon.
    - b. Nella SendMessage sezione, per la SQScoda, scegli una SQS coda Amazon esistente, ARN ad esempio `arn:aws:sqs:us-west-2:123456789012:TestQueue` dall'elenco a discesa. Per creare una nuova coda, scegli Crea nuova SQS coda per accedere alla console AmazonSQS. Dopo aver completato la creazione di una coda, torna alla console

EventBridge Scheduler e aggiorna il menu a discesa. La nuova coda ARN viene visualizzata e può essere selezionata.

- c. Per Target, inserisci il payload che desideri che EventBridge Scheduler distribuisca alla destinazione. Per questo esempio, invieremo il seguente messaggio alla coda di destinazione: **Hello, it's EventBridge Scheduler.**
8. Scegli Avanti, quindi nella pagina Impostazioni - opzionale, procedi come segue:
  9.
    - a. Nella sezione Stato di pianificazione, per Abilita pianificazione, attiva o disattiva la funzione utilizzando l'interruttore. Per impostazione predefinita, lo EventBridge Scheduler abilita la tua pianificazione.
    - b. Nella sezione Azione dopo il completamento della pianificazione, configura l'azione intrapresa dallo EventBridge Scheduler dopo il completamento della pianificazione:
      - Scegli DELETE se desideri che la pianificazione venga eliminata automaticamente. Per le pianificazioni una tantum, ciò si verifica dopo che la pianificazione ha richiamato l'obiettivo una volta. Per le pianificazioni ricorrenti, ciò si verifica dopo l'ultima chiamata pianificata della pianificazione. Per ulteriori informazioni sull'eliminazione automatica, vedere. [the section called "Eliminazione dopo il completamento della pianificazione"](#)
      - Scegliete NONE o non scegliete un valore se non desiderate che EventBridge Scheduler intraprenda alcuna azione dopo il completamento della pianificazione.
    - c. Nella sezione Criteri di riprova e coda lettere morte (DLQ), per Criterio Riprova, attiva Riprova per configurare un criterio di riprova per la tua pianificazione. Con le politiche di riprova, se una pianificazione non riesce a richiamare il suo obiettivo, Scheduler esegue nuovamente la pianificazione. EventBridge Se configurato, è necessario impostare il tempo di conservazione massimo e i nuovi tentativi per la pianificazione.
    - d. Per Età massima dell'evento, facoltativo, inserisci il numero massimo di ore e minuti in cui EventBridge Scheduler deve conservare un evento non elaborato.

 Note

Il valore massimo è 24 ore.

- e. Per Numero massimo di tentativi, inserisci il numero massimo di volte in cui EventBridge Scheduler riprova la pianificazione se la destinazione restituisce un errore.

 Note

Il valore massimo è 185 tentativi.

- f. Per Dead-letter queue (DLQ), scegliete una delle seguenti opzioni:
- Nessuno: scegliete questa opzione se non desiderate configurare un DLQ
  - Seleziona una SQS coda Amazon nel mio AWS account come DLQ: scegli questa opzione, quindi seleziona una coda ARN dall'elenco a discesa, configurane una DLQ Account AWS uguale a quella in cui stai creando la pianificazione.
  - Specificare una SQS coda Amazon in un altro AWS account come DLQ: scegli questa opzione, quindi inserisci la ARN coda configurata come DLQ, se la coda si trova in un altro Account AWS Devi inserire l'esatto ARN per la coda per utilizzare questa opzione.
- g. Nella sezione Crittografia, scegli Personalizza le impostazioni di crittografia (avanzate) per utilizzare una KMS chiave gestita dal cliente per crittografare l'input di destinazione. Se scegli questa opzione, inserisci una KMS chiave esistente ARN o scegli Crea una AWS KMS chiave per accedere alla AWS KMS console. Per ulteriori informazioni su come EventBridge Scheduler crittografa i dati inattivi, consulta. [the section called "Crittografia a riposo"](#)
- h. Per Autorizzazioni, scegli Usa il ruolo esistente, quindi seleziona il ruolo che hai creato durante la procedura di [configurazione](#) dall'elenco a discesa. Puoi anche scegliere Vai alla IAM console per creare un nuovo ruolo.

Se desideri che EventBridge Scheduler crei un nuovo ruolo di esecuzione per te, scegli invece Crea nuovo ruolo per questa pianificazione. Inserisci, quindi, un nome per Nome ruolo. Se scegli questa opzione, EventBridge Scheduler aggiunge al ruolo le autorizzazioni necessarie per la destinazione basata sul modello.

10. Scegli Next (Successivo).
11. Nella pagina Rivedi e crea pianificazione, rivedi i dettagli della pianificazione. In ogni sezione, scegli Modifica per tornare a tale passaggio e modificarne i dettagli.
12. Scegli Crea pianificazione per completare la creazione della nuova pianificazione. Puoi visualizzare un elenco delle pianificazioni nuove ed esistenti nella pagina Pianificazioni. Nella colonna Stato, accertati che la nuova pianificazione sia Abilitata.
13. Per verificare che la tua pianificazione richiami il SQS target Amazon, apri la SQS console Amazon ed esegui le seguenti operazioni:

- a. Scegli la coda di destinazione dall'elenco delle code.
- b. Scegli Invia e ricevi messaggi.
- c. Nella pagina Invia e ricevi messaggi, in Ricevi messaggi, scegli Esamina messaggi per recuperare i messaggi di test che la tua pianificazione ha inviato alla coda di destinazione.

## Crea una pianificazione utilizzando il AWS CLI

L'esempio seguente mostra come utilizzare il AWS CLI comando per [create-schedule](#) creare una EventBridge pianificazione Scheduler con un target Amazon SQS basato su modelli. Sostituisci i valori segnaposto per i seguenti parametri con le tue informazioni:

- `--name` — Inserisci un nome per la pianificazione.
- `RoleArn` — Inserisci ARN il ruolo di esecuzione che desideri associare alla pianificazione.
- `Arn` — Inserite il valore ARN per la destinazione. In questo caso, l'obiettivo è una SQS coda Amazon.
- `Input`: inserisci un messaggio che EventBridge Scheduler invia alla coda di destinazione.

```
$ aws scheduler create-schedule --name sqs-templated-schedule --schedule-expression 'rate(5 minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn": "QUEUE_ARN", "Input": "TEST_PAYLOAD" }' \
--flexible-time-window '{ "Mode": "OFF" }'
```

## Crea una pianificazione utilizzando lo Scheduler EventBridge SDKs

Nell'esempio seguente, utilizzi EventBridge Scheduler SDKs per creare una EventBridge pianificazione Scheduler con un target Amazon basato su modelli. SQS

### Example Python SDK

```
import boto3
scheduler = boto3.client('scheduler')

flex_window = { "Mode": "OFF" }

sqs_templated = {
    "RoleArn": "<ROLE_ARN>",
```

```
"Arn": "<QUEUE_ARN>",
  "Input": "Message for scheduleArn: '<aws.scheduler.schedule-arn>', scheduledTime:
'<aws.scheduler.scheduled-time>'"
}

scheduler.create_schedule(
  Name="sqs-python-templated",
  ScheduleExpression="rate(5 minutes)",
  Target=sqs_templated,
  FlexibleTimeWindow=flex_window)
```

## Example Java SDK

```
package com.example;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.scheduler.SchedulerClient;
import software.amazon.awssdk.services.scheduler.model.*;

public class MySchedulerApp {

    public static void main(String[] args) {

        final SchedulerClient client = SchedulerClient.builder()
            .region(Region.US_WEST_2)
            .build();

        Target sqsTarget = Target.builder()
            .roleArn("<ROLE_ARN>")
            .arn("<QUEUE_ARN>")
            .input("Message for scheduleArn: '<aws.scheduler.schedule-arn>',
scheduledTime: '<aws.scheduler.scheduled-time>'"")
            .build();

        CreateScheduleRequest createScheduleRequest = CreateScheduleRequest.builder()
            .name("<SCHEDULE NAME>")
            .scheduleExpression("rate(10 minutes)")
            .target(sqsTarget)
            .flexibleTimeWindow(FlexibleTimeWindow.builder()
                .mode(FlexibleTimeWindowMode.OFF)
                .build())
            .build();
```

```
        client.createSchedule(createScheduleRequest);
        System.out.println("Created schedule with rate expression and an Amazon SQS
templated target");
    }
}
```

## Fasi successive

- Per ulteriori informazioni sulla gestione della pianificazione tramite la console o lo EventBridge SchedulerSDK, consulta [Gestire una pianificazione](#). AWS CLI
- Per ulteriori informazioni su come configurare gli obiettivi basati su modelli e sull'utilizzo del parametro universal target, vedere. [Gestione degli obiettivi](#)
- [Per ulteriori informazioni sui tipi di dati e sulle API operazioni dello EventBridge Scheduler, vedere Scheduler Reference. EventBridge API](#)

# Tipi di pianificazione in EventBridge Scheduler

L'argomento seguente descrive i diversi tipi di pianificazione supportati da Amazon EventBridge Scheduler, nonché come EventBridge Scheduler gestisce l'ora legale e la pianificazione in diversi fusi orari. Puoi scegliere tra tre tipi di pianificazione durante la configurazione: pianificazioni basate sulla tariffa, basate su cron e pianificazioni una tantum.

Sia le pianificazioni basate sulla frequenza che quelle basate sul cronometro sono pianificazioni ricorrenti. Ogni tipo di pianificazione ricorrente viene configurato utilizzando un'espressione di pianificazione per il tipo di pianificazione che si desidera configurare e specificando un fuso orario in cui Scheduler valuta l'espressione. EventBridge

Una pianificazione unica è una pianificazione che richiama un obiettivo solo una volta. Si configura una pianificazione unica specificando l'ora, la data e il fuso orario in cui EventBridge Scheduler valuta la pianificazione.

## Note

Tutti i tipi di EventBridge pianificazione su Scheduler richiamano i propri obiettivi con una precisione di 60 secondi. Ciò significa che se imposti la pianificazione in modo che venga eseguita `1:00`, invocherà l'obiettivo API compreso tra `1:00:00` e `1:00:59`, supponendo che non sia impostata una finestra temporale flessibile.

Utilizza le seguenti sezioni per scoprire come configurare le espressioni di pianificazione per ogni tipo di pianificazione ricorrente e come impostare una pianificazione una tantum su Scheduler. EventBridge

## Argomenti

- [Pianificazioni basate sulle tariffe](#)
- [Pianificazioni basate su CRON](#)
- [Pianificazioni una tantum](#)
- [Fusi orari su Scheduler EventBridge](#)
- [Ora EventBridge legale su Scheduler](#)

## Pianificazioni basate sulle tariffe

Una pianificazione basata sulle tariffe inizia dopo la data di inizio specificata per la pianificazione e viene eseguita a una frequenza regolare definita dall'utente fino alla data di fine della pianificazione. È possibile impostare i casi d'uso più comuni di pianificazione ricorrente utilizzando una pianificazione basata sulla tariffa. Ad esempio, se desideri una pianificazione che richiami l'obiettivo ogni 15 minuti, una volta ogni due ore o una volta ogni cinque giorni, puoi utilizzare una pianificazione basata sulla frequenza per raggiungere questo obiettivo. È possibile configurare una pianificazione basata sulla tariffa utilizzando un'espressione di frequenza.

Con le pianificazioni basate sulle tariffe, si utilizza la [StartDate](#) proprietà per impostare la prima occorrenza della pianificazione. Se non si fornisce una `StartDate` pianificazione basata sulla tariffa, la pianificazione inizia a richiamare immediatamente l'obiettivo.

Le espressioni tariffarie hanno due campi obbligatori separati da uno spazio bianco, come illustrato di seguito.

### Sintassi

```
rate(value unit)
```

value

Un numero positivo.

unità

L'unità di tempo in cui desideri che la tua pianificazione richiami è target.

Ingressi validi: | | minutes hours days

### Esempi

L'esempio seguente mostra come utilizzare le espressioni di frequenza con il AWS CLI `create-schedule` comando per configurare una pianificazione basata sulla tariffa. Questo esempio crea una pianificazione che viene eseguita ogni cinque minuti e invia un messaggio a una SQS coda Amazon, utilizzando il tipo di destinazione basato su `modelsqsParameters`.

Poiché questo esempio non imposta un valore per il `--start-date` parametro, la pianificazione inizia a richiamare la destinazione immediatamente dopo la creazione e l'attivazione.

```
$ aws scheduler create-schedule --schedule-expression 'rate(5 minutes)' --
name schedule-name \
--target '{"RoleArn": "role-arn", "Arn": "QUEUE_ARN", "Input": "TEST_PAYLOAD" }' \
--flexible-time-window '{ "Mode": "OFF" }'
```

## Pianificazioni basate su CRON

Un'espressione cron crea una pianificazione ricorrente dettagliata che viene eseguita in un momento specifico a tua scelta. EventBridge Scheduler supporta la configurazione di pianificazioni basate su cron in Universal Coordinated Time (UTC) o nel fuso orario specificato al momento della creazione della pianificazione. Con le pianificazioni basate su cron, hai un maggiore controllo su quando e con che frequenza viene eseguita la pianificazione. Utilizza le pianificazioni basate su cron quando hai bisogno di una pianificazione di ricorrenza personalizzata che non sia supportata da una delle espressioni di frequenza di EventBridge Scheduler. Ad esempio, puoi creare una pianificazione basata su cron che venga eseguita alle 8:00 PST il primo lunedì di ogni mese. Si configura una pianificazione basata su cron utilizzando un'espressione cron.

Un'espressione cron è composta da cinque campi obbligatori separati da spazi bianchi: minuti, ore day-of-month, mese e un campo opzionale day-of-week, anno, come illustrato di seguito.

## Sintassi

```
cron(minutes hours day-of-month month day-of-week year)
```

Campo	Valori	Caratteri jolly
Minuti	0-59	, - * /
Ore	0-23	, - * /
Day-of-month	1-31	, - * ? / L W
Mese	1-12 o JAN - DEC	, - * /
Day-of-week	1-7 o SUN - SAT	, - * ? L #
Anno	1970-2199	, - * /

## Caratteri jolly

- Il carattere jolly , (virgola) include valori aggiuntivi. Nel campo Mese, JAN, FEB, MAR include gennaio, febbraio e marzo.
- Il carattere jolly - (trattino) specifica gli intervalli. Nel campo Day (Giorno), 1-15 include i primi 15 giorni del mese specificato.
- Il carattere jolly \* (asterisco) include tutti i valori nel campo. Nel campo Hours (Ore), \* include ogni ora. Non puoi usare \* in entrambi i ay-of-week campi D ay-of-month e D. Se viene utilizzato in uno di tali campi, è necessario utilizzare ? nell'altro.
- Il carattere jolly / (barra) specifica gli incrementi. Nel campo Minutes (Minuti), puoi inserire 1/10 per specificare ogni decimo minuto, a partire dal primo minuto dell'ora (ad esempio, l'11°, il 21° e il 31° minuto e così via).
- Il carattere jolly ? (punto interrogativo) specifica qualsiasi valore. Nel ay-of-month campo D puoi inserire 7 e se qualsiasi giorno della settimana fosse accettabile, potresti inserire ? nel ay-of-week campo D.
- Il carattere jolly L nei ay-of-week campi D ay-of-month o D specifica l'ultimo giorno del mese o della settimana.
- Il carattere **W** jolly nel ay-of-month campo D specifica un giorno della settimana. Nel ay-of-month campo D, **3W** specifica il giorno della settimana più vicino al terzo giorno del mese.
- Il carattere jolly # nel ay-of-week campo D specifica una determinata istanza del giorno della settimana specificato all'interno di un mese. Ad esempio, **3#2** sarebbe il secondo martedì del mese: il 3 fa riferimento a martedì perché è il terzo giorno di ogni settimana e il 2 fa riferimento al secondo giorno di questo tipo in un mese.

### Note

Se si utilizza un carattere '#', è possibile definire solo un'espressione nel day-of-week campo. Ad esempio, "3#1, 6#3" non è valido perché viene interpretato come due espressioni.

## Esempi

L'esempio seguente mostra come utilizzare le espressioni cron con il AWS CLI `create-schedule` comando per configurare una pianificazione basata su cron. Questo esempio crea una pianificazione che viene eseguita alle 10:15 UTC +0 l'ultimo venerdì di ogni mese negli anni dal 2022 al 2023

e invia un messaggio a una SQS coda Amazon, utilizzando il tipo di destinazione basato su `modelloSqsParameters`.

```
$ aws scheduler create-schedule --schedule-expression "cron(15 10 ? * 6L 2022-2023)" --
name schedule-name \
--target '{"RoleArn": "role-arn", "Arn": "QUEUE_ARN", "Input": "TEST_PAYLOAD" }' \
--flexible-time-window '{ "Mode": "OFF" }'
```

## Pianificazioni una tantum

Una pianificazione unica richiamerà un obiettivo solo una volta alla data e all'ora specificate utilizzando una data e un timestamp validi. EventBridge Scheduler supporta la pianificazione in Universal Coordinated Time (UTC) o nel fuso orario specificato al momento della creazione della pianificazione.

### Note

Una pianificazione unica viene comunque conteggiata ai fini della quota dell'account anche dopo che è stata completata l'esecuzione e ha richiamato l'obiettivo. Ti consigliamo di [eliminare](#) le tue pianificazioni una tantum al termine della loro esecuzione.

Puoi configurare una pianificazione unica utilizzando un'espressione `at`. Un'espressione `at` è costituita dalla data e dall'ora in cui si desidera che EventBridge Scheduler richiami la pianificazione, come illustrato di seguito.

## Sintassi

```
at(yyyy-mm-ddThh:mm:ss)
```

Quando si configura una pianificazione una tantum, EventBridge Scheduler ignora l'`StartDate` e specificato per la `EndDate` pianificazione.

## Esempi

L'esempio seguente mostra come utilizzare le espressioni `at` con il AWS CLI `create-schedule` comando per configurare una pianificazione una tantum. Questo esempio crea una pianificazione che

viene eseguita una volta alle 13:00 UTC -8 del 20 novembre 2022 e invia un messaggio a una SQS coda Amazon, utilizzando il tipo di destinazione basato su modello `SqsParameters`.

```
$ aws scheduler create-schedule --schedule-expression "at(2022-11-20T13:00:00)" --
name schedule-name \
--target '{"RoleArn": "role-arn", "Arn": "QUEUE_ARN", "Input": "TEST_PAYLOAD" }' \
--schedule-expression-timezone "America/Los_Angeles"
--flexible-time-window '{ "Mode": "OFF" }'
```

## Fusi orari su Scheduler EventBridge

EventBridge Scheduler supporta la configurazione di pianificazioni singole e basate su cron in qualsiasi fuso orario specificato. EventBridge Scheduler utilizza il [database dei fusi orari](#) gestito dalla Internet Assigned Numbers Authority (IANA).

Con AWS CLI, è possibile impostare il fuso orario in cui si desidera che EventBridge Scheduler valuti la pianificazione utilizzando il `--schedule-expression-timezone` parametro. Ad esempio, il comando seguente crea una pianificazione basata su cron che richiama un SQS `SendMessage` target Amazon basato su modelli in `America/New_York` ogni giorno alle 8:30.

```
$ aws scheduler create-schedule --schedule-expression "cron(30 8 * * ? *)" --name
schedule-in-est \
--target '{"RoleArn": "role-arn", "Arn": "QUEUE_ARN", "Input": "This schedule runs
in the America/New_York time zone." }' \
--schedule-expression-timezone "America/New_York"
--flexible-time-window '{ "Mode": "OFF" }'
```

## Ora EventBridge legale su Scheduler

EventBridge Scheduler regola automaticamente la pianificazione in base all'ora legale. Quando l'ora passa in avanti in primavera, se un'espressione cron cade su una data e un'ora inesistenti, la chiamata alla pianificazione viene saltata. Quando il tempo torna indietro in autunno, la pianificazione viene eseguita una sola volta e non ripete la sua invocazione. Le seguenti invocazioni si verificano normalmente alla data e all'ora specificate.

EventBridge Scheduler regola la pianificazione in base al fuso orario specificato al momento della creazione della pianificazione. Se configuri una pianificazione in `America/New_York`, la pianificazione viene modificata quando l'ora cambia in quel fuso orario, mentre una pianificazione in `America/Los_Angeles` viene modificata tre ore dopo, quando l'ora cambia sulla costa occidentale.

Per le pianificazioni basate sulle tariffe che utilizzano `days` come unità, ad esempio, rappresenta una durata di 24 ore sull'orologio. `rate(1 days) days` Ciò significa che quando l'ora legale riduce un giorno a 23 ore o si estende a 25 ore, EventBridge Scheduler valuta comunque l'espressione della tariffa 24 ore dopo l'ultima chiamata della pianificazione.

#### Note

Alcuni fusi orari non rispettano l'ora legale, in base alle norme e ai regolamenti locali. Se si crea una pianificazione in un fuso orario che non rispetta l'ora legale, EventBridge Scheduler non modifica la pianificazione. Le regolazioni dell'ora legale non si applicano agli orari in base all'ora coordinata universale (`Z`). UTC

#### Esempio

Considera uno scenario in cui crei una pianificazione utilizzando la seguente espressione cron in `America/Los_Angeles`: `cron(30 2 * * ? *)` Questa pianificazione viene eseguita ogni giorno alle 2:30 del mattino nel fuso orario specificato.

- **Spring-forward:** quando l'ora passa in avanti in primavera dall'1:59 alle 3:00, EventBridge Scheduler salta la chiamata alla pianificazione di quel giorno e riprende a eseguire la pianificazione normalmente il giorno successivo.
- **Fallback:** quando l'orario cambia all'indietro in autunno dalle 2:59 alle 2:00, EventBridge Scheduler esegue la pianificazione solo una volta alle 2:30 prima che si verifichi il turno, ma non ripete più la chiamata alla pianificazione alle 2:30 dopo il turno orario.

# Gestione di una pianificazione in EventBridge Scheduler

Una pianificazione è la risorsa principale che puoi creare, configurare e gestire utilizzando Amazon EventBridge Scheduler.

Ogni pianificazione ha un'espressione di pianificazione che determina quando e con quale frequenza viene eseguita. EventBridge Scheduler supporta tre tipi di pianificazioni: rate, cron e pianificazioni singole. Per ulteriori informazioni sui diversi tipi di pianificazione, vedere. [Tipi di pianificazione](#)

Quando si crea una pianificazione, si configura un obiettivo per la pianificazione da richiamare. Un obiettivo è un'API operazione che EventBridge Scheduler chiama per conto dell'utente ogni volta che viene eseguita la pianificazione. EventBridge Scheduler supporta due tipi di destinazioni: le destinazioni basate su modelli richiamano API operazioni comuni su un gruppo principale di servizi e il parametro di destinazione universale (UTP) che puoi utilizzare per chiamare più di 6.000 operazioni su oltre 270 servizi. Per ulteriori informazioni sulla configurazione degli obiettivi, vedere. [Gestione degli obiettivi](#)

È possibile configurare il modo in cui la pianificazione gestisce gli errori, quando EventBridge Scheduler non è in grado di inviare correttamente un evento a una destinazione, utilizzando due meccanismi principali: una politica di ripetizione dei tentativi e una coda di lettere morte (DLQ). Una politica di nuovo tentativo determina il numero di volte in cui EventBridge Scheduler deve riprovare un evento non riuscito e per quanto tempo conservare un evento non elaborato. A DLQ è una coda standard che Amazon SQS Queue EventBridge Scheduler utilizza per inviare eventi non riusciti, una volta esaurita la politica di ripetizione dei tentativi. Puoi usare a DLQ per risolvere problemi relativi alla tua pianificazione o alla sua destinazione a valle. Per ulteriori informazioni su, vedere. [the section called "Configurazione di un DLQ"](#)

In questa sezione, puoi trovare esempi per gestire le pianificazioni di EventBridge Scheduler utilizzando la console, lo Scheduler AWS CLI e lo EventBridge SDKs Scheduler.

## Argomenti

- [Modifica dello stato della pianificazione in Scheduler EventBridge](#)
- [Configurazione di finestre temporali flessibili in Scheduler EventBridge](#)
- [Configurazione della coda di lettere morte di una pianificazione in Scheduler EventBridge](#)
- [Eliminazione di una pianificazione in Scheduler EventBridge](#)
- [Fasi successive](#)

## Modifica dello stato della pianificazione in Scheduler EventBridge

Una EventBridge pianificazione Scheduler ha due stati: abilitato e disabilitato. L'esempio seguente utilizza `UpdateSchedule` per disabilitare una pianificazione che si attiva ogni cinque minuti e richiama un target Lambda.

Quando si utilizza `UpdateSchedule`, è necessario fornire tutti i parametri richiesti. EventBridge Scheduler sostituisce la pianificazione con le informazioni fornite dall'utente. Se non specifichi un parametro che hai impostato in precedenza, il valore predefinito è `null`.

### Example AWS CLI

```
$ aws scheduler update-schedule --name lambda-universal --schedule-expression 'rate(5
minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn": "arn:aws:scheduler::aws-sdk:lambda:invoke"
"Input": "{\"FunctionName\": \"arn:aws:lambda:REGION:123456789012:function:HelloWorld
\", \"InvocationType\": \"Event\", \"Payload\": \"{\\\"message\\\": \\\"testing function\\
\\\"}\" }' \
--flexible-time-window '{ "Mode": "OFF" }' \
--state DISABLED
```

```
{
  "ScheduleArn": "arn:aws:scheduler:us-west-2:123456789012:schedule/default/lambda-
universal"
}
```

L'esempio seguente utilizza Python SDK e l'`UpdateSchedule` operazione per disabilitare una pianificazione destinata ad Amazon SQS utilizzando un target basato su modelli.

### Example Python SDK

```
import boto3
scheduler = boto3.client('scheduler')

sqs_templated = {
    "RoleArn": "<ROLE_ARN>",
    "Arn": "<QUEUE_ARN>",
    "Input": "{}"

flex_window = { "Mode": "OFF" }
```

```
scheduler.update_schedule(Name="your-schedule",
  ScheduleExpression="rate(5 minutes)",
  Target=sqs_templated,
  FlexibleTimeWindow=flex_window,
  State='DISABLED')
```

## Configurazione di finestre temporali flessibili in Scheduler EventBridge

Quando configuri la pianificazione con una finestra temporale flessibile, EventBridge Scheduler richiama l'obiettivo entro la finestra temporale impostata. Ciò è utile nei casi che non richiedono una chiamata programmata precisa degli obiettivi. L'impostazione di una finestra temporale flessibile migliora l'affidabilità della pianificazione disperdendo le chiamate di destinazione.

Ad esempio, se configuri una finestra temporale flessibile di 15 minuti per una pianificazione che viene eseguita ogni ora, l'obiettivo viene richiamato entro 15 minuti dall'orario pianificato. Gli SDK esempi seguenti AWS CLI e EventBridge Scheduler vengono utilizzati UpdateSchedule per impostare una finestra temporale flessibile di 15 minuti per una pianificazione che viene eseguita una volta ogni ora.

### Note

È necessario specificare se si desidera impostare una finestra temporale flessibile o meno. Se non desiderate impostare questa opzione, specificate OFF. Se impostate il valore su FLEXIBLE, dovete quindi specificare una finestra di tempo massima durante la quale verrà eseguita la pianificazione.

### Example AWS CLI

```
$ aws scheduler update-schedule --name lambda-universal --schedule-expression 'rate(1
hour)' \
--target '{"RoleArn": "ROLE_ARN", "Arn": "arn:aws:scheduler::aws-sdk:lambda:invoke"
"Input": "{\"FunctionName\": \"arn:aws:lambda:REGION:123456789012:function:HelloWorld
\", \"InvocationType\": \"Event\", \"Payload\": \"{\\\"message\\\": \\\"testing function\\
\\\"}\" }' \
--flexible-time-window '{ "Mode": "FLEXIBLE", "MaximumWindowInMinutes": 15} \
```

```
{
  "ScheduleArn": "arn:aws:scheduler:us-west-2:123456789012:schedule/lambda-universal"
}
```

## Example Python SDK

```
import boto3
scheduler = boto3.client('scheduler')

sqs_templated = {
  "RoleArn": "<ROLE_ARN>",
  "Arn": "<QUEUE_ARN>",
  "Input": "{}"}

flex_window = { "Mode": "FLEXIBLE", "MaximumWindowInMinutes": 15}

scheduler.update_schedule(Name="your-schedule",
  ScheduleExpression="rate(1 hour)",
  Target=sqs_templated,
  FlexibleTimeWindow=flex_window)
```

## Configurazione della coda di lettere morte di una pianificazione in Scheduler EventBridge

Amazon EventBridge Scheduler supporta le code di lettere morte (DLQ) utilizzando Amazon Simple Queue Service. Quando una pianificazione non riesce a richiamare la sua destinazione, EventBridge Scheduler invia un JSON payload contenente i dettagli di chiamata e qualsiasi risposta ricevuta dalla destinazione a una coda Amazon SQS standard specificata.

Il seguente argomento si riferisce a questo evento come a un evento non valido. JSON Un evento con lettera morta consente di risolvere problemi relativi alla pianificazione o agli obiettivi. Se configuri una politica di nuovi tentativi per la tua EventBridge pianificazione, Scheduler invia l'evento «dead-letter» che contiene, esaurendo il numero massimo di tentativi impostato.

I seguenti argomenti descrivono come configurare una SQS coda Amazon come programma, impostare le autorizzazioni necessarie a EventBridge Scheduler DLQ per recapitare messaggi ad Amazon SQS e ricevere eventi con lettera morta da DLQ

### Argomenti

- [Crea una SQS coda Amazon](#)
- [Imposta le autorizzazioni per i ruoli di esecuzione](#)
- [Specificate una coda di lettere non scritte](#)
- [Recupera l'evento con lettera morta](#)

## Crea una SQS coda Amazon

Prima di configurarne una DLQ per la tua pianificazione, devi creare una SQS coda Amazon standard. Per istruzioni sulla creazione di una coda utilizzando la SQS console Amazon, consulta [Creating an Amazon SQS queue nella Amazon Simple Queue Service Developer Guide](#).

### Note

EventBridge Scheduler non supporta l'utilizzo di una FIFO coda come pianificazione. DLQ

Utilizzate il seguente AWS CLI comando per creare una coda standard.

```
$ aws sqs create-queue --queue-name queue-name
```

In caso di successo, lo vedrai QueueURL nell'output.

```
{
  "QueueUrl": "https://sqs.us-west-2.amazonaws.com/123456789012/scheduler-dlq-test"
}
```

Dopo aver creato la coda, prendi nota della codaARN. Ti servirà ARN quando specifichi una DLQ per la tua EventBridge pianificazione di Scheduler. Puoi trovare la tua coda ARN nella SQS console Amazon o utilizzando il [get-queue-attributes](#) AWS CLI comando.

```
$ aws sqs get-queue-attributes --queue-url your-dlq-url --attribute-names QueueArn
```

In caso di successo, vedrai la coda ARN nell'output.

```
{
  "Attributes": {
    "QueueArn": "arn:aws:sqs:us-west-2:123456789012:scheduler-dlq-test"
  }
}
```

```
}  
}
```

Nella sezione successiva, aggiungerai le autorizzazioni necessarie al tuo ruolo di esecuzione della pianificazione per consentire a EventBridge Scheduler di inviare eventi con lettera morta ad Amazon SQS.

## Imposta le autorizzazioni per i ruoli di esecuzione

Per consentire a EventBridge Scheduler di inviare eventi con lettera morta ad AmazonSQS, il tuo ruolo di esecuzione della pianificazione richiede la seguente politica di autorizzazione. Per ulteriori informazioni su come allegare una nuova politica di autorizzazione al ruolo di esecuzione pianificata, consulta [Configurazione](#) del ruolo di esecuzione.

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

### Note

Il tuo ruolo di esecuzione della pianificazione potrebbe già avere le autorizzazioni richieste allegate se utilizzi EventBridge Scheduler per richiamare un target Amazon SQS API.

Nella sezione successiva, utilizzerai la console EventBridge Scheduler e specificherai una DLQ per la tua pianificazione.

## Specificate una coda di lettere non scritte

Per specificare aDLQ, usa la console EventBridge Scheduler o AWS CLI per aggiornare una pianificazione esistente o crearne una nuova.

## Console

Per specificare un DLQ utilizzando la console

1. [Accedi a AWS Management Console, quindi scegli il seguente link per aprire la sezione EventBridge Scheduler della EventBridge console: home https://console.aws.amazon.com/scheduler/](https://console.aws.amazon.com/scheduler/)
2. Sulla console EventBridge Scheduler, crea una nuova pianificazione o scegli una pianificazione esistente dall'elenco di pianificazioni da modificare.
3. Nella pagina Impostazioni, per Dead-letter queue (DLQ), esegui una delle seguenti operazioni:
  - Scegli Seleziona una SQS coda Amazon nel mio AWS account come fileDLQ, quindi scegli la coda ARN desiderata DLQ dall'elenco a discesa.
  - Scegli Specificare una SQS coda Amazon in altri AWS account come a DLQ, quindi inserisci la coda ARN per il tuo. DLQ Se scegli una coda in un altro AWS account, la console EventBridge Scheduler non sarà in grado di visualizzare la coda ARNs in un elenco a discesa.
4. Controlla le tue selezioni, quindi scegli Crea pianificazione o Salva pianificazione per completare la configurazione di un. DLQ
5. (Facoltativo) Per visualizzare DLQ i dettagli di una pianificazione, scegli il nome della pianificazione dall'elenco, quindi scegli la scheda Coda Dead-Letter nella pagina dei dettagli della pianificazione.

## AWS CLI

Per aggiornare una pianificazione esistente utilizzando il AWS CLI

- Usa il [update-schedule](#) comando per aggiornare la tua pianificazione. Specificate la SQS coda Amazon che avete creato in precedenza come. DLQ Specificate il IAM ruolo ARN a cui avete associato le SQS autorizzazioni Amazon richieste come ruolo di esecuzione. Sostituisci tutti gli altri valori segnaposto con le tue informazioni.

```
$ aws scheduler update-schedule --name existing-schedule \  
  --schedule-expression 'rate(5 minutes)' \  
  --target '{"DeadLetterConfig": {"Arn": "DLQ_ARN"}, "RoleArn": "ROLE_ARN",  
  "Arn": "QUEUE_ARN", "Input": "Hello world!" }' \  
  \
```

```
--flexible-time-window '{ "Mode": "OFF"}
```

Per creare una nuova pianificazione utilizzando DLQ AWS CLI

- Utilizzare il [create-schedule](#) comando per creare una pianificazione. Sostituisci tutti i valori segnaposto con le tue informazioni.

```
$ aws scheduler create-schedule --name new-schedule \  
  --schedule-expression 'rate(5 minutes)' \  
  --target '{"DeadLetterConfig": {"Arn": "DLQ_ARN"}, "RoleArn": "ROLE_ARN",  
  "Arn": "QUEUE_ARN", "Input": "Hello world!" }' \  
  --flexible-time-window '{ "Mode": "OFF"}
```

Nella sezione successiva, utilizzerai il AWS CLI per ricevere un evento senza lettera morta da DLQ

## Recupera l'evento con lettera morta

Utilizzate il [receive-message](#) comando, come illustrato di seguito, per recuperare un evento con lettera morta da DLQ. È possibile impostare il numero di messaggi da recuperare utilizzando l'attributo. `--max-number-of-messages`

```
$ aws sqs receive-message --queue-url your-dlq-url --attribute-names All --message-  
attribute-names All --max-number-of-messages 1
```

In caso di successo, verrà visualizzato un output simile al seguente.

```
{  
  "Messages": [  
    {  
      "MessageId": "2aeg3510-fe3a-4f5a-ab6a-6906560eaf7e",  
      "ReceiptHandle": "AQEBkNKTD0MrWgHKPoITRBwrPoK3eCSZICzWvqCY0BZ  
+FfTcORFpopJbtCqj36VbBT1HreM8+qM/m5jcwqS1A1GmIJ0/hYmMgn/  
+dwIty9izE7HnpvRhhEyHxbeTZ5V05RbeasYaBdNyi9WLcnAHviDh6MebLXXNWoFyYnsxdwJuG0f/  
w3htX6r3dpxXvvFNPGoQb8ihY37+u0gtsbuIwhLtUSmE8rbldeEwiUfi3IJ1zEZpUS77n/k1GWrMrnYg0Gx/  
BuaLz0rFi2F738XI/  
Hnh45uv3ca60YwS1ojPQ1LtX2URg1haV5884FY1aRvY8jR1pCZabTkYRTZKSXG5KNgYZnHpmsspii6JNkjitYVFKPo0H91w  
      "MD5ofBody": "07adc3fc889d6107d8bb8fda42fe0573",  
      "Body": "{\"MessageBody\": \"Hello, world!\", \"QueueUrl\": \"https://sqs.us-  
west-2.amazonaws.com/123456789012/does-not-exist\"}",  
      "Attributes": {
```

```

    "SenderId": "ARO2DZE3W4CTL5ZR7EIN:ff00212d8c453aaaae644bc6846d4723",
    "ApproximateFirstReceiveTimestamp": "1652499058144",
    "ApproximateReceiveCount": "2",
    "SentTimestamp": "1652490733042"
  },
  "MD5ofMessageAttributes": "f72c1d78100860e00403d849831d4895",
  "MessageAttributes": {
    "ERROR_CODE": {
      "StringValue": "AWS.SimpleQueueService.NonExistentQueue",
      "DataType": "String"
    },
    "ERROR_MESSAGE": {
      "StringValue": "The specified queue does not exist for this wsdl
version.",
      "DataType": "String"
    },
    "EXECUTION_ID": {
      "StringValue": "ad06616e51cdf74a",
      "DataType": "String"
    },
    "EXHAUSTED_RETRY_CONDITION": {
      "StringValue": "MaximumEventAgeInSeconds",
      "DataType": "String"
    },
    "IS_PAYLOAD_TRUNCATED": {
      "StringValue": "false",
      "DataType": "String"
    },
    "RETRY_ATTEMPTS": {
      "StringValue": "0",
      "DataType": "String"
    },
    "SCHEDULED_TIME": {
      "StringValue": "2022-05-14T01:12:00Z",
      "DataType": "String"
    },
    "SCHEDULE_ARN": {
      "StringValue": "arn:aws:scheduler:us-west-2:123456789012:schedule/
DLQ-test",
      "DataType": "String"
    },
    "TARGET_ARN": {
      "StringValue": "arn:aws:scheduler::aws-sdk:sqs:sendMessage",
      "DataType": "String"
    }
  }
}

```

```

    }
  }
]
}

```

Nota i seguenti attributi nell'evento dead-letter per aiutarti a identificare e risolvere i possibili motivi per cui l'invocazione di Target non è riuscita.

- **ERROR\_CODE**— Contiene il codice di errore che EventBridge Scheduler riceve dal servizio della destinazione. API Nell'esempio precedente, il codice di errore restituito da Amazon SQS è `AWS.SimpleQueueService.NonExistentQueue`. Se la pianificazione non riesce a richiamare un obiettivo a causa di un problema con EventBridge Scheduler, vedrai invece il seguente codice di errore: `AWS.Scheduler.InternalServerError`
- **ERROR\_MESSAGE**— Contiene il messaggio di errore che EventBridge Scheduler riceve dal servizio della destinazione. API Nell'esempio precedente, il messaggio di errore restituito da Amazon SQS è `The specified queue does not exist for this wsdl version`. Se la pianificazione fallisce a causa di un problema con EventBridge Scheduler, vedrai invece il seguente messaggio di errore: `Unexpected error occurred while processing the request`
- **TARGET\_ARN**- La ARN destinazione richiamata dalla pianificazione, nel seguente formato di servizio ARN: `arn:aws:scheduler::aws-sdk:service:apiAction`
- **EXHAUSTED\_RETRY\_CONDITION**— Indica il motivo per cui l'evento è stato consegnato a DLQ. Questo attributo sarà presente se l'errore proveniente dalla destinazione API è un errore ripetibile e non un errore permanente. L'attributo può contenere i valori `MaximumRetryAttempts` se EventBridge Scheduler lo ha inviato DLQ dopo aver superato il numero massimo di tentativi configurato per la pianificazione oppure `MaximumEventAgeInSeconds` se l'evento è più vecchio dell'età massima configurata nella pianificazione e continua a non riuscire a consegnarlo.

Nell'esempio precedente, possiamo determinare, in base al codice di errore e al messaggio di errore, che la coda di destinazione specificata per la pianificazione non esiste.

## Eliminazione di una pianificazione in Scheduler EventBridge

È possibile eliminare una pianificazione configurando l'eliminazione automatica o eliminando manualmente una singola pianificazione. Utilizza gli argomenti seguenti per scoprire come eliminare una pianificazione utilizzando entrambi i metodi e perché potresti scegliere un metodo piuttosto che un altro.

## Argomenti

- [Eliminazione dopo il completamento della pianificazione](#)
- [Eliminazione manuale](#)

## Eliminazione dopo il completamento della pianificazione

Configura l'eliminazione automatica dopo il completamento della pianificazione se desideri evitare di dover gestire individualmente le risorse di EventBridge pianificazione su Scheduler. Nelle applicazioni in cui crei migliaia di pianificazioni alla volta e hai bisogno di flessibilità per aumentare il numero di pianificazioni su richiesta, l'eliminazione automatica può garantire che non venga raggiunta la quota del tuo account per il [numero di pianificazioni](#) in una determinata regione.

Quando si configura l'eliminazione automatica per una EventBridge pianificazione, Scheduler elimina la pianificazione dopo l'ultima chiamata alla destinazione. Per le pianificazioni una tantum, ciò si verifica dopo che la pianificazione ha richiamato la destinazione una volta. Per le pianificazioni ricorrenti impostate con espressioni rate o cron, la pianificazione viene eliminata dopo l'ultima chiamata. L'ultima chiamata di una pianificazione ricorrente è la chiamata che si verifica più vicino a quella specificata. [EndDate](#) Se si configura una pianificazione con l'eliminazione automatica ma non si specifica un valore per `EndDate`, EventBridge Scheduler non elimina automaticamente la pianificazione.

È possibile impostare l'eliminazione automatica quando si crea per la prima volta una pianificazione o aggiornare le preferenze per una pianificazione esistente. I passaggi seguenti descrivono come configurare l'eliminazione automatica per una pianificazione esistente.

### AWS Management Console

1. Apri la console EventBridge Scheduler all'indirizzo <https://console.aws.amazon.com/scheduler/>.
2. Dall'elenco delle pianificazioni, seleziona la pianificazione che desideri modificare, quindi scegli Modifica.
3. Dall'elenco di navigazione a sinistra, scegli Impostazioni.
4. Nella sezione Azione dopo il completamento della pianificazione, seleziona DELETE dall'elenco a discesa, quindi salva le modifiche.

## AWS CLI

1. Apri una nuova finestra di richiesta.
2. Utilizzate il AWS CLI comando [update-schedule](#) per aggiornare una pianificazione esistente, come illustrato di seguito. Il comando imposta il `--action-after-completion DELETE`. L'esempio presuppone che la configurazione di destinazione sia stata definita localmente in un JSON file. Per aggiornare una pianificazione, è necessario fornire l'obiettivo e tutti gli altri parametri di pianificazione che si desidera configurare per la pianificazione esistente.

Si tratta di una pianificazione ricorrente con una frequenza di una chiamata all'ora. Pertanto, si specifica una data di fine quando si imposta il parametro `--action-after-completion`

```
$ aws scheduler update-schedule --name schedule-name \
--action-after-completion 'DELETE' \
--schedule-expression 'rate(1 hour)' \
--end-date '2024-01-01T00:00:00' \
--target file://target-configuration.json \
--flexible-time-window '{ "Mode": "OFF" }' \
```

## Eliminazione manuale

Quando non è più necessaria una pianificazione, è possibile eliminarla utilizzando l'[DeleteSchedule](#) operazione.

### Example AWS CLI

```
$ aws scheduler delete-schedule --name your-schedule
```

### Example Python SDK

```
import boto3
scheduler = boto3.client('scheduler')

scheduler.delete_schedule(Name="your-schedule")
```

## Fasi successive

- Per ulteriori informazioni su come configurare target basati su modelli per Lambda e Step Functions e per imparare a usare il parametro universal target, consulta. [Gestione degli obiettivi](#)
- [Per ulteriori informazioni sui tipi di dati e sulle API operazioni dello EventBridge Scheduler, consulta lo Scheduler Reference. EventBridge API](#)

# Gestione di un gruppo di pianificazioni in EventBridge Scheduler

Un gruppo di pianificazione è una risorsa Amazon EventBridge Scheduler che usi per organizzare le tue pianificazioni.

Il tuo Account AWS viene fornito con un gruppo di default scheduler. Puoi associare una nuova pianificazione al default gruppo o ai gruppi di pianificazione che crei e gestisci. Puoi creare fino a [500 gruppi di pianificazione](#) nel tuo Account AWS. Con EventBridge Scheduler, puoi organizzare gruppi di pianificazioni, anziché singole pianificazioni, applicando [tag](#).

Un tag è un'etichetta composta da una chiave con distinzione tra maiuscole e minuscole e un valore con distinzione tra maiuscole e minuscole definiti dall'utente. È possibile creare tag per classificare le pianificazioni in base a criteri quali scopo, proprietario o ambiente. Ad esempio, puoi identificare l'ambiente a cui appartengono le tue pianificazioni con il seguente tag: `environment:production`.

## Important

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti AWS servizi, inclusa la fatturazione. I tag non sono destinati ad essere utilizzati per dati privati o sensibili.

Un gruppo di pianificazione ha due [stati](#) possibili: ACTIVE e DELETING.

La prima volta che crei un gruppo, lo è ACTIVE per impostazione predefinita. È possibile aggiungere pianificazioni a un ACTIVE gruppo. Quando si elimina un gruppo, lo stato cambia DELETING fino a quando EventBridge Scheduler non completa l'eliminazione delle pianificazioni associate. Dopo che EventBridge Scheduler ha eliminato le pianificazioni nel gruppo, il gruppo non è più disponibile nel tuo account.

Utilizza i seguenti argomenti per creare un gruppo di pianificazioni e applicarvi un tag. Inoltre assocerai una pianificazione al gruppo. Infine, eliminerai il gruppo.

## Argomenti

- [Creazione di un gruppo di pianificazione in EventBridge Scheduler](#)
- [Eliminazione di un gruppo di pianificazioni in EventBridge Scheduler](#)

- [Risorse correlate](#)

## Creazione di un gruppo di pianificazione in EventBridge Scheduler

Utilizza i gruppi di pianificazione e i tag per organizzare pianificazioni che condividono uno scopo comune o appartengono allo stesso ambiente. Nei passaggi seguenti, create un nuovo gruppo di pianificazioni e lo etichettate utilizzando un tag. Quindi associ una nuova pianificazione a quel gruppo.

### Note

Una volta creato un gruppo, non puoi rimuovere una pianificazione da quel gruppo o associare la pianificazione a un gruppo diverso. Puoi associare una pianificazione a un gruppo solo quando la crei per la prima volta.

## Fase uno: creare un nuovo gruppo di pianificazioni

I seguenti argomenti descrivono come creare un nuovo gruppo di pianificazioni ed etichettarlo con il seguente tag: `environment:development`.

### AWS Management Console

Per creare un nuovo gruppo utilizzando il AWS Management Console

1. Accedi a AWS Management Console e apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel riquadro di navigazione a sinistra, scegli Pianifica gruppi.
3. Nella pagina Gruppi di pianificazione, scegli Crea gruppo di pianificazione.
4. Nella sezione Dettagli del gruppo di pianificazione, in Nome, inserisci un nome per il gruppo. Ad esempio **TestGroup**.
5. Nella sezione Tag, procedi come segue:
  - a. Scegli Aggiungi nuovo tag.
  - b. Per Chiave, inserisci il nome che desideri assegnare a questa chiave. Per questo tutorial, per etichettare l'ambiente a cui appartiene questo gruppo di pianificazione, inserisci **environment**.

- c. Per Valore, facoltativo, inserisci il valore che desideri assegnare a questa chiave. Per questo tutorial, inserisci il valore della tua chiave **development** di ambiente.

 Note

Puoi aggiungere altri tag al tuo gruppo dopo averlo creato.

6. Per finire, scegli Crea gruppo di pianificazione. Il tuo nuovo gruppo viene visualizzato nell'elenco dei gruppi di pianificazione.
7. (Facoltativo) Per modificare un gruppo o gestirne i tag, seleziona la casella di controllo relativa al nuovo gruppo e scegli Modifica.

 Note

Non puoi modificare il gruppo di default pianificazione.

## AWS CLI

Per creare un nuovo gruppo utilizzando il AWS CLI

1. Aprire il prompt dei comandi in una nuova finestra.
2. Da AWS Command Line Interface (AWS CLI), immettete il seguente [create-schedule-group](#) comando per creare un nuovo gruppo. Questo comando crea un gruppo con un tag: `environment:development`. È possibile utilizzare questo tag o un sistema di etichettatura simile per etichettare i gruppi di pianificazione in base all'ambiente a cui appartengono.

Sostituisci il nome della pianificazione e la chiave e il valore del tag con le tue informazioni.

```
$ aws scheduler create-schedule-group --name TestGroup --tags  
Key=environment,Value=development
```

Per impostazione predefinita, il nuovo gruppo si trova nello ACTIVE stato. Ora puoi associare nuove pianificazioni al nuovo gruppo che hai creato.

## Fase due: associazione di una pianificazione al gruppo

Utilizza i seguenti passaggi per associare una nuova pianificazione al gruppo creato nel [passaggio precedente](#).

### AWS Management Console

Per associare una pianificazione a un gruppo utilizzando il AWS Management Console

1. Accedi a AWS Management Console e apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel riquadro di navigazione a sinistra, scegli Pianificazioni nel riquadro di navigazione a sinistra.
3. Dalla tabella Pianificazioni, scegli Crea pianificazione per creare una nuova pianificazione.
4. Nella pagina Specificare i dettagli della pianificazione, per il gruppo Pianificazione, seleziona il nome del nuovo gruppo dall'elenco a discesa. Ad esempio, seleziona `TestGroup`.
5. Specificate uno schema di pianificazione, un obiettivo, le impostazioni, quindi rivedete la selezione nella pagina Rivedi e salva la pianificazione. Per ulteriori informazioni sulla configurazione di una nuova pianificazione, vedere [Nozioni di base](#).
6. Per completare e salvare la pianificazione, scegli Salva pianificazione.

### AWS CLI

Per associare una pianificazione a un gruppo utilizzando il AWS CLI

1. Aprire il prompt dei comandi in una nuova finestra.
2. Da AWS Command Line Interface (AWS CLI), immettete il seguente [create-schedule](#) comando. Questo crea una pianificazione e la associa al gruppo del [passaggio precedente](#), denominato `sqs-test-schedule`. Questa pianificazione utilizza il tipo di SQS destinazione [Amazon basato su](#) modelli per richiamare l'operazione. `SendMessage` Sostituisci il nome della pianificazione, il nome del target e del gruppo con le tue informazioni.

```
$ aws scheduler create-schedule --name sqs-test-schedule --schedule-expression  
'rate(5 minutes)' \  
--target '{"RoleArn": "ROLE_ARN", "Arn": "QUEUE_ARN", "Input": "TEST_PAYLOAD" }'  
\   
--group-name TestGroup
```

```
--flexible-time-window '{ "Mode": "OFF"}
```

La tua nuova pianificazione è ora associata al gruppo di TestGroup pianificazione.

## Eliminazione di un gruppo di pianificazioni in EventBridge Scheduler

Di seguito, puoi scoprire come eliminare un gruppo di pianificazioni utilizzando AWS Management Console e il AWS Command Line Interface. Quando si elimina un gruppo, questo rimane DELETING nello stato fino a quando EventBridge Scheduler non elimina tutte le pianificazioni del gruppo. Dopo che EventBridge Scheduler ha eliminato le pianificazioni nel gruppo, il gruppo non è più disponibile nel tuo account.

### Note

Una volta creato un gruppo, non puoi rimuovere una pianificazione da quel gruppo o associare la pianificazione a un gruppo diverso. Puoi associare una pianificazione a un gruppo solo quando la crei per la prima volta.

### AWS Management Console

Per eliminare un gruppo utilizzando il AWS Management Console

1. Accedi a AWS Management Console e apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel riquadro di navigazione a sinistra, scegli Pianifica gruppi nel riquadro di navigazione a sinistra.
3. Nella pagina Pianifica i gruppi, individua il gruppo che desideri eliminare dall'elenco dei gruppi esistenti nell'elenco corrente Regione AWS. Se non vedi il gruppo che stai cercando, scegline un altro Regione AWS.

### Note

Non puoi eliminare o modificare il gruppo predefinito.

4. Seleziona la casella di controllo relativa al gruppo che desideri eliminare.

5. Scegli Elimina.
6. Nella finestra di dialogo Elimina gruppo di pianificazione, inserisci il nome del gruppo per confermare la scelta, quindi scegli Elimina.
7. Nell'elenco dei gruppi di pianificazione, la colonna Stato cambia per indicare che il gruppo è in corso di eliminazione. Il gruppo rimane in questo stato finché EventBridge Scheduler non elimina tutte le pianificazioni associate al gruppo.
8. Per aggiornare l'elenco e confermare che il gruppo è stato eliminato, scegli l'icona Aggiorna.

## AWS CLI

Per eliminare un gruppo utilizzando il AWS CLI

1. Aprire il prompt dei comandi in una nuova finestra.
2. Da AWS Command Line Interface (AWS CLI), immettete il seguente [delete-schedule-group](#) comando per eliminare il gruppo di pianificazioni. Sostituisci il valore di `--name` con le tue informazioni.

```
$ aws scheduler delete-schedule-group --name TestGroup
```

In caso di successo, questa AWS CLI operazione non restituisce una risposta.

3. Per verificare che il gruppo sia nello DELETING stato, esegui il [get-schedule-group](#) comando seguente.

```
$ aws scheduler get-schedule-group --name TestGroup
```

In caso di successo, riceverete un output simile al seguente:

```
{
  "Arn": "arn:aws::scheduler:us-west-2:123456789012:schedule-group/TestGroup",
  "CreationDate": "2023-01-01T09:00:00.000000-07:00",
  "LastModificationDate": "2023-01-01T09:00:00.000000-07:00",
  "Name": "TestGroup",
  "State": "DELETING"
}
```

EventBridge Scheduler elimina il gruppo dopo aver eliminato le pianificazioni associate al gruppo. Se si esegue di `get-schedule-group` nuovo, si riceve la seguente risposta: `ResourceNotFoundException`

```
An error occurred (ResourceNotFoundException) when calling the GetScheduleGroup operation: Schedule group TestGroup does not exist.
```

## Risorse correlate

Per ulteriori informazioni sui gruppi di pianificazione, consulta le seguenti risorse:

- [CreateScheduleGroup](#) operazione nello EventBridge Scheduler API Reference.
- [DeleteScheduleGroup](#) operazione nello EventBridge Scheduler API Reference.

# Gestione degli obiettivi in EventBridge Scheduler

I seguenti argomenti descrivono come utilizzare modelli e target universali con EventBridge Scheduler e forniscono un elenco di AWS servizi supportati che è possibile configurare utilizzando il parametro di destinazione universale di EventBridge Scheduler.

Gli obiettivi basati su modelli sono un insieme di API operazioni comuni su un gruppo di AWS servizi principali come Amazon, SQS Lambda e Step Functions. Ad esempio, puoi indirizzare l'API operazione [Invoke](#) di Lambda fornendo la funzione ARN o l'[SendMessage](#) operazione SQS di Amazon con la coda ARN della destinazione.

L'obiettivo universale è un set di parametri personalizzabile che consente di richiamare un set di API operazioni più ampio per molti servizi. AWS Ad esempio, puoi utilizzare il parametro di destinazione universale di EventBridge Scheduler (UTP) per creare una nuova SQS coda Amazon utilizzando l'[CreateQueue](#) operazione.

Per configurare obiettivi basati su modelli o universali, la tua pianificazione deve avere l'autorizzazione a richiamare l'API operazione che configuri come destinazione. A tale scopo, è necessario allegare le autorizzazioni richieste al ruolo di esecuzione della pianificazione. Ad esempio, per indirizzare [SendMessage](#) l'operazione SQS di Amazon, al ruolo di esecuzione viene concessa l'autorizzazione a eseguire l'`sqs:SendMessage` operazione. Nella maggior parte dei casi, puoi aggiungere le autorizzazioni necessarie utilizzando le [politiche AWS gestite](#) supportate dal servizio di destinazione. Tuttavia, puoi anche creare [politiche personalizzate gestite dai clienti](#) o aggiungere [autorizzazioni in linea](#) a una politica esistente associata al ruolo di esecuzione. Negli argomenti seguenti vengono illustrati esempi di aggiunta di autorizzazioni sia per i tipi di oggetto basati su modelli che per quelli universali.

Per ulteriori informazioni sulla configurazione di un ruolo di esecuzione per una pianificazione, vedere [the section called “Configurare il ruolo di esecuzione”](#)

## Argomenti

- [Utilizzo di obiettivi basati su modelli in Scheduler EventBridge](#)
- [Utilizzo di obiettivi universali in EventBridge Scheduler](#)
- [Aggiungere attributi di contesto in EventBridge Scheduler](#)
- [Fasi successive](#)

## Utilizzo di obiettivi basati su modelli in Scheduler EventBridge

Gli obiettivi basati su modelli sono un insieme di API operazioni comuni su un gruppo di AWS servizi principali, come Amazon, SQS Lambda e Step Functions. Ad esempio, puoi indirizzare [Invoke](#) l'operazione di Lambda fornendo la funzione ARN o l'[SendMessage](#) operazione SQS di Amazon utilizzando la coda ARN. Per configurare un target basato su modelli, devi anche concedere le autorizzazioni al ruolo di esecuzione della pianificazione per eseguire l'operazione di destinazione. API

Per configurare una destinazione basata su modelli in modo programmatico utilizzando lo Scheduler AWS CLI o uno degli EventBridge Scheduler SDKs, è necessario specificare il ruolo ARN di esecuzione, la risorsa ARN for target, un input opzionale che si desidera che EventBridge Scheduler fornisca alla destinazione e, per alcune destinazioni basate su modelli, un set unico di parametri con opzioni di configurazione aggiuntive per tale destinazione. Quando si specifica il ARN per una risorsa di destinazione basata su modelli, EventBridge Scheduler presuppone automaticamente che si desideri chiamare l'API operazione supportata per quel servizio. [Se si desidera che EventBridge Scheduler utilizzi come destinazione un'API operazione diversa per il servizio, è necessario configurare la destinazione come destinazione universale.](#)

Di seguito è riportato un elenco completo di tutte le destinazioni basate su modelli supportate da EventBridge Scheduler e, se applicabile, del set unico di parametri associati a ciascuna destinazione. Scegli il link per ogni set di parametri per visualizzare i campi obbligatori e facoltativi nello Scheduler Reference. EventBridge API

- CodeBuild – [StartBuild](#)
- CodePipeline – [StartPipelineExecution](#)
- Amazon ECS — [RunTask](#)
  - Parametri: [EcsParameters](#)
- EventBridge – [PutEvents](#)
  - Parametri: [EventBridgeParameters](#)
- Amazon Inspector — [StartAssessmentRun](#)
- Kinesis: [PutRecord](#)
  - Parametri: [KinesisParameters](#)
- Firehose — [PutRecord](#)
- Lambda – [Invoke](#)

- SageMaker – [StartPipelineExecution](#)
  - Parametri: [SageMakerPipelineParameters](#)
- Amazon SNS — [Publish](#)
- Amazon SQS — [SendMessage](#)
  - Parametri: [SqsParameters](#)
- Step Functions — [StartExecution](#)

Utilizza i seguenti esempi per imparare a configurare diverse destinazioni basate su modelli e le IAM autorizzazioni richieste per ciascuna destinazione descritta.

## Amazon SQS `SendMessage`

Example Politica di autorizzazione per il ruolo di esecuzione

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

Example AWS CLI

```
$ aws scheduler create-schedule --name sqs-templated --schedule-expression 'rate(5
minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn":"QUEUE_ARN", "Input": "Message for scheduleArn:
<aws.scheduler.schedule-arn>', scheduledTime: '<aws.scheduler.scheduled-time>"}' \
--flexible-time-window '{"Mode": "OFF"}'
```

Example Python SDK

```
import boto3
scheduler = boto3.client('scheduler')
```

```
flex_window = { "Mode": "OFF" }

sqs_templated = {
    "RoleArn": "<ROLE_ARN>",
    "Arn": "<QUEUE_ARN>",
    "Input": "Message for scheduleArn: '<aws.scheduler.schedule-arn>', scheduledTime:
'<aws.scheduler.scheduled-time>' "
}

scheduler.create_schedule(
    Name="sqs-python-templated",
    ScheduleExpression="rate(5 minutes)",
    Target=sqs_templated,
    FlexibleTimeWindow=flex_window)
```

## Example Java SDK

```
package com.example;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.scheduler.SchedulerClient;
import software.amazon.awssdk.services.scheduler.model.*;

public class MySchedulerApp {

    public static void main(String[] args) {

        final SchedulerClient client = SchedulerClient.builder()
            .region(Region.US_WEST_2)
            .build();

        Target sqsTarget = Target.builder()
            .roleArn("<ROLE_ARN>")
            .arn("<QUEUE_ARN>")
            .input("Message for scheduleArn: '<aws.scheduler.schedule-arn>',
scheduledTime: '<aws.scheduler.scheduled-time>'")
            .build();

        CreateScheduleRequest createScheduleRequest = CreateScheduleRequest.builder()
            .name("<SCHEDULE_NAME>")
            .scheduleExpression("rate(10 minutes)")
```

```

        .target(sqsTarget)
        .flexibleTimeWindow(FlexibleTimeWindow.builder()
            .mode(FlexibleTimeWindowMode.OFF)
            .build())
        .build();

    client.createSchedule(createScheduleRequest);
    System.out.println("Created schedule with rate expression and an Amazon SQS
templated target");
    }
}

```

## Lambda Invoke

Example Politica di autorizzazione per il ruolo di esecuzione

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}

```

Example AWS CLI

```

$ aws scheduler create-schedule --name lambda-templated-schedule --schedule-expression
'rate(5 minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn":"FUNCTION_ARN", "Input": "{ \"Payload\":
\"TEST_PAYLOAD\" }" }' \
--flexible-time-window '{ "Mode": "OFF"}'

```

Example Python SDK

```

import boto3
scheduler = boto3.client('scheduler')

```

```
flex_window = { "Mode": "OFF" }

lambda_templated = {
  "RoleArn": "<ROLE_ARN>",
  "Arn": "<LAMBDA_ARN>",
  "Input": "{ 'Payload': 'TEST_PAYLOAD' }"}
}

scheduler.create_schedule(
  Name="lambda-python-templated",
  ScheduleExpression="rate(5 minutes)",
  Target=lambda_templated,
  FlexibleTimeWindow=flex_window)
```

## Example Java SDK

```
package com.example;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.scheduler.SchedulerClient;
import software.amazon.awssdk.services.scheduler.model.*;

public class MySchedulerApp {

    public static void main(String[] args) {

        final SchedulerClient client = SchedulerClient.builder()
            .region(Region.US_WEST_2)
            .build();

        Target lambdaTarget = Target.builder()
            .roleArn("<ROLE_ARN>")
            .arn("<Lambda ARN>")
            .input("{ 'Payload': 'TEST_PAYLOAD' }")
            .build();

        CreateScheduleRequest createScheduleRequest = CreateScheduleRequest.builder()
            .name("<SCHEDULE_NAME>")
            .scheduleExpression("rate(10 minutes)")
            .target(lambdaTarget)
            .flexibleTimeWindow(FlexibleTimeWindow.builder()
                .mode(FlexibleTimeWindowMode.OFF)
```

```

        .build())
        .clientToken("<Token GUID>")
        .build());

    client.createSchedule(createScheduleRequest);
    System.out.println("Created schedule with rate expression and Lambda templated
target");
    }
}

```

## Step Functions **StartExecution**

Example Politica di autorizzazione per il ruolo di esecuzione

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "states:StartExecution"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}

```

Example AWS CLI

```

$ aws scheduler create-schedule --name sfn-templated-schedule --schedule-expression
'rate(5 minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn": "STATE_MACHINE_ARN", "Input": "{ \"Payload\":
\"TEST_PAYLOAD\" }" }' \
--flexible-time-window '{ "Mode": "OFF"}'

```

Example Python SDK

```

import boto3
scheduler = boto3.client('scheduler')

flex_window = { "Mode": "OFF" }

```

```
sfn_templated= {
  "RoleArn": "<ROLE_ARN>",
  "Arn": "<STATE_MACHINE_ARN>",
  "Input": "{ 'Payload': 'TEST_PAYLOAD' }"
}

scheduler.create_schedule(Name="sfn-python-templated",
  ScheduleExpression="rate(5 minutes)",
  Target=sfn_templated,
  FlexibleTimeWindow=flex_window)
```

## Example Java SDK

```
package com.example;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.scheduler.SchedulerClient;
import software.amazon.awssdk.services.scheduler.model.*;

public class MySchedulerApp {

    public static void main(String[] args) {

        final SchedulerClient client = SchedulerClient.builder()
            .region(Region.US_WEST_2)
            .build();

        Target stepFunctionsTarget = Target.builder()
            .roleArn("<ROLE_ARN>")
            .arn("<STATE_MACHINE_ARN>")
            .input("{ 'Payload': 'TEST_PAYLOAD' }")
            .build();

        CreateScheduleRequest createScheduleRequest = CreateScheduleRequest.builder()
            .name("<SCHEDULE_NAME>")
            .scheduleExpression("rate(10 minutes)")
            .target(stepFunctionsTarget)
            .flexibleTimeWindow(FlexibleTimeWindow.builder()
                .mode(FlexibleTimeWindowMode.OFF)
                .build())
            .clientToken("<Token GUID>")
            .build();
```

```
        client.createSchedule(createScheduleRequest);
        System.out.println("Created schedule with rate expression and Step Function
templated target");
    }
}
```

## Utilizzo di obiettivi universali in EventBridge Scheduler

Un target universale è un set di parametri personalizzabile che consente di richiamare un set di API operazioni più ampio per molti servizi. AWS Ad esempio, puoi utilizzare un parametro di destinazione universale (UTP) per creare una nuova SQS coda Amazon utilizzando l'[CreateQueue](#) operazione.

Per configurare un obiettivo universale per la tua pianificazione utilizzando lo AWS CLI Scheduler o uno degli EventBridge Scheduler SDKs, devi specificare le seguenti informazioni:

- **RoleArn**— Il ruolo ARN di esecuzione che si desidera utilizzare per l'obiettivo. Il ruolo di esecuzione specificato deve disporre delle autorizzazioni per chiamare l'API operazione a cui si desidera indirizzare la pianificazione.
- **Arn**: il servizio completo ARN, inclusa l'API operazione a cui desideri rivolgerti, nel seguente formato: `arn:aws:scheduler:::aws-sdk:service:apiAction`

Ad esempio, per AmazonSQS, il nome del servizio specificato è `arn:aws:scheduler:::aws-sdk:sqs:sendMessage`.

- **Input**: un formato ben formato JSON che specifichi con i parametri di richiesta che EventBridge Scheduler invia alla destinazione. API I parametri e la forma del JSON file impostato Input sono determinati dal servizio richiamato API dalla pianificazione. Per trovare queste informazioni, consulta il API riferimento per il servizio che desideri scegliere come target.

## Azioni non supportate

EventBridge Scheduler non supporta API azioni di sola lettura, come le GET operazioni comuni, che iniziano con il seguente elenco di prefissi:

```
get
describe
list
poll
receive
```

```
search
scan
query
select
read
lookup
discover
validate
batchGet
batchDescribe
batchRead
transactGet
adminGet
adminList
testMigration
retrieve
testConnection
translateDocument
isAuthorized
invokeModel
```

Ad esempio, il servizio ARN per l'[GetQueueUrl](#) API azione sarebbe il seguente:

```
arn:aws:scheduler::aws-sdk:sqs:getQueueURL
```

Poiché l'API azione inizia con il get prefisso, EventBridge Scheduler non supporta questa destinazione. Allo stesso modo, l'azione Amazon MQ non [ListBrokers](#) è supportata come destinazione perché l'operazione inizia con il prefisso. list

## Esempi che utilizzano il target universale

I parametri passati nel Input campo di pianificazione dipendono dai parametri di richiesta accettati dal servizio che API si desidera richiamare. [Ad esempio, per scegliere come target Lambda Invoke, puoi impostare i parametri elencati in AWS Lambda API Reference.](#) Ciò include il JSON [payload](#) opzionale che è possibile passare a una funzione Lambda.

Per determinare i parametri che puoi impostare per diversi tipi API, consulta il API riferimento per quel servizio. Analogamente a LambdaInvoke, alcuni API accettano URI parametri e un payload del corpo della richiesta. In questi casi, si specificano i parametri del URI percorso e il JSON payload nella pianificazione. Input

Gli esempi seguenti mostrano come utilizzare il target universale per richiamare API operazioni comuni con Lambda, SQS Amazon e Step Functions.

## Example Lambda

```
$ aws scheduler create-schedule --name lambda-universal-schedule --schedule-expression
'rate(5 minutes)' \
--target '{"RoleArn": "ROLE_ARN", "Arn": "arn:aws:scheduler::aws-sdk:lambda:invoke"
"Input": "{\"FunctionName\": \"arn:aws:lambda:REGION:123456789012:function:HelloWorld
\", \"InvocationType\": \"Event\", \"Payload\": \"{\\\"message\\\": \\\"testing function\\
\\\"}\" }' \
--flexible-time-window '{ "Mode": "OFF" }'
```

## Example Amazon SQS

```
import boto3
scheduler = boto3.client('scheduler')

flex_window = { "Mode": "OFF" }

sqs_universal= {
    "RoleArn": "<ROLE_ARN>",
    "Arn": "arn:aws:scheduler::aws-sdk:sqs:sendMessage",
    "Input": "{\"MessageBody\": \"My message\", \"QueueUrl\": \"<QUEUE_URL>\"}"
}

scheduler.create_schedule(
    Name="sqs-sdk-test",
    ScheduleExpression="rate(5 minutes)",
    Target=sqs_universal,
    FlexibleTimeWindow=flex_window)
```

## Example Step Functions

```
package com.example;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.scheduler.SchedulerClient;
import software.amazon.awssdk.services.scheduler.model.*;

public class MySchedulerApp {

    public static void main(String[] args) {
```

```

    final SchedulerClient client = SchedulerClient.builder()
        .region(Region.US_WEST_2)
        .build();

    Target stepFunctionsUniversalTarget = Target.builder()
        .roleArn("<ROLE_ARN>")
        .arn("arn:aws:scheduler::aws-sdk:sfn:startExecution")
        .input("{\"Input\": \"{}\", \"StateMachineArn\": \"<STATE_MACHINE_ARN>\"}")
        .build();

    CreateScheduleRequest createScheduleRequest = CreateScheduleRequest.builder()
        .name("<SCHEDULE_NAME>")
        .scheduleExpression("rate(10 minutes)")
        .target(stepFunctionsUniversalTarget)
        .flexibleTimeWindow(FlexibleTimeWindow.builder()
            .mode(FlexibleTimeWindowMode.OFF)
            .build())
        .clientToken("<Token GUID>")
        .build();

    client.createSchedule(createScheduleRequest);
    System.out.println("Created schedule with rate expression and Step Function
universal target");
}
}

```

## Aggiungere attributi di contesto in EventBridge Scheduler

Utilizza le seguenti parole chiave nel payload che passi alla destinazione per raccogliere i metadati relativi alla pianificazione. EventBridge Scheduler sostituisce ogni parola chiave con il rispettivo valore quando la pianificazione richiama l'obiettivo.

- **<aws.scheduler.schedule-arn>**— Il calendario. ARN
- **<aws.scheduler.scheduled-time>**— L'ora specificata per la pianificazione per richiamare la destinazione, 2022-03-22T18:59:43Z ad esempio.
- **<aws.scheduler.execution-id>**— L'ID univoco che EventBridge Scheduler assegna per ogni tentativo di invocazione di un obiettivo, ad esempio, d32c5kddcf5bb8c3
- **<aws.scheduler.attempt-number>**— Un contatore che identifica il numero del tentativo per la chiamata corrente, ad esempio, 1

Questo esempio mostra la creazione di una pianificazione che si attiva ogni cinque minuti e richiama l'SQSSendMessageoperazione Amazon come obiettivo universale. Il corpo del messaggio include il valore per. schedule-time

### Example AWS CLI

```
$ aws scheduler create-schedule --name your-schedule \  
  --schedule-expression 'rate(5 minutes)' \  
  --target '{"RoleArn": "ROLE_ARN", \  
    "Arn": "arn:aws:scheduler::aws-sdk:sqs:sendMessage", \  
    "Input": "{\\"MessageBody\\":\\"<aws.scheduler.scheduled-time>\\"",\\"QueueUrl\\":  
\\"https://sqs.us-west-2.amazonaws.com/123456789012/scheduler-cli-test\\"}"}' \  
  --flexible-time-window '{"Mode": "OFF"}'
```

### Example Python SDK

```
import boto3  
scheduler = boto3.client('scheduler')  
  
sqs_universal= {  
    "RoleArn": "<ROLE_ARN>",  
    "Arn": "arn:aws:scheduler::aws-sdk:sqs:sendMessage",  
    "Input": "{\\"MessageBody\\":\\"<aws.scheduler.scheduled-time>\\"",\\"QueueUrl\\":  
\\"https://sqs.us-west-2.amazonaws.com/123456789012/scheduler-cli-test\\"}"  
}  
  
flex_window = { "Mode": "OFF" }  
  
scheduler.update_schedule(Name="your-schedule",  
    ScheduleExpression="rate(5 minutes)",  
    Target=sqs_universal,  
    FlexibleTimeWindow=flex_window)
```

## Fasi successive

Per ulteriori informazioni sui tipi di dati e sulle API operazioni dello EventBridge Scheduler, vedere [EventBridge Scheduler API Reference](#).

# Sicurezza in Amazon EventBridge Scheduler

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- **Sicurezza del cloud:** AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei [AWS Programmi di AWS conformità dei Programmi di conformità](#) dei di . Per informazioni sui programmi di conformità che si applicano ad Amazon EventBridge Scheduler, consulta [AWS Services in Scope by Compliance Program AWS](#) .
- **Sicurezza nel cloud:** la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza EventBridge Scheduler. I seguenti argomenti mostrano come configurare EventBridge Scheduler per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse di EventBridge Scheduler.

## Argomenti

- [Gestione dell'accesso ad Amazon EventBridge Scheduler](#)
- [Protezione dei dati in Amazon EventBridge Scheduler](#)
- [Convalida della conformità per Amazon EventBridge Scheduler](#)
- [Resilienza in Amazon Scheduler EventBridge](#)
- [Sicurezza dell'infrastruttura in Amazon EventBridge Scheduler](#)

## Gestione dell'accesso ad Amazon EventBridge Scheduler

AWS Identity and Access Management (IAM) è uno strumento AWS servizio che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAM gli amministratori

controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (dispone delle autorizzazioni) a utilizzare le risorse di Scheduler. EventBridge IAM è un programma AWS servizio che puoi utilizzare senza costi aggiuntivi.

## Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come funziona EventBridge Scheduler con IAM](#)
- [Utilizzo di politiche basate sull'identità in Scheduler EventBridge](#)
- [Vice prevenzione confusa in Scheduler EventBridge](#)
- [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon EventBridge Scheduler](#)

## Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in EventBridge Scheduler.

**Utente del servizio:** se utilizzi il servizio EventBridge Scheduler per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di EventBridge Scheduler per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di EventBridge Scheduler, consulta [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon EventBridge Scheduler](#)

**Amministratore del servizio:** se sei responsabile delle risorse di EventBridge Scheduler presso la tua azienda, probabilmente hai pieno accesso a EventBridge Scheduler. È tuo compito determinare a quali funzionalità e risorse di EventBridge Scheduler devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAM amministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base di IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM EventBridge Scheduler, consulta [Come funziona EventBridge Scheduler con IAM](#).

**IAM amministratore:** se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso a EventBridge Scheduler. Per visualizzare esempi di policy basate

sull'identità di EventBridge Scheduler che puoi utilizzare in, consulta. IAM [Utilizzo di politiche basate sull'identità in Scheduler EventBridge](#)

## Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta [Firmare AWS API le richieste](#) nella Guida per l'IAMutente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta [Autenticazione a più fattori](#) nella Guida per l'AWS IAM Identity Center utente e [Utilizzo dell'autenticazione a più fattori \(MFA\) AWS nella Guida per l'IAMutente](#).

## Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte AWS servizi le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root

può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'IAMutente.

## Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere AWS servizi utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le AWS servizi credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per informazioni su IAM Identity Center, vedi [Cos'è IAM Identity Center?](#) nella Guida AWS IAM Identity Center per l'utente.

## IAM users and groups

Un [IAMutente](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta [Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente. IAM

Un [IAMgruppo](#) è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile assegnare un nome a un gruppo IAMAdminse concedere a tale gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali

temporanee. Per ulteriori informazioni, consulta [Quando creare un IAM utente \(anziché un ruolo\)](#) nella Guida per l'IAMutente.

## IAMruoli

Un [IAMruolo](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console [cambiando ruolo](#). È possibile assumere un ruolo chiamando un' AWS API/operazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere [Utilizzo IAM dei ruoli](#) nella Guida per l'IAMutente.

IAMI ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, vedere [Creazione di un ruolo per un provider di identità di terze parti](#) nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in IAM. Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .
- **Autorizzazioni IAM utente temporanee:** un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso su più account:** puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni AWS servizi, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la [sezione Accesso alle risorse su più account IAM nella Guida per l'utente](#). IAM
- **Accesso tra servizi:** alcuni AWS servizi utilizzano funzionalità in altri AWS servizi. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - **Sessioni di accesso diretto (FAS):** quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire

un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un AWS servizio, in combinazione con la richiesta di effettuare richieste AWS servizio ai servizi downstream. FAS le richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).

- Ruolo di servizio: un ruolo di servizio è un [IAM ruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, vedere [Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAM utente](#).
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un AWS servizio. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2 istanza e che effettuano AWS CLI o richiedono AWS API. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2 istanza. Per assegnare un AWS ruolo a un'EC2 istanza e renderlo disponibile per tutte le sue applicazioni, crea un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta [Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAM utente](#).

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta [Quando creare un IAM ruolo \(anziché un utente\)](#) nella Guida per l'IAM utente.

## Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere [Panoramica delle JSON politiche](#) nella Guida per l'IAM utente.

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAM le politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

## Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. [Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM](#)

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta [Scelta tra politiche gestite e politiche in linea nella Guida](#) per l'IAM utente.

## Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite contenute IAM in una policy basata sulle risorse.

## Elenchi di controllo degli accessi (ACLs)

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la [panoramica di Access control list \(ACL\)](#) nella Amazon Simple Storage Service Developer Guide.

## Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- **Limiti delle autorizzazioni:** un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. [Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente.](#) IAM IAM
- **Politiche di controllo del servizio (SCPs):** SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCP Limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations and SCPs, consulta [le politiche di controllo dei servizi](#) nella Guida AWS Organizations per l'utente.
- **Policy di sessione:** le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [le politiche di sessione](#) nella Guida IAM per l'utente.

## Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle politiche](#) nella Guida per l'IAMutente.

## Come funziona EventBridge Scheduler con IAM

Prima di utilizzare Scheduler IAM per gestire l'accesso a EventBridge Scheduler, scopri quali IAM funzionalità sono disponibili per l'uso con EventBridge Scheduler.

IAMfunzionalità che puoi usare con Amazon EventBridge Scheduler

IAMfunzionalità	EventBridge supporto Scheduler
<a href="#">Policy basate su identità</a>	Sì
<a href="#">Policy basate su risorse</a>	No
<a href="#">Azioni di policy</a>	Sì
<a href="#">Risorse relative alle policy</a>	Sì
<a href="#">Chiavi di condizione della policy (specifica del servizio)</a>	Sì
<a href="#">ACLs</a>	No
<a href="#">ABAC(tag nelle politiche)</a>	Parziale
<a href="#">Credenziali temporanee</a>	Sì
<a href="#">Autorizzazioni del principale</a>	Sì
<a href="#">Ruoli di servizio</a>	Sì
<a href="#">Ruoli collegati al servizio</a>	No

Per avere una panoramica generale del funzionamento di EventBridge Scheduler e degli altri AWS servizi con la maggior parte delle IAM funzionalità, consulta [AWS i servizi che funzionano con IAM nella Guida](#) per l'IAMutente.

## Politiche basate sull'identità per Scheduler EventBridge

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. [Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM](#)

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il [riferimento agli elementi IAM JSON della politica](#) nella Guida per l'IAMutente.

Esempi di policy basate sull'identità per Scheduler EventBridge

Per visualizzare esempi di politiche basate sull'identità di EventBridge Scheduler, vedere. [Utilizzo di politiche basate sull'identità in Scheduler EventBridge](#)

## Politiche basate sulle risorse all'interno di Scheduler EventBridge

Supporta le policy basate su risorse: no

Le politiche basate sulle risorse sono documenti di policy allegati a JSON una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il

principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta la sezione [Cross Account Resource Access IAM nella Guida IAM per l'utente](#).

## Azioni politiche per EventBridge Scheduler

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'Actionelemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni EventBridge Scheduler, consulta [Actions defined by Amazon EventBridge Scheduler](#) nel Service Authorization Reference.

Le azioni politiche in EventBridge Scheduler utilizzano il seguente prefisso prima dell'azione:

```
scheduler
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [  
  "scheduler:action1",  
  "scheduler:action2"  
]
```

È possibile specificare più azioni tramite caratteri jolly (\*). Ad esempio, per specificare tutte le azioni che iniziano con la parola List, includi la seguente azione:

```
"Action": [  
  "scheduler:List*"  
]
```

## Risorse politiche per Scheduler EventBridge

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento Resource JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento Resource o un elemento NotResource. Come best practice, specifica una risorsa utilizzando il relativo [Amazon Resource Name \(ARN\)](#). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (\*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse EventBridge Scheduler e relativi ARNs, consulta [Resources defined by Amazon EventBridge Scheduler](#) nel Service Authorization Reference. Per sapere con quali azioni puoi specificare le caratteristiche ARN di ogni risorsa, consulta [Azioni definite da Amazon EventBridge Scheduler](#).

Per visualizzare esempi di politiche basate sull'identità di EventBridge Scheduler, consulta [Utilizzo di politiche basate sull'identità in Scheduler EventBridge](#)

## Chiavi relative alle condizioni delle policy per Scheduler EventBridge

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento Condition (o blocco Condition) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento Condition è facoltativo. Puoi compilare espressioni condizionali

che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi Condition in un'istruzione o più chiavi in un singolo elemento Condition, questi vengono valutati da AWS utilizzando un'operazione AND logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica OR. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta [gli elementi IAM della politica: variabili e tag](#) nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'IAM utente.

Per visualizzare un elenco delle chiavi di condizione di EventBridge Scheduler, consulta [Condition keys for Amazon EventBridge Scheduler](#) nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta [Azioni definite da Amazon EventBridge Scheduler](#).

Per visualizzare esempi di politiche basate sull'identità di EventBridge Scheduler, consulta [Utilizzo di politiche basate sull'identità in Scheduler EventBridge](#)

## ACLs in EventBridge Scheduler

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

## ABAC con Scheduler EventBridge

Supporti ABAC (tag nelle politiche): Parziale

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo

passo di ABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABAC è utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, vedere [Cos'è? ABAC](#) nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazione ABAC, consulta [Utilizzare il controllo di accesso basato sugli attributi \(ABAC\)](#) nella Guida per l'IAM utente.

## Utilizzo di credenziali temporanee con Scheduler EventBridge

Supporta le credenziali temporanee: sì

Alcuni AWS servizi non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che AWS servizi funzionano con credenziali temporanee, consulta la sezione [AWS servizi relativa alla funzionalità IAM nella Guida](#) per l'IAM utente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta [Passare a un ruolo \(console\)](#) nella Guida per l'IAM utente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere [Credenziali di sicurezza temporanee](#) in IAM.

## Autorizzazioni principali per diversi servizi per Scheduler EventBridge

Supporta sessioni di accesso diretto ( ) FAS: Sì

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un AWS servizio, in combinazione con la richiesta AWS servizio per effettuare richieste ai servizi downstream. FAS le richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).

## Ruoli di servizio per EventBridge Scheduler

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un [IAM ruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, vedere [Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAM utente](#).

### Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere EventBridge la funzionalità di Scheduler. Modifica i ruoli di servizio solo quando EventBridge Scheduler fornisce indicazioni in tal senso.

## Ruoli collegati ai servizi per Scheduler EventBridge

Supporta i ruoli collegati ai servizi: no

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un AWS servizio. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

[Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta AWS Servizi compatibili con IAM](#) Trova un servizio nella tabella che include un Yes nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

## Utilizzo di politiche basate sull'identità in Scheduler EventBridge

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse di Scheduler. EventBridge Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta [Creazione di IAM politiche](#) nella Guida per l'IAMutente.

Per dettagli sulle azioni e sui tipi di risorse definiti da EventBridge Scheduler, incluso il formato di ARNs per ogni tipo di risorsa, consulta [Azioni, risorse e chiavi di condizione per Amazon EventBridge Scheduler](#) nel Service Authorization Reference.

### Argomenti

- [Best practice per le policy](#)
- [EventBridge Autorizzazioni Scheduler](#)
- [AWS politiche gestite per Scheduler EventBridge](#)
- [Politiche gestite dal cliente per Scheduler EventBridge](#)
- [AWS aggiornamenti delle politiche gestite](#)

### Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di EventBridge Scheduler nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta [le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative](#) nella Guida per l'IAMutente.

- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta [Politiche](#) e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico AWS servizio, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta [Elementi IAM JSON della politica: Condizione](#) nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy ( ) e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere [Convalida delle policy di IAM Access Analyzer nella Guida per l'utente](#). IAM
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, consulta [Configurazione dell'API accesso MFA protetto nella Guida](#) per l'IAMutente.

Per ulteriori informazioni sulle procedure consigliate in IAM, consulta la sezione [Procedure consigliate in materia di sicurezza IAM nella Guida](#) per l'IAMutente.

## EventBridge Autorizzazioni Scheduler

Affinché un IAM principale (utente, gruppo o ruolo) possa creare pianificazioni in EventBridge Scheduler e accedere alle risorse di EventBridge Scheduler tramite la console o il API, il principale deve avere un set di autorizzazioni aggiunto alla propria politica di autorizzazione. È possibile configurare queste autorizzazioni in base alla funzione lavorativa del responsabile. Ad esempio, un utente o un ruolo che utilizza solo la console EventBridge Scheduler per visualizzare un elenco di pianificazioni esistenti non deve disporre delle autorizzazioni necessarie per chiamare l'operazione. `CreateSchedule` API Ti consigliamo di personalizzare le autorizzazioni basate sull'identità per fornire solo l'accesso con i privilegi minimi.

L'elenco seguente mostra le risorse di EventBridge Scheduler e le azioni supportate corrispondenti.

- Pianificazione
  - `scheduler:ListSchedules`
  - `scheduler:GetSchedule`
  - `scheduler:CreateSchedule`
  - `scheduler:UpdateSchedule`
  - `scheduler>DeleteSchedule`
- Gruppo di pianificazione
  - `scheduler:ListScheduleGroups`
  - `scheduler:GetScheduleGroup`
  - `scheduler:CreateScheduleGroup`
  - `scheduler>DeleteScheduleGroup`
  - `scheduler:ListTagsForResource`
  - `scheduler:TagResource`
  - `scheduler:UntagResource`

Puoi utilizzare le autorizzazioni di EventBridge Scheduler per creare le tue politiche gestite dai clienti da utilizzare con EventBridge Scheduler. È inoltre possibile utilizzare le politiche AWS gestite descritte nella sezione seguente per concedere le autorizzazioni necessarie per casi d'uso comuni senza dover gestire le proprie politiche.

## AWS politiche gestite per Scheduler EventBridge

AWS affronta molti casi d'uso comuni fornendo IAM politiche autonome che AWS creano e amministrano. Le policy gestite, dette anche predefinite, concedono le autorizzazioni necessarie per casi d'uso comune, in modo da non dover determinare quali autorizzazioni sono necessarie. Per ulteriori informazioni, consulta le [politiche AWS gestite nella Guida](#) per l'IAMutente. Le seguenti politiche AWS gestite che puoi allegare agli utenti del tuo account sono specifiche di EventBridge Scheduler:

- [the section called “AmazonEventBridgeSchedulerFullAccess”](#)— Garantisce l'accesso completo a EventBridge Scheduler utilizzando la console e il. API
- [the section called “AmazonEventBridgeSchedulerReadOnlyAccess”](#)— Concede l'accesso in sola lettura a Scheduler. EventBridge

## AmazonEventBridgeSchedulerFullAccess

La politica AmazonEventBridgeSchedulerFullAccess gestita concede le autorizzazioni per utilizzare tutte le azioni di EventBridge Scheduler per le pianificazioni e i gruppi di pianificazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "scheduler:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::*:role/*",
      "Condition": {
        "StringLike": {
          "iam:PassedToService": "scheduler.amazonaws.com"
        }
      }
    }
  ]
}
```

## AmazonEventBridgeSchedulerReadOnlyAccess

La politica AmazonEventBridgeSchedulerReadOnlyAccess gestita concede autorizzazioni di sola lettura per visualizzare i dettagli sulle pianificazioni e sui gruppi di pianificazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ]
    }
  ],
}
```

```

        "Resource": "*"
    }
]
}

```

## Politiche gestite dal cliente per Scheduler EventBridge

Utilizza i seguenti esempi per creare politiche personalizzate gestite dai clienti per EventBridge Scheduler. Le [politiche gestite dai clienti](#) consentono di concedere le autorizzazioni solo per le azioni e le risorse necessarie per le applicazioni e gli utenti del team in base alla funzione lavorativa del responsabile.

### Argomenti

- [Esempio: CreateSchedule](#)
- [Esempio: GetSchedule](#)
- [Esempio: UpdateSchedule](#)
- [Esempio: DeleteScheduleGroup](#)

### Esempio: **CreateSchedule**

Quando crei una nuova pianificazione, scegli se crittografare i tuoi dati su EventBridge Scheduler utilizzando una chiave o una chiave [Chiave di proprietà di AWS](#) gestita [dal cliente](#).

La seguente politica consente a un responsabile di creare una pianificazione e applicare la crittografia utilizzando un. Chiave di proprietà di AWS Con an Chiave di proprietà di AWS, AWS gestisce le risorse su AWS Key Management Service (AWS KMS) per te in modo da non aver bisogno di autorizzazioni aggiuntive con AWS KMS cui interagire.

```

{
  "Version": "2012-10-17",
  "Statement":
  [
    {
      "Action":
      [
        "scheduler:CreateSchedule"
      ],
      "Effect": "Allow",
      "Resource":

```

```

    [
      "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-
schedule-name"
    ]
  },
  {
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::123456789012:role/*",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "scheduler.amazonaws.com"
      }
    }
  }
]
}

```

Utilizza la seguente politica per consentire a un responsabile di creare una pianificazione e utilizzare una chiave gestita AWS KMS dal cliente per la crittografia. Per utilizzare una chiave gestita dal cliente, l'amministratore deve disporre dell'autorizzazione ad accedere alle AWS KMS risorse del tuo account. Questa politica consente l'accesso a una singola KMS chiave specificata da utilizzare per crittografare i dati su EventBridge Scheduler. In alternativa, puoi utilizzare un carattere wildcard (\*) per concedere l'accesso a tutte le chiavi di un account o a un sottoinsieme che corrisponde a un determinato modello di nome.

```

{
  "Version": "2012-10-17"
  "Statement":
  [
    {
      "Action":
      [
        "scheduler:CreateSchedule"
      ],
      "Effect": "Allow",
      "Resource":
      [
        "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-
schedule-name"
      ]
    },
  ],
}

```

```

    {
      "Action":
        [
          "kms:DescribeKey",
          "kms:GenerateDataKey",
          "kms:Decrypt"
        ],
      "Effect": "Allow",
      "Resource":
        [
          "arn:aws:kms:us-west-2:123456789012:key/my-key-id"
        ],
      "Conditions": {
        "StringLike": {
          "kms:ViaService": "scheduler.amazonaws.com",
          "kms:EncryptionContext:aws:scheduler:schedule:arn":
            "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-schedule-name"
        }
      }
    }
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/*",
      "Condition": {
        "StringLike": {
          "iam:PassedToService": "scheduler.amazonaws.com"
        }
      }
    }
  ]
}

```

## Esempio: **GetSchedule**

Utilizzate la seguente politica per consentire a un preside di ottenere informazioni su una pianificazione.

```

{
  "Version": "2012-10-17",
  "Statement":
    [
      {
        "Action":

```

```

    [
      "scheduler:GetSchedule"
    ],
    "Effect": "Allow",
    "Resource":
    [
      "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-
schedule-name"
    ]
  }
]
}

```

### Esempio: **UpdateSchedule**

Utilizza le seguenti politiche per consentire a un responsabile di aggiornare una pianificazione richiamando l'`scheduler:UpdateSchedule` azione. Analogamente `CreateSchedule`, la politica dipende dal fatto che la pianificazione utilizzi una chiave di crittografia AWS KMS Chiave di proprietà di AWS o una chiave gestita dal cliente per la crittografia. Per una pianificazione configurata con un Chiave di proprietà di AWS, utilizza la seguente politica:

```

{
  "Version": "2012-10-17",
  "Statement":
  [
    {
      "Action":
      [
        "scheduler:UpdateSchedule"
      ],
      "Effect": "Allow",
      "Resource":
      [
        "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-
schedule-name"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/*",
      "Condition": {
        "StringLike": {

```

```

        "iam:PassedToService": "scheduler.amazonaws.com"
    }
}
]
}

```

Per una pianificazione configurata con una chiave gestita dal cliente, utilizza la seguente politica. Questa politica include autorizzazioni aggiuntive che consentono a un principale di accedere alle AWS KMS risorse del tuo account:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "scheduler:UpdateSchedule"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-schedule-name"
      ],
    },
    {
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:kms:us-west-2:123456789012:key/my-key-id"
      ],
      "Conditions": {
        "StringLike": {
          "kms:ViaService": "scheduler.amazonaws.com",
          "kms:EncryptionContext:aws:scheduler:schedule:arn":
            "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-schedule-name"
        }
      }
    }
  ]
}

```

```

    }
  }
  {
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::123456789012:role/*",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "scheduler.amazonaws.com"
      }
    }
  }
]
}

```

### Esempio: **DeleteScheduleGroup**

Utilizza la seguente politica per consentire a un responsabile di eliminare un gruppo di pianificazioni. Quando si elimina un gruppo, si eliminano anche le pianificazioni associate a quel gruppo. Il responsabile che elimina il gruppo deve disporre dell'autorizzazione per eliminare anche le pianificazioni associate a quel gruppo. Questa politica concede l'autorizzazione principale a richiamare l'`scheduler:DeleteScheduleGroup` sui gruppi di pianificazioni specificati, nonché su tutte le pianificazioni del gruppo:

#### Note

EventBridge Scheduler non supporta la specificazione delle autorizzazioni a livello di risorsa per le singole pianificazioni. Ad esempio, la seguente dichiarazione non è valida e non deve essere inclusa nella politica:

```
"Resource": "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-schedule-name"
```

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "scheduler:DeleteSchedule",
      "Resource": "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/*"
    }
  ]
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": "scheduler:DeleteScheduleGroup",
      "Resource": "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/*",
      "Condition": {
        "StringLike": {
          "iam:PassedToService": "scheduler.amazonaws.com"
        }
      }
    }
  ]
}

```

## AWS aggiornamenti delle politiche gestite

Modifica	Descrizione	Data
<a href="#">the section called “AmazonEventBridgeSchedulerFullAccess”</a> — Nuova politica gestita	EventBridge Scheduler aggiunge il supporto per una nuova politica gestita che garantisce agli utenti l'accesso completo a tutte le risorse, incluse le pianificazioni e i gruppi di pianificazione.	10 novembre 2022
<a href="#">the section called “AmazonEventBridgeSchedulerReadOnlyAccess”</a> — Nuova politica gestita	EventBridge Scheduler aggiunge il supporto per una nuova policy gestita che garantisce agli utenti l'accesso in sola lettura a tutte le risorse, incluse le pianificazioni e i gruppi di pianificazione.	10 novembre 2022

Modifica	Descrizione	Data
EventBridge Scheduler ha iniziato a tenere traccia delle modifiche	EventBridge Scheduler ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	10 novembre 2022

## Vice prevenzione confusa in Scheduler EventBridge

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel AWS, l'impersonificazione tra servizi può portare alla confusione del problema del vicesceriffo. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Ti consigliamo di utilizzare le chiavi di contesto [aws:SourceArn](#) [aws:SourceAccount](#) global condition nel tuo ruolo di esecuzione della pianificazione per limitare le autorizzazioni concesse da EventBridge Scheduler a un altro servizio per accedere alla risorsa. Utilizza `aws:SourceArn` se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Il modo più efficace per proteggersi dal confuso problema del vice è utilizzare la chiave di contesto ARN della condizione `aws:SourceArn` globale con l'intera risorsa. La condizione seguente è valida per un singolo gruppo di pianificazione: `arn:aws:scheduler:*:123456789012:schedule-group/your-schedule-group`

Se non conosci l'intera ARN risorsa o se stai specificando più risorse, usa la chiave di condizione di contesto `aws:SourceArn` globale con caratteri jolly (\*) per le parti sconosciute di. ARN Ad esempio: `arn:aws:scheduler:*:123456789012:schedule-group/*`.

Il valore di `aws:SourceArn` deve essere il gruppo di EventBridge pianificazione Scheduler ARN a cui desideri applicare questa condizione.

**⚠ Important**

Non limitate l'`aws:SourceArn` a una pianificazione specifica o al prefisso del nome della pianificazione. Il gruppo ARN specificato deve essere un gruppo di pianificazioni.

L'esempio seguente mostra come utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition nella politica di attendibilità del ruolo di esecuzione per prevenire il problema del confuso vice:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "scheduler.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "aws:SourceArn": "arn:aws:scheduler:us-
west-2:123456789012:schedule-group/your-schedule-group"
        }
      }
    }
  ]
}
```

## Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon EventBridge Scheduler

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi comuni che potresti riscontrare quando lavori con EventBridge Scheduler e IAM

### Argomenti

- [Non sono autorizzato a eseguire un'azione in Scheduler EventBridge](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)

- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse di EventBridge Scheduler](#)

## Non sono autorizzato a eseguire un'azione in Scheduler EventBridge

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` tenta di utilizzare la console per visualizzare i dettagli su una `my-example-widget` risorsa fittizia ma non dispone delle autorizzazioni fittizie. scheduler: `GetWidget`

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: scheduler: GetWidget on resource: my-example-widget
```

In questo caso, la policy deve essere aggiornata in modo che Mateo possa accedere alla risorsa `my-example-widget` mediante l'operazione scheduler: `GetWidget`.

Se hai bisogno di assistenza, contatta l'amministratore. AWS L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'azione `iam:PassRole`, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a EventBridge Scheduler.

Alcuni AWS servizi consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in EventBridge Scheduler. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di assistenza, contatta l' AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse di EventBridge Scheduler

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se EventBridge Scheduler supporta queste funzionalità, consulta [Come funziona EventBridge Scheduler con IAM](#)
- Per informazioni su Account AWS come fornire l'accesso alle risorse di tua proprietà, consulta [Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà](#) nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a persone Account AWS di proprietà di terzi](#) nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso agli utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle [risorse tra account nella Guida per l'utente](#). IAM IAM

## Protezione dei dati in Amazon EventBridge Scheduler

Il modello di [responsabilità AWS condivisa modello](#) si applica alla protezione dei dati in Amazon EventBridge Scheduler. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della

protezione e delle attività di gestione per i AWS servizi utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione [Privacy dei dati FAQ](#). Per informazioni sulla protezione dei dati in Europa, consulta il [Modello di responsabilitàAWS condivisa e GDPR](#) il post sul blog sulla AWS sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS servizi.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di FIPS 140-3 moduli crittografici convalidati per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, vedere [Federal Information Processing Standard \(FIPS\) 140-3](#).

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con EventBridge Scheduler o altro AWS servizi utilizzando la console, API, AWS CLI o AWS SDKs. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per la fatturazione o i log di diagnostica. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

## Crittografia inattiva in Scheduler EventBridge

Questa sezione descrive come Amazon EventBridge Scheduler crittografa e decrittografa i dati inattivi. I dati inattivi sono dati archiviati in EventBridge Scheduler e nei componenti sottostanti del servizio. EventBridge Scheduler si integra con AWS Key Management Service (AWS KMS) per crittografare e decrittografare i dati utilizzando un [AWS KMS key](#). EventBridge [Scheduler supporta due tipi di KMS chiavi: Chiavi di proprietà di AWS e chiavi gestite dal cliente.](#)

**Note**

EventBridge Scheduler supporta solo l'utilizzo di chiavi di crittografia [simmetriche](#). KMS

Chiavi di proprietà di AWS sono KMS chiavi possedute e gestite da un AWS servizio per l'utilizzo in più account. AWS Sebbene gli utilizzi di Chiavi di proprietà di AWS EventBridge Scheduler non siano memorizzati nel tuo AWS account, EventBridge Scheduler li utilizza per proteggere i tuoi dati e le tue risorse. Per impostazione predefinita, EventBridge Scheduler crittografa e decrittografa tutti i dati utilizzando una chiave proprietaria. AWS Non è necessario gestire la propria Chiave di proprietà di AWS o la relativa politica di accesso. Non dovrete sostenere alcuna commissione quando EventBridge Scheduler utilizza Scheduler Chiavi di proprietà di AWS per proteggere i vostri dati e il loro utilizzo non rientra nelle AWS KMS quote assegnate all'account.

Le chiavi gestite dal cliente sono KMS chiavi memorizzate nel tuo AWS account che crei, possiedi e gestisci. Se il tuo caso d'uso specifico richiede il controllo e la verifica delle chiavi di crittografia che proteggono i dati su EventBridge Scheduler, puoi utilizzare una chiave gestita dal cliente. Se scegli una chiave gestita dal cliente, devi gestire la tua politica delle chiavi. Le chiavi gestite dal cliente sono soggette a una tariffa mensile e a una tariffa qualora l'utilizzo superi i termini del piano gratuito. Anche l'utilizzo di una chiave gestita dal cliente fa parte della tua [AWS KMS quota](#). Per ulteriori informazioni sui prezzi, consulta la pagina [AWS Key Management Service dei prezzi](#).

**Argomenti**

- [Artefatti di crittografia](#)
- [Gestione delle chiavi KMS](#)
- [CloudTrail esempio di evento](#)

**Artefatti di crittografia**

La tabella seguente descrive i diversi tipi di dati che EventBridge Scheduler crittografa quando sono inattivi e il tipo di KMS chiave supportato per ogni categoria.

Tipo di dati	Descrizione	Chiave di proprietà di AWS	chiave gestita dal cliente
Carico utile (fino a 256 KB)	I dati che specifich i nel TargetInp	Supportato	Supportato

Tipo di dati	Descrizione	Chiave di proprietà di AWS	chiave gestita dal cliente
	ut parametro della pianificazione quando configuri la pianificazione da consegnare alla destinazione.		
Identificatore e stato	Il nome univoco e lo stato (abilitazione, disabilitazione) della pianificazione.	Supportato	Non supportato
Scheduling configuration (Configurazione della pianificazione)	L'espressione di pianificazione, ad esempio l'espressione rate o cron per le pianificazioni ricorrenti e il timestamp per le chiamate singole, nonché la data di inizio, la data di fine e il fuso orario della pianificazione.	Supportato	Non supportato
Configurazione di Target	Amazon Resource Name (ARN) della destinazione e altri dettagli di configurazione relativi alla destinazione.	Supportato	Non supportato

Tipo di dati	Descrizione	Chiave di proprietà di AWS	chiave gestita dal cliente
Configurazione del comportamento di invocazione e errore	Configurazione flessibile della finestra temporale, politica di riprova della pianificazione e dettagli sulla coda delle lettere non scritte utilizzati per le consegne non riuscite.	Supportato	Non supportato

EventBridge Scheduler utilizza le chiavi gestite dai clienti solo per crittografare e decrittografare il payload di destinazione, come descritto nella tabella precedente. Se si sceglie di utilizzare una chiave gestita dal cliente, EventBridge Scheduler crittografa e decrittografa il payload due volte: una volta utilizzando l'impostazione predefinita Chiave di proprietà di AWS e un'altra volta utilizzando la chiave gestita dal cliente specificata. Per tutti gli altri tipi di dati, EventBridge Scheduler utilizza solo l'impostazione predefinita Chiave di proprietà di AWS per proteggere i dati inattivi.

Utilizza la [the section called “Gestione delle chiavi KMS”](#) sezione seguente per scoprire come gestire IAM le risorse e le politiche chiave per utilizzare una chiave gestita dal cliente con EventBridge Scheduler.

## Gestione delle chiavi KMS

Se lo si desidera, è possibile fornire una chiave gestita dal cliente per crittografare e decrittografare il payload che la pianificazione distribuisce al destinatario. EventBridge Scheduler crittografa e decrittografa il payload fino a 256 KB di dati. L'utilizzo di una chiave gestita dal cliente comporta una tariffa mensile e una commissione superiore al piano gratuito. L'utilizzo di una chiave gestita dal cliente fa parte della tua [AWS KMS quota](#). Per ulteriori informazioni sui prezzi, consulta la sezione [AWS Key Management Service prezzi](#)

EventBridge Scheduler utilizza IAM le autorizzazioni associate al principale che crea una pianificazione per crittografare i dati. Ciò significa che è necessario assegnare le AWS KMS relative autorizzazioni richieste all'utente o al ruolo che chiama Scheduler. EventBridge API Inoltre, EventBridge Scheduler utilizza politiche basate sulle risorse per decrittografare i dati. Ciò significa

che il ruolo di esecuzione associato alla pianificazione deve disporre anche delle autorizzazioni AWS KMS correlate necessarie per richiamarlo durante la decrittografia dei dati. AWS KMS API

### Note

EventBridge Scheduler non supporta l'utilizzo di [concessioni](#) per autorizzazioni temporanee.

Utilizza la sezione seguente per scoprire come gestire la [politica AWS KMS chiave e le IAM autorizzazioni richieste per utilizzare una chiave](#) gestita dal cliente su Scheduler. EventBridge

### Argomenti

- [Aggiungi autorizzazioni IAM](#)
- [Gestisci la politica chiave](#)

### Aggiungi autorizzazioni IAM

Per utilizzare una chiave gestita dal cliente, è necessario aggiungere le seguenti autorizzazioni al IAM principio basato sull'identità che crea una pianificazione, nonché il ruolo di esecuzione associato alla pianificazione.

### Autorizzazioni basate sull'identità per le chiavi gestite dal cliente

È necessario aggiungere le seguenti AWS KMS azioni alla politica di autorizzazione associata a qualsiasi principale (utenti, gruppi o ruoli) che richiama lo EventBridge Scheduler durante la creazione di una pianificazione API.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "scheduler:*",

        # Required to pass the execution role
        "iam:PassRole",

        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*",
    "Effect": "Allow"
  },
]
}

```

- **kms:DescribeKey**— Obbligatorio per verificare che la chiave fornita sia una chiave di crittografia [simmetrica](#). KMS
- **kms:GenerateDataKey**— Richiesto per generare la chiave dati utilizzata da EventBridge Scheduler per eseguire la crittografia lato client.
- **kms:Decrypt**— Obbligatorio decrittografare la chiave dati crittografata che EventBridge Scheduler memorizza insieme ai dati crittografati.

Autorizzazioni per il ruolo di esecuzione per le chiavi gestite dal cliente

È necessario aggiungere la seguente azione alla politica di autorizzazione del ruolo di esecuzione della pianificazione per fornire l'accesso a EventBridge Scheduler da chiamare AWS KMS API durante la decrittografia dei dati.

```

{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Allow EventBridge Scheduler to decrypt data using a customer managed key",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:your-region:123456789012:key/your-key-id"
    }
  ]
}

```

- **kms:Decrypt**— Obbligatorio decrittografare la chiave dati crittografata che EventBridge Scheduler archivia insieme ai dati crittografati.

Se si utilizza la console EventBridge Scheduler per creare un nuovo ruolo di esecuzione quando si crea una nuova EventBridge pianificazione, Scheduler assegnerà automaticamente l'autorizzazione richiesta al ruolo di esecuzione. Tuttavia, se si sceglie un ruolo di esecuzione esistente, è necessario aggiungere le autorizzazioni richieste al ruolo per poter utilizzare le chiavi gestite dal cliente.

### Gestisci la politica chiave

Quando crei una chiave gestita dal cliente utilizzando AWS KMS, per impostazione predefinita, la tua chiave ha la seguente politica chiave per fornire l'accesso ai ruoli di esecuzione delle tue pianificazioni.

```
{
  "Id": "key-policy-1",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Provide required IAM Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": "kms:*",
      "Resource": "*"
    }
  ]
}
```

Facoltativamente, puoi limitare l'ambito della tua politica chiave in modo da fornire l'accesso solo al ruolo di esecuzione. È possibile eseguire questa operazione se si desidera utilizzare la chiave gestita dai clienti solo con le risorse EventBridge Scheduler. Utilizza il seguente esempio di [policy chiave](#) per limitare le risorse di EventBridge Scheduler che possono utilizzare la tua chiave.

```
{
  "Id": "key-policy-2",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Provide required IAM Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::695325144837:root"
      },
    },
  ],
}
```

```

    "Action": "kms:*",
    "Resource": "*"
  },
  {
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:role/schedule-execution-role"
    },
    "Action": [
      "kms:Decrypt"
    ],
    "Resource": "*"
  }
]
}

```

## CloudTrail esempio di evento

AWS CloudTrail cattura tutti gli eventi API delle chiamate. Ciò include API le chiamate ogni volta che EventBridge Scheduler utilizza la chiave gestita dal cliente per decrittografare i dati. L'esempio seguente mostra una voce di CloudTrail evento che dimostra che EventBridge Scheduler utilizza l'`kms:Decrypt` utilizzando una chiave gestita dal cliente.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ABCDEABCD1AB12ABABAB0:70abcd123a123a12345a1aa12aa1bc12",
    "arn": "arn:aws:sts::123456789012:assumed-role/execution-role/70abcd123a123a12345a1aa12aa1bc12",
    "accountId": "123456789012",
    "accessKeyId": "ABCDEFGH1JKLMNOP2Q3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ABCDEABCD1AB12ABABAB0",
        "arn": "arn:aws:iam::123456789012:role/execution-role",
        "accountId": "123456789012",
        "userName": "execution-role"
      },
      "webIdFederationData": {},
      "attributes": {

```

```
        "creationDate": "2022-10-31T21:03:15Z",
        "mfaAuthenticated": "false"
    }
},
"eventTime": "2022-10-31T21:03:15Z",
"eventSource": "kms.amazonaws.com",
"eventName": "Decrypt",
"awsRegion": "eu-north-1",
"sourceIPAddress": "13.50.87.173",
"userAgent": "aws-sdk-java/2.17.295 Linux/4.14.291-218.527.amzn2.x86_64 OpenJDK_64-
Bit_Server_VM/11.0.17+9-LTS Java/11.0.17 kotlin/1.3.72-release-468 (1.3.72) vendor/
Amazon.com_Inc. md/internal exec-env/AWS_ECS_FARGATE io/sync http/Apache cfg/retry-
mode/standard AwsCrypto/2.4.0",
"requestParameters": {
    "keyId": "arn:aws:kms:us-west-2:123456789012:key/2321abab-2110-12ab-a123-
a2b34c5abc67",
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "encryptionContext": {
        "aws:scheduler:schedule:arn": "arn:aws:scheduler:us-
west-2:123456789012:schedule/default/execution-role"
    }
},
"responseElements": null,
"requestID": "request-id",
"eventID": "event-id",
"readOnly": true,
"resources": [
    {
        "accountId": "123456789012",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-west-2:123456789012:key/2321abab-2110-12ab-a123-
a2b34c5abc67"
    }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_256_GCM_SHA384",
    "clientProvidedHostHeader": "kms.us-west-2.amazonaws.com"
}
```

}

## Crittografia in transito in Scheduler EventBridge

EventBridge Scheduler crittografa i dati in transito mentre viaggiano sulla rete. Transport Layer Security (TLS) crittografa i dati quando si richiama qualsiasi API operazione di EventBridge Scheduler, nonché quando EventBridge Scheduler chiama qualsiasi destinazione APIs quando richiama la pianificazione. Per impostazione predefinita, EventBridge Scheduler utilizza TLS 1.2 per crittografare i dati in transito. Non è necessario configurare la crittografia in transito e non è possibile scegliere una TLS versione diversa quando si utilizza EventBridge Scheduler.

Utilizzo dello EventBridge Scheduler API: quando si esegue un'API operazione, ad esempio `CreateSchedule`, EventBridge Scheduler crittografa l'intera HTTP richiesta, inclusi il corpo e le intestazioni della richiesta. EventBridge Scheduler crittografa anche l'intero oggetto di risposta che ricevi dal nostro. APIs

Utilizzo di target APIs: quando EventBridge Scheduler richiama la tua pianificazione, chiama la destinazione API che hai specificato quando hai creato la pianificazione. Quando invia un evento a un target, EventBridge Scheduler crittografa l'intera richiesta, incluso il corpo della richiesta e tutte le intestazioni, nonché la risposta che riceve dalla destinazione.

## Convalida della conformità per Amazon EventBridge Scheduler

Per sapere se un AWS servizio programma rientra nell'ambito di specifici programmi di conformità, consulta AWS servizi la sezione [Scope by Compliance Program AWS servizi](#) e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo AWS servizi è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Guide introduttive su sicurezza e conformità](#): queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.

- [Architettura per la HIPAA sicurezza e la conformità su Amazon Web Services](#): questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee. HIPAA

#### Note

Non tutte sono idonee. AWS servizi HIPAA Per ulteriori informazioni, consulta la [Guida ai servizi HIPAA idonei](#).

- [AWS Risorse per AWS](#) per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il tuo settore e la tua località.
- [AWS Guide alla conformità dei clienti](#): comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione AWS servizi e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization ()). ISO
- [Evaluating Resources with Rules](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- [AWS Security Hub](#)— Ciò AWS servizio fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina [Documentazione di riferimento sui controlli della Centrale di sicurezza](#).
- [Amazon GuardDuty](#): AWS servizio rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, ad esempio PCI DSS soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- [AWS Audit Manager](#)— Ciò AWS servizio consente di verificare continuamente AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

## Resilienza in Amazon Scheduler EventBridge

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza

interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

[Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS](#)

Oltre all'infrastruttura AWS globale, EventBridge Scheduler offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati.

## Sicurezza dell'infrastruttura in Amazon EventBridge Scheduler

In quanto servizio gestito, Amazon EventBridge Scheduler è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta [AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Si utilizzano le API chiamate AWS pubblicate per accedere a EventBridge Scheduler attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Suite di crittografia con perfetta segretezza di inoltro (PFS) come (Ephemeral Diffie-Hellman) o DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale. IAM In alternativa, è possibile utilizzare [AWS Security Token Service](#) (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

# Monitoraggio e parametri per Amazon EventBridge Scheduler

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon EventBridge Scheduler e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per guardare EventBridge Scheduler, segnalare quando qualcosa non va e intraprendere azioni automatiche se necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).
- AWS CloudTrail acquisisce le API chiamate e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di registro a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la [Guida per l'utente AWS CloudTrail](#).

## Argomenti

- [Monitoraggio di Amazon EventBridge Scheduler con Amazon CloudWatch](#)
- [Registrazione delle chiamate Amazon EventBridge Scheduler tramite API AWS CloudTrail](#)

## Monitoraggio di Amazon EventBridge Scheduler con Amazon CloudWatch

Puoi monitorare Amazon EventBridge Scheduler utilizzando CloudWatch, che raccoglie dati grezzi e li elabora in parametri leggibili quasi in tempo reale. EventBridge Scheduler emette una serie di parametri per tutte le pianificazioni e un set aggiuntivo di parametri per le pianificazioni a cui è associata una coda non valida (DLQ). Se [configuri una DLQ](#) per la tua pianificazione, EventBridge Scheduler pubblica metriche aggiuntive quando la pianificazione esaurisce la sua politica di ripetizione dei tentativi.

Queste statistiche vengono conservate per 15 mesi, in modo da poter accedere alle informazioni storiche e avere una prospettiva migliore sul motivo per cui una pianificazione non funziona e risolvere i problemi sottostanti. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).

## Argomenti

- [Termini](#)
- [Dimensioni](#)
- [Accesso ai parametri](#)
- [Elenco delle metriche](#)
- [EventBridge Metriche di utilizzo dello Scheduler](#)

## Termini

### Spazio dei nomi

Un namespace è un contenitore per le CloudWatch metriche di un servizio. AWS Per EventBridge Scheduler, lo spazio dei nomi è `AWS/Scheduler`

### CloudWatch metriche

Una CloudWatch metrica rappresenta un insieme ordinato nel tempo di punti dati specifici per CloudWatch

### Dimensione

Una dimensione è una coppia nome-valore che fa parte dell'identità di un parametro.

### Unità

Una statistica ha un'unità di misura. Per EventBridge Scheduler, le unità includono Count.

## Dimensioni

Questa sezione descrive il raggruppamento delle CloudWatch dimensioni per le metriche di EventBridge Scheduler in CloudWatch

Dimensione	Descrizione
ScheduleGroup	Il gruppo di pianificazioni per cui desideri visualizzare le metriche utilizzando CloudWatch. Se non hai ancora creato alcun gruppo, EventBridge Scheduler associa le tue pianificazioni al gruppo. default

## Accesso ai parametri

Questa sezione descrive come accedere alle metriche delle prestazioni CloudWatch per una pianificazione di Scheduler specifica EventBridge .

Per visualizzare le metriche delle prestazioni per una dimensione

1. Apri la [pagina Metriche](#) sulla console. CloudWatch
2. Usa il selettore AWS della regione per scegliere la regione per la tua pianificazione
3. Scegli lo spazio dei nomi Scheduler.
4. Nella scheda Tutte le metriche, scegli una dimensione, ad esempio Schedule Group Metrics. Per visualizzare le metriche per tutte le pianificazioni che hai creato nella regione selezionata, scegli Account Metrics.
5. Scegli una CloudWatch metrica per una dimensione. Ad esempio InvocationDroppedCount, InvocationAttemptCount oppure scegli Graph search.
6. Scegli la scheda Metriche grafiche per visualizzare le statistiche sulle prestazioni per le metriche di EventBridge Scheduler.

## Elenco delle metriche

Le tabelle seguenti elencano le metriche per tutte le EventBridge pianificazioni di Scheduler, oltre a metriche aggiuntive per le pianificazioni per le quali hai configurato un. DLQ

## Metriche per tutte le pianificazioni

Spazio dei nomi	Parametro	Unità	Descrizione
AWS/Scheduler	InvocationAttemptCount	Conteggio	Emesso per ogni tentativo di invocazione. Usa questa metrica per verificare che EventBridge Scheduler stia tentando di richiamare le tue pianificazioni e per vedere quando le chiamate si avvicinano alle quote del tuo account.
AWS/Scheduler	TargetErrorCount	Conteggio	Emesso quando il target restituisce un'eccezione dopo che Scheduler ha chiamato il target. EventBridge API Usalo per verificare quando la consegna a un obiettivo fallisce.
AWS/Scheduler	TargetErrorThrottledCount	Conteggio	Emesso quando l'invocazione del bersaglio fallisce a causa della API limitazione da parte del bersaglio. Usalo per diagnosticare gli errori di consegna quando il motivo di fondo è l'obiettivi

Spazio dei nomi	Parametro	Unità	Descrizione
			vo di limitare le chiamate effettuate da Scheduler API EventBridge
AWS/Scheduler	InvocationThrottleCount	Conteggio	Emesso quando EventBridge Scheduler limita una chiamata di destinazione perché supera le quote di servizio impostate da Scheduler. EventBridge Utilizzatelo per determinare quando avete superato la quota limite di limitazione delle chiamate. Per ulteriori informazioni sulle quote di servizio, vedere. <a href="#">Quote</a>

Spazio dei nomi	Parametro	Unità	Descrizione
AWS/Scheduler	InvocationDroppedCount	Conteggio	Emesso quando EventBridge Scheduler smette di tentare di richiamare il target dopo che la politica di riprova di una pianificazione è stata esaurita. Per ulteriori informazioni sulle politiche di riprova, consulta lo Scheduler Reference . <a href="#">RetryPolicy</a> EventBridge API

## Metriche per pianificazioni con un DLQ

Spazio dei nomi	Parametro	Unità	Descrizione
AWS/Scheduler	InvocationsSentToDeadLetterCount	Conteggio	Emesso per ogni consegna avvenuta con successo in base a una pianificazione. DLQ Usalo per determinare quando gli eventi vengono inviati a DLQ, quindi

Spazio dei nomi	Parametro	Unità	Descrizione
			controlla l'evento inviato alla pianificazione DLQ per ulteriori dettagli che ti aiutino a determinare la causa dell'errore.

Spazio dei nomi	Parametro	Unità	Descrizione
AWS/Scheduler	InvocationsFailedToBeSentToDeadLetterCount	Conteggio	Emesso quando EventBridge Scheduler non è in grado di fornire un evento a DLQ. Utilizza queste due metriche per determinare il motivo per cui EventBridge Scheduler non è in grado di inviare un evento a DLQ, e modifica la DLQ configurazione per risolvere il problema.
AWS/Scheduler	InvocationsFailedToBeSentToDeadLetterCount_<error_code>	Conteggio	Di seguito è riportato un esempio di <code>InvocationsFailedToBeSentToDeadLetterCount_&lt;error_code&gt;</code>

Spazio dei nomi	Parametro	Unità	Descrizione
			<p>&gt; metrica quando la SQS coda Amazon specificata come a DLQ non esiste: Invocatio nsFailedT oBeSentTo DeadLette rCount_ <b>AWS.Simp</b> <b>eQueueSer</b> <b>vice.NonE</b> <b>xistentQu</b> <b>eue</b></p>

Spazio dei nomi	Parametro	Unità	Descrizione
AWS/Scheduler	InvocationsSentToDeadLetterCount_Truncated_MessageSize Exceeded	Conteggio	Viene emesso quando il payload dell'evento inviato DLQ supera la dimensione e massima consentita da Amazon SQS e EventBridge Scheduler tronca il payload specifica to nell'attributo di una pianificazione. Input

## EventBridge Metriche di utilizzo dello Scheduler

CloudWatch raccoglie metriche che tengono traccia dell'utilizzo di alcune risorse. AWS Queste metriche corrispondono alle quote di servizio. AWS Il monitoraggio di questi parametri consente di gestire in modo proattivo le tue quote. Utilizza le seguenti metriche per determinare quando hai superato le quote dello Scheduler. EventBridge Per ulteriori informazioni sulle quote di servizio, consulta. [Quote](#)

Queste metriche sono contenute nel AWS/Usage namespace, anzichéAWS/Scheduler, e vengono raccolte ogni minuto.

Attualmente, l'unico nome di metrica in questo spazio dei nomi che pubblica è. CloudWatch CallCount Questo parametro viene pubblicato con le dimensioni Resource, Service e Type. La Resource dimensione specifica il nome dell'operazione da tracciare. API

Ad esempio, la `CallCount` metrica con le seguenti dimensioni indica il numero di volte in cui l'EventBridge Pianificatore `CreateScheduleAPI` operazione è stata chiamata nel tuo account:

- «Service»: «Scheduler»
- «Tipo»: "» API
- «Risorsa»: "CreateSchedule»

Il parametro `CallCount` non ha un'unità specificata. La statistica più utile per il parametro è `SUM`, che rappresenta il conteggio totale delle operazioni per il periodo di 1 minuto.

## Metriche

Parametro	Descrizione		
<code>CallCount</code>	Il numero di operazioni specificate eseguite nel tuo account.		

## Dimensioni

Dimensione	Descrizione		
<code>Service</code>	<p>Il nome del AWS servizio che contiene la risorsa.</p> <p>Per le metriche di Pianificatore EventBridge utilizzo, il valore per questa dimensione è <code>Scheduler</code>.</p>		
<code>Class</code>	<p>La classe della risorsa monitorata.</p> <p>Pianificatore EventBridge API le metriche di utilizzo utilizzano questa dimensione con un valore di <code>None</code>.</p>		
<code>Type</code>	Il tipo di risorsa monitorata.		

Dimensione	Descrizione		
	Attualmente, quando la dimensione è <code>Service</code> è <code>Scheduler</code> , l'unico valore valido per <code>Type</code> è <code>API</code> .		
Resource	<p>Il nome dell'API operazione. I valori validi includono i seguenti:</p> <ul style="list-style-type: none"> <li>• <code>CreateSchedule</code></li> <li>• <code>CreateScheduleGroup</code></li> <li>• <code>DeleteSchedule</code></li> <li>• <code>DeleteScheduleGroup</code></li> <li>• <code>GetSchedule</code></li> <li>• <code>GetScheduleGroup</code></li> <li>• <code>ListScheduleGroups</code></li> <li>• <code>ListSchedules</code></li> <li>• <code>ListTagsForResource</code></li> <li>• <code>TagResource</code></li> <li>• <code>UntagResource</code></li> <li>• <code>UpdateSchedule</code></li> </ul>		

## Registrazione delle chiamate Amazon EventBridge Scheduler tramite API AWS CloudTrail

Amazon EventBridge Scheduler è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in EventBridge Scheduler. CloudTrail acquisisce tutte le API chiamate per EventBridge Scheduler come eventi. Le chiamate acquisite includono chiamate dalla console EventBridge Scheduler e chiamate in codice alle operazioni di Scheduler. EventBridge API Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Scheduler. EventBridge Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta

effettuata a EventBridge Scheduler, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la [Guida per l'AWS CloudTrail utente](#).

## EventBridge Informazioni sullo scheduler in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in EventBridge Scheduler, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi in tuo Account AWS, inclusi gli eventi per EventBridge Scheduler, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un percorso](#)
- [CloudTrail servizi e integrazioni supportati](#)
- [Configurazione delle SNS notifiche Amazon per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Tutte le API azioni di EventBridge Scheduler vengono registrate CloudTrail e documentate in [Amazon EventBridge Scheduler Reference](#). API Ad esempio, le chiamate a `UpdateSchedule` e le `CreateSchedule` `DeleteSchedule` azioni generano voci nei file di registro. 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 root o AWS Identity and Access Management (IAM).
- 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 AWS servizio.

Per ulteriori informazioni, vedete l'[CloudTrail userIdentityelemento](#).

## Informazioni sulle voci EventBridge dei file di registro di Scheduler

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia stack ordinata delle API chiamate pubbliche, quindi non vengono visualizzati in un ordine specifico.

## Quote per Amazon EventBridge Scheduler

Il tuo AWS account dispone di quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica. Puoi richiedere aumenti per la maggior parte delle quote, ma alcune non possono essere aumentate.

Per visualizzare le quote per EventBridge Scheduler, apri la console [Service Quotas](#). Nel riquadro di navigazione, scegli AWS servizi, quindi seleziona Scheduler. EventBridge

Per richiedere un aumento delle quote, consultare [Richiesta di aumento delle quote](#) nella Guida dell'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il [modulo di incremento dei limiti](#).

Il tuo AWS account ha le seguenti quote relative a EventBridge Scheduler.

Nome	Predefinita	Adattate	Descrizione
CreateSchedule tariffa di richiesta	ca-central-1:250 eu-central-1: 1.000 Ogni altra regione supportata: 50	<a href="#">Sì</a>	Numero massimo di richieste al secondo CreateSchedule . Quando si raggiunge questa quota, EventBridge Scheduler rifiuta le richieste di questa operazione per il resto dell'intervallo.
CreateScheduleGroup tasso di richiesta	Ogni regione supportata: 10	<a href="#">Sì</a>	Numero massimo CreateScheduleGroup di richieste al secondo. Quando si raggiunge questa quota, EventBridge Scheduler rifiuta le richieste di questa operazione per il resto dell'intervallo.

Nome	Predefinita	Adattate	Descrizione
DeleteSchedule tasso di richiesta	ca-central-1:250 eu-central-1: 1.000 Ogni altra regione supportata: 50	<a href="#">Sì</a>	Numero massimo di richieste al secondo DeleteSchedule . Quando si raggiunge questa quota, EventBridge Scheduler rifiuta le richieste di questa operazione per il resto dell'intervallo.
DeleteScheduleGroup tasso di richiesta	Ogni regione supportata: 10	<a href="#">Sì</a>	Numero massimo DeleteScheduleGroup di richieste al secondo. Quando si raggiunge questa quota, EventBridge Scheduler rifiuta le richieste di questa operazione per il resto dell'intervallo.
GetSchedule tasso di richiesta	ca-central-1:250 eu-central-1: 1.000 Ogni altra regione supportata: 50	<a href="#">Sì</a>	Numero massimo di richieste al secondo GetSchedule . Quando si raggiunge questa quota, EventBridge Scheduler rifiuta le richieste di questa operazione per il resto dell'intervallo.

Nome	Predefinita	Adatta	Descrizione
GetScheduleGroup tasso di richiesta	Ogni regione supportata: 10	<a href="#">Sì</a>	Numero massimo GetScheduleGroup di richieste al secondo. Quando si raggiunge questa quota, EventBridge Scheduler rifiuta le richieste di questa operazione per il resto dell'intervallo.
Limite di invocazioni in transazioni al secondo	eu-central-1: 1.000 Ogni altra regione supportata: 500	<a href="#">Sì</a>	Una chiamata è un payload pianificato che viene consegnato alla destinazione definita. Una volta raggiunto il limite, le invocazioni vengono limitate, ovvero vengono comunque eseguite ma in ritardo.
ListScheduleGroups tasso di richiesta	Ogni regione supportata: 10	<a href="#">Sì</a>	Numero massimo ListScheduleGroups di richieste al secondo. Quando si raggiunge questa quota, EventBridge Scheduler rifiuta le richieste di questa operazione per il resto dell'intervallo.

Nome	Predefinita	Adattata	Descrizione
ListSchedules tasso di richiesta	Ogni Regione supportata: 50	<a href="#">Sì</a>	Numero massimo ListSchedules di richieste al secondo. Quando si raggiunge questa quota, EventBridge Scheduler rifiuta le richieste di questa operazione per il resto dell'intervallo.
ListTagsForResource tasso di richiesta	Ogni regione supportata: 10	<a href="#">Sì</a>	Elenca i tag associati alla risorsa Scheduler.
Numero di gruppi di pianificazione	Ogni regione supportata: 500	<a href="#">Sì</a>	Numero massimo di gruppi di pianificazione per regione.
Numero di pianificazioni	ca-central-1:10.000.000 eu-central-1:10.000.000 Ciascuna delle altre regioni supportate: 1.000.000	<a href="#">Sì</a>	Il numero massimo di pianificazioni per regione. Questa quota include le pianificazioni una tantum che sono state completate. Ti consigliamo di configurare le pianificazioni in modo che vengano eliminate automaticamente dopo il completamento dell'utilizzo della ActionAfterCompletion funzione.
TagResource tariffa di richiesta	Ogni regione supportata: 1	<a href="#">Sì</a>	Assegna uno o più tag (coppie chiave-valore) alla risorsa Scheduler specificata.

Nome	Predefinita	Adattate	Descrizione
UntagResource tariffa di richiesta	Ogni regione supportata: 1	<a href="#">Sì</a>	Rimuove uno o più tag dalla risorsa Scheduler specificata.
UpdateSchedule tariffa di richiesta	ca-central-1:250 eu-central-1: 1.000 Ogni altra regione supportata: 50	<a href="#">Sì</a>	Numero massimo di richieste al secondo UpdateSchedule . Quando si raggiunge questa quota, EventBridge Scheduler rifiuta le richieste di questa operazione per il resto dell'intervallo.

Per ulteriori informazioni sulle quote e gli endpoint di servizio per EventBridge Scheduler, consulta gli [endpoint e le quote di Amazon EventBridge Scheduler](#) nella guida di riferimento generale.AWS

## Risoluzione dei problemi relativi alle quote in Scheduler EventBridge

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare riguardo alle quote di EventBridge Scheduler.

### ServiceQuotaExceededException

Ricevo errori di limitazione relativi a, o alla frequenza delle UpdateSchedule richieste CreateSchedule DeleteScheduleGetSchedule, anche se sono al di sotto del limite di frequenza predefinito.

#### Causa comune

Il 7 settembre 2023, EventBridge Scheduler ha iniziato a supportare le ScheduleGroup ARN (Amazon Resource Name) anziché le politiche di fiducia del ruolo Schedule ARN in execution. I clienti

autorizzati a continuare a utilizzare Schedule ARNs nella loro politica di fiducia possono avere limiti di 50TPS, anziché i limiti predefiniti da 250 a 1000 TPS (a seconda della regione).

## Risoluzione

Contatta l'[assistenza](#) per richiedere un limite massimo più elevato.

## Prevenzione

Modifica le tue politiche di fiducia esistenti in uno dei seguenti modi:

- Rimozione di tutti gli ambiti dal ruolo.
- Definizione dell'ambito del ruolo in modo che possa essere assunto utilizzando Schedule ARN o. ScheduleGroup ARN

Ad esempio, supponiamo di avere la seguente politica di fiducia esistente:

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "scheduler.amazonaws.com"
  },
  "Action": "sts:AssumeRole",
  "Condition": {
    "StringEquals": {
      "aws:SourceArn":
"arn:aws:scheduler:region:account:schedule/schedule_group/schedule"
    }
  }
}
```

È possibile aggiornare la politica di fiducia nel modo seguente:

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "scheduler.amazonaws.com"
  },
  "Action": "sts:AssumeRole",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:SourceArn": [
```

```
    "arn:aws:scheduler:region:account:schedule/schedule_group/schedule",  
    "arn:aws:scheduler:region:account:schedule-group/schedule_group"  
  ]  
}  
}
```

# Cronologia dei documenti per la EventBridge Scheduler User Guide

La tabella seguente descrive le versioni della documentazione per EventBridge Scheduler.

Modifica	Descrizione	Data
<a href="#">Modifiche al ruolo di esecuzione e prevenzione confusa dei sostituti</a>	<p>Questo aggiornamento descrive le modifiche al modo in cui il ruolo di esecuzione viene applicato a una risorsa del gruppo di pianificazione quando si implementa la prevenzione della confusione e tra delegati nella politica di autorizzazione del ruolo.</p> <ul style="list-style-type: none"> <li><a href="#">the section called "Prevenzione del "confused deputy""</a></li> </ul>	7 settembre 2023
<a href="#">Eliminazione automatica delle pianificazioni dopo il completamento</a>	<p>EventBridge Scheduler supporta l'eliminazione automatica. Quando configuri l'eliminazione automatica, EventBridge Scheduler elimina la tua pianificazione dopo l'ultima chiamata pianificata.</p> <ul style="list-style-type: none"> <li><a href="#">the section called "Eliminazione dopo il completamento della pianificazione"</a></li> </ul>	2 agosto 2023
<a href="#">Argomento aggiornato sull'utilizzo degli obiettivi universali</a>	<p>È stato aggiornato l'elenco dei servizi supportati che EventBridge Scheduler può utilizzare come target e con cui può integrarsi. Questo</p>	17 marzo 2023

aggiornamento include anche un elenco di GET API operazioni non supportate e include miglioramenti agli esempi di Universal Target, oltre ad altri miglioramenti minori presenti in tutta la guida.

- [the section called “Utilizzo di obiettivi universali”](#)

[Informazioni aggiornate sulle pianificazioni basate sulle tariffe che non hanno una data di inizio](#)

Sono state aggiunte informazioni su come EventBridge Scheduler gestisce le pianificazioni basate sulla tariffa se non si specifica a. [StartDate](#)

17 marzo 2023

- [the section called “Pianificazioni basate sulle tariffe”](#)

[Nuovo argomento sulla gestione dei gruppi di scheduler](#)

Aggiunto un nuovo capitolo su come creare gruppi di scheduler con EventBridge Scheduler. Usa questo capitolo per imparare a creare un gruppo, aggiungere e pianificazioni al gruppo, applicare tag per gestire e monitorare più facilmente e le risorse di EventBridge Scheduler e infine eliminare un gruppo.

17 marzo 2023

- [Gestione di un gruppo di pianificazioni](#)

### [Nuovi argomenti sull'ora legale e sui fusi orari](#)

Sono state aggiunte nuove sezioni che descrivono come EventBridge Scheduler gestisce l'ora legale e come è possibile creare pianificazioni in fusi orari diversi.

17 novembre 2022

- [the section called “Ora legale”](#)
- [the section called “Fusi orari”](#)

### [Nuovo argomento sulle metriche](#)

È stato aggiunto un nuovo argomento che descrive le metriche su cui EventBridge Scheduler pubblica CloudWatch. È possibile utilizzare queste metriche per monitorare gli errori di chiamata e capire come risolvere i problemi relativi alle pianificazioni.

15 novembre 2022

- [the section called “Monitoraggio con CloudWatch”](#)

### [Versione iniziale](#)

Versione iniziale della Scheduler User Guide EventBridge .

10 novembre 2022

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.