



Guida per gli sviluppatori

Amazon Data Firehose



Amazon Data Firehose: Guida per gli sviluppatori

Copyright © 2026 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 dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

.....	x
Che cos'è Amazon Data Firehose	1
Scopri i concetti chiave	1
Comprendi il flusso di dati in Amazon Data Firehose	2
Lavorare con AWS SDKs	3
Prerequisiti completi per configurare Firehose	5
Registrati per AWS	5
(Facoltativo) Scarica librerie e strumenti	5
Tutorial: Creare uno stream Firehose	7
Scegli la fonte e la destinazione per il tuo stream Firehose	7
Configurazione delle impostazioni di origine	9
Configurazione delle impostazioni di origine per Amazon MSK	10
Configurazione delle impostazioni di origine per Amazon Kinesis Data Streams	11
(Facoltativo) Configurare la trasformazione dei record e la conversione del formato	12
Configurare le impostazioni di destinazione	14
Configurazione delle impostazioni di destinazione per Amazon S3	15
Configura le impostazioni di destinazione per Apache Iceberg Tables	19
Configurazione delle impostazioni di destinazione per Amazon Redshift	19
Configurare OpenSearch le impostazioni di destinazione per il servizio	25
Configura le impostazioni di destinazione per Serverless OpenSearch	28
Configura le impostazioni di destinazione per HTTP Endpoint	29
Configura le impostazioni di destinazione per Datadog	31
Configura le impostazioni di destinazione per Honeycomb	34
Configura le impostazioni di destinazione per Coralogix	35
Configura le impostazioni di destinazione per Dynatrace	37
Configura le impostazioni di destinazione per LogicMonitor	39
Configura le impostazioni di destinazione per Logz.io	41
Configurare le impostazioni di destinazione per MongoDB Atlas	43
Configura le impostazioni di destinazione per New Relic	45
Configura le impostazioni di destinazione per Snowflake	47
Configura le impostazioni di destinazione per Splunk	50
Configura le impostazioni di destinazione per Splunk Observability Cloud	53
Configura le impostazioni di destinazione per Sumo Logic	54
Configura le impostazioni di destinazione per Elastic	56

Configurare le impostazioni di backup	57
Configura i suggerimenti per il buffering	59
Configurare le impostazioni avanzate	62
Metti alla prova il tuo stream Firehose	64
Prerequisiti	64
Prova con Amazon S3	64
Esegui test con Amazon Redshift	65
Esegui il test con Service OpenSearch	66
Prova con Splunk	66
Prova con Apache Iceberg Tables	67
Inviare dati a uno stream Firehose	68
Configurare l'agente Kinesis per l'invio di dati	68
Prerequisiti	69
Gestisci le AWS credenziali	69
Crea provider di credenziali personalizzati	70
Scarica e installa l'agente	71
Configura e avvia l'agente	73
Specificare le impostazioni di configurazione dell'agente	74
Configura più directory e stream di file	78
Preelabora i dati con gli agenti	79
Usa i comandi CLI dell'agente comuni	83
Risolvi i problemi relativi all'invio da Kinesis Agent	84
Inviare dati con AWS SDK	86
Operazioni di scrittura singole utilizzando PutRecord	86
Operazioni di scrittura in batch utilizzando PutRecordBatch	87
Invia CloudWatch log a Firehose	87
Decomprimi i log CloudWatch	88
Estrai il messaggio dopo la decompressione dei registri CloudWatch	88
Abilitare la decompressione su un nuovo stream Firehose dalla console	89
Abilitare la decompressione su un flusso Firehose esistente	90
Disattiva la decompressione sullo stream Firehose	91
Risoluzione dei problemi di decompressione in Firehose	92
Invia CloudWatch eventi a Firehose	93
AWS IoT Configurare l'invio di dati a Firehose	94
Trasforma i dati di origine	95
Comprendi il flusso di trasformazione dei dati	95

Durata della chiamata Lambda	95
Parametri richiesti per la trasformazione dei dati	96
Blueprint Lambda supportati	97
Gestisci gli errori nella trasformazione dei dati	98
Esegui il backup dei record di origine	100
Partizione dei dati di streaming	101
Abilita il partizionamento dinamico	101
Comprendi le chiavi di partizionamento	102
Crea chiavi di partizionamento con analisi in linea	103
Crea chiavi di partizionamento con una funzione AWS Lambda	104
Usa il prefisso del bucket Amazon S3 per fornire dati	107
Aggiungi un nuovo delimitatore di riga durante la distribuzione di dati ad Amazon S3	109
Applica il partizionamento dinamico ai dati aggregati	109
Risolvi gli errori di partizionamento dinamico	110
Dati buffer per il partizionamento dinamico	110
Convertire il formato dei dati di input	112
Deserializer	112
Schema	113
Serializer	114
Abilita la conversione del formato di registrazione	114
Abilita la conversione del formato di registrazione dalla console	115
Gestione della conversione del formato di record dall'API Firehose	115
Gestione degli errori per la conversione del formato dei dati	116
Comprendi la distribuzione dei dati	117
Comprendi la distribuzione tra account e regioni AWS	120
Comprendi le specifiche di richiesta e risposta di consegna degli endpoint HTTP	120
Formato della richiesta	120
Formato della risposta	124
Esempi	127
Gestisci gli errori di consegna dei dati	128
Simple Storage Service (Amazon S3)	128
Amazon Redshift	129
Amazon OpenSearch Service e OpenSearch Serverless	129
Splunk	130
Destinazione endpoint HTTP	131
Snowflake	132

Configurazione del formato dei nomi degli oggetti Amazon S3	133
Comprendi i prefissi personalizzati per gli oggetti Amazon S3	142
Configura la rotazione dell'indice per Service OpenSearch	147
Sospendere e riprendere la consegna dei dati	148
Mettere in pausa uno stream Firehose	148
Riprendere uno stream Firehose	149
Fornisci dati a Apache Iceberg Tables	150
Considerazioni e limitazioni	150
Prerequisiti	153
Prerequisiti per la consegna a Iceberg Tables in Amazon S3	154
Prerequisiti per la distribuzione su Amazon S3 Tables	154
Configurare lo stream Firehose	155
Configurazione dell'origine e della destinazione	155
Configura la trasformazione dei dati	156
Connect data catalog	156
Configura le espressioni JQ	157
Configura chiavi univoche	157
Specificare la durata del nuovo tentativo	159
Gestire la consegna o l'elaborazione non riuscite	159
Handle errors	159
Configura i buffer hint	160
Configurare le impostazioni avanzate	160
Indirizza i record in entrata a una singola tabella Iceberg	161
Indirizza i record in entrata a diverse tabelle Iceberg	161
Fornire informazioni di routing a JSONQuery Firehose con espressione	162
Fornisci informazioni di routing utilizzando una funzione AWS Lambda	163
Monitoraggio di parametri	167
Comprendi i tipi di dati supportati	168
Esempi di tipi di dati	169
Resources	173
Etichetta uno stream Firehose	174
Comprendi le nozioni di base sui tag	174
Tieni traccia dei costi con l'etichettatura	175
Conosci le restrizioni relative ai tag	175
Sicurezza	177
Protezione dei dati	178

Crittografia lato server con Kinesis Data Streams	178
Crittografia lato server con Direct PUT o altre fonti di dati	178
Controllo dell'accesso	180
Concedi l'accesso alle tue risorse Firehose	181
Concedi a Firehose l'accesso al tuo cluster Amazon MSK privato	182
Consenti a Firehose di assumere un ruolo IAM	182
Concedi a Firehose l'accesso a AWS Glue per la conversione del formato dei dati	183
Concedi a Firehose l'accesso a una destinazione Amazon S3	184
Concedi a Firehose l'accesso alle tabelle Amazon S3	187
Concedi a Firehose l'accesso a una destinazione Apache Iceberg Tables	194
Concedi a Firehose l'accesso a una destinazione Amazon Redshift	195
Concedi a Firehose l'accesso a una destinazione di servizio pubblico OpenSearch	200
Concedere a Firehose l'accesso a una destinazione OpenSearch di servizio in un VPC	201
Concedere a Firehose l'accesso a una destinazione Serverless pubblica OpenSearch	202
Concedi a Firehose l'accesso a una destinazione OpenSearch Serverless in un VPC	205
Concedi a Firehose l'accesso a una destinazione Splunk	206
Accesso a Splunk in VPC	209
Tutorial: inserisci i log di flusso VPC in Splunk utilizzando Amazon Data Firehose	211
Accesso a Snowflake o all'endpoint HTTP	211
Concedi a Firehose l'accesso a una destinazione Snowflake	212
Accesso a Snowflake in VPC	214
Concedere a Firehose l'accesso a una destinazione endpoint HTTP	218
Consegna su più account da Amazon MSK	219
Consegna su più account a una destinazione Amazon S3	222
Consegna tra più account a una OpenSearch destinazione del servizio	223
Utilizzo dei tag per controllare l'accesso	225
Effettua l'autenticazione con Gestione dei segreti AWS	227
Comprendi i segreti	228
Creazione di un segreto	229
Usa il segreto	229
Ruota il segreto	231
Gestisci i ruoli IAM tramite console	231
Scegli un ruolo IAM esistente	232
Crea un nuovo ruolo IAM dalla console	232
Modifica il ruolo IAM dalla console	234
Convalida della conformità	236

Resilienza	236
Ripristino di emergenza	237
Comprendi la sicurezza dell'infrastruttura	237
Utilizzo di Firehose con AWS PrivateLink	238
Implementa le migliori pratiche di sicurezza	243
Implementazione dell'accesso con privilegi minimi	243
Uso di ruoli IAM	243
Implementa la crittografia lato server nelle risorse dipendenti	243
Utilizzato CloudTrail per monitorare le chiamate API	244
Monitoraggio di Amazon Data Firehose	245
Implementa le migliori pratiche con Alarms CloudWatch	245
Monitoraggio con metriche CloudWatch	246
CloudWatch metriche per il partizionamento dinamico	247
CloudWatch metriche per la distribuzione dei dati	248
Metriche di ingestione dei dati	262
Metriche a livello di API CloudWatch	271
CloudWatch Metriche di trasformazione dei dati	275
CloudWatch Registra le metriche di decompressione	275
Metriche di conversione del formato CloudWatch	276
Metriche di crittografia lato server (SSE) CloudWatch	277
Dimensioni per Amazon Data Firehose	278
Metriche di utilizzo di Amazon Data Firehose	278
CloudWatch Metriche di accesso per Amazon Data Firehose	279
Monitoraggio con log CloudWatch	280
Errori di consegna dei dati	281
CloudWatch Log di accesso per Amazon Data Firehose	318
Monitora lo stato di salute degli agenti	319
Monitora con CloudWatch	319
Registra le chiamate API Firehose	320
Informazioni su Firehose in CloudTrail	320
Esempio: voci del file di registro Firehose	322
Esempi di codice	327
Nozioni di base	327
Azioni	328
Scenari	339
Inserire i record in Firehose	340

Risoluzione degli errori	353
Problemi comuni	353
Stream Firehose non disponibile	354
Nessun dato a destinazione	354
La metrica di freschezza dei dati aumenta o non viene emessa	354
La conversione del formato di registrazione in Apache Parquet non riesce	355
Campi mancanti per l'oggetto trasformato per Lambda	356
Risoluzione dei problemi Amazon S3	357
Risoluzione dei problemi di Amazon Redshift	358
Risoluzione dei problemi con Amazon OpenSearch Service	359
Risoluzione dei problemi di Splunk	360
Risoluzione dei problemi relativi a Snowflake	362
La creazione dello stream Firehose non riesce	362
Risoluzione dei problemi di raggiungibilità degli endpoint Firehose	363
Risoluzione dei problemi degli endpoint HTTP	364
CloudWatch Registri	365
Risoluzione dei problemi relativi a MSK come origine	368
Creazione di hose non riuscita	368
Hose sospeso	369
Hose in contropressione	369
Aggiornamento dei dati non corretto	369
Problemi di connessione al cluster MSK	369
Quota	373
Cronologia dei documenti	377

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.

Cos'è Amazon Data Firehose?

Amazon Data Firehose è un servizio completamente gestito per la distribuzione di [dati di streaming](#) in tempo reale a destinazioni come Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Service, Amazon Serverless, Splunk OpenSearch , Apache Iceberg Tables e qualsiasi endpoint HTTP personalizzato o endpoint HTTP di proprietà di provider di servizi terzi supportati, tra cui LogicMonitor Datadog, Dynatrace, MongoDB MongoDB, New Relic, Coralogix ed Elastic. OpenSearch Con Amazon Data Firehose, non è necessario scrivere applicazioni o gestire risorse. Configurate i vostri produttori di dati per inviare dati ad Amazon Data Firehose, che li consegna automaticamente alla destinazione specificata. Puoi anche configurare Amazon Data Firehose per trasformare i tuoi dati prima di distribuirli.

Per ulteriori informazioni sulle soluzioni per i AWS big data, consulta [Big Data on AWS](#). Per ulteriori informazioni sulle soluzioni AWS per i dati in streaming, consulta [Cosa sono i dati in streaming?](#)

Scopri i concetti chiave

Quando inizi a usare Amazon Data Firehose, puoi trarre vantaggio dalla comprensione dei seguenti concetti.

Flusso Firehose

L'entità sottostante di Amazon Data Firehose. Puoi utilizzare Amazon Data Firehose creando uno stream Firehose e inviandogli dati. Per ulteriori informazioni, consultare [Tutorial: Creare uno stream Firehose dalla console](#) e [Inviare dati a uno stream Firehose](#).

Registra

I dati di interesse che il produttore di dati invia a uno stream Firehose. Un record può avere dimensioni fino a 1.000 KB.

Produttore di dati

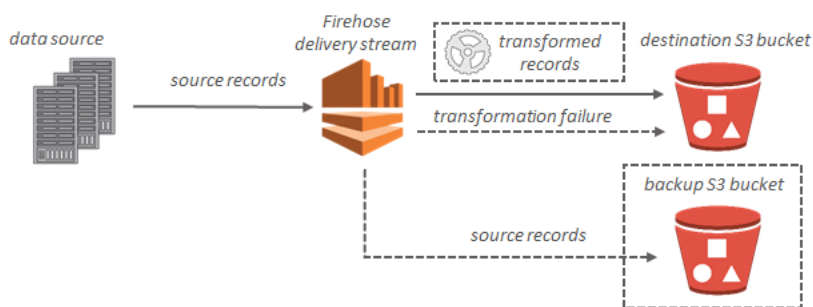
I produttori inviano i dischi agli stream di Firehose. Ad esempio, un server Web che invia dati di registro a un flusso Firehose è un produttore di dati. Puoi anche configurare lo stream Firehose per leggere automaticamente i dati da un flusso di dati Kinesis esistente e caricarli nelle destinazioni. Per ulteriori informazioni, consulta [Inviare dati a uno stream Firehose](#).

Dimensione e intervallo del buffer

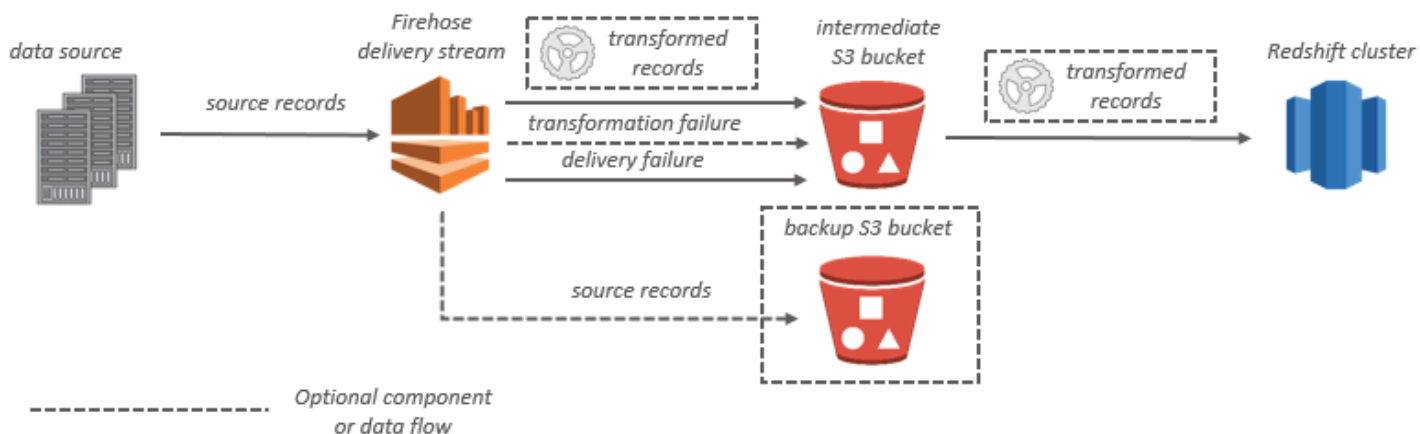
Amazon Data Firehose memorizza nel buffer i dati di streaming in entrata fino a una certa dimensione o per un determinato periodo di tempo prima di consegnarli alle destinazioni. Buffer Size è in MBs e lo è in pochi Buffer Interval secondi.

Comprendi il flusso di dati in Amazon Data Firehose

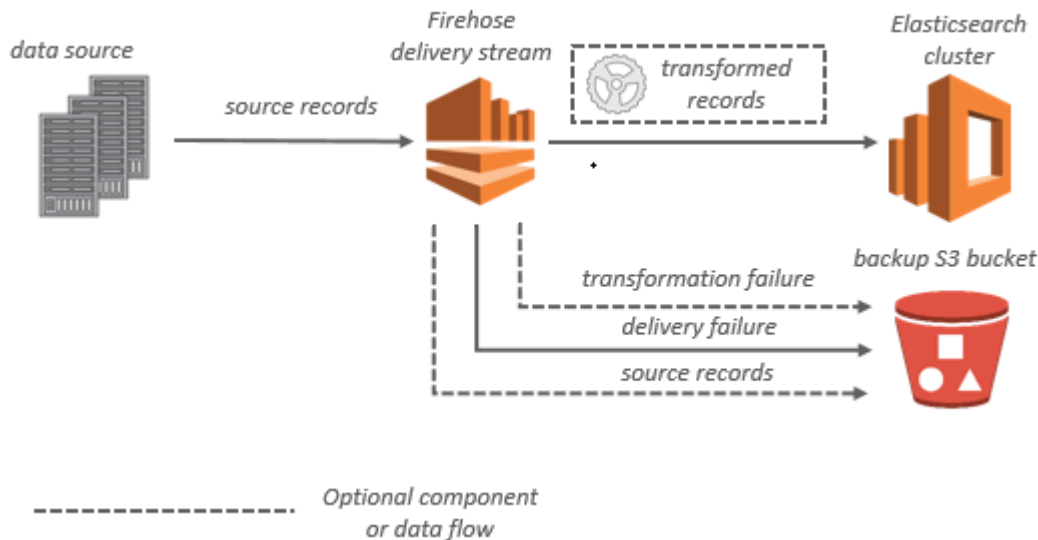
Per le destinazioni Amazon S3, i dati in streaming vengono distribuiti sul bucket S3. Se è abilitata la trasformazione dei dati, puoi scegliere di eseguire il backup dei dati di origine su un altro bucket Amazon S3.



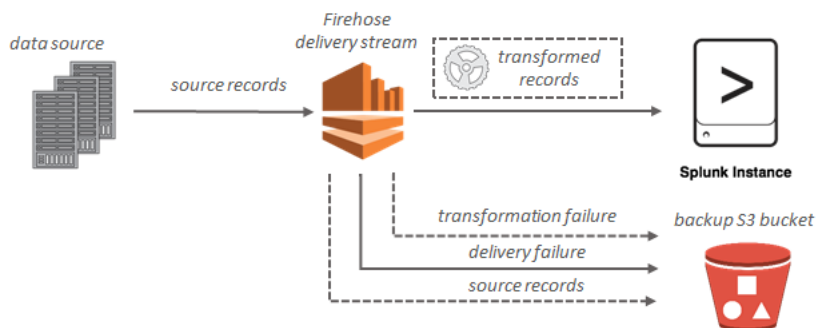
Per le destinazioni Amazon Redshift, i dati in streaming vengono distribuiti prima sul bucket S3. Amazon Data Firehose emette quindi un comando Amazon COPY Redshift per caricare i dati dal bucket S3 al cluster Amazon Redshift. Se è abilitata la trasformazione dei dati, puoi scegliere di eseguire il backup dei dati di origine su un altro bucket Amazon S3.



Per le destinazioni OpenSearch del servizio, i dati in streaming vengono distribuiti al cluster di OpenSearch servizio e, facoltativamente, possono essere sottoposti a backup contemporaneamente nel bucket S3.



Per le destinazioni Splunk, i dati in streaming vengono distribuiti su Splunk e se ne può eseguire contemporaneamente il backup sul bucket S3.



Utilizzo di Firehose con un SDK AWS

AWS i kit di sviluppo software (SDKs) sono disponibili per molti linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK

Esempi di codice

[AWS SDK per C++](#)

[AWS SDK per C++ esempi di codice](#)

Documentazione sugli SDK	Esempi di codice
AWS CLI	AWS CLI esempi di codice
AWS SDK per Go	AWS SDK per Go esempi di codice
AWS SDK per Java	AWS SDK per Java esempi di codice
AWS SDK per JavaScript	AWS SDK per JavaScript esempi di codice
AWS SDK per Kotlin	AWS SDK per Kotlin esempi di codice
AWS SDK per .NET	AWS SDK per .NET esempi di codice
AWS SDK per PHP	AWS SDK per PHP esempi di codice
AWS Strumenti per PowerShell	AWS Strumenti per PowerShell esempi di codice
AWS SDK per Python (Boto3)	AWS SDK per Python (Boto3) esempi di codice
AWS SDK per Ruby	AWS SDK per Ruby esempi di codice
AWS SDK per Rust	AWS SDK per Rust esempi di codice
AWS SDK per SAP ABAP	AWS SDK per SAP ABAP esempi di codice
AWS SDK per Swift	AWS SDK per Swift esempi di codice

Esempio di disponibilità

Non riesci a trovare quello che ti serve? Richiedi un esempio di codice utilizzando il link [Fornisci un feedback](#) nella parte inferiore di questa pagina.

Prerequisiti completi per configurare Amazon Data Firehose

Prima di utilizzare Amazon Data Firehose per la prima volta, completa le seguenti attività.

Processi

- [Registrati per AWS](#)
- [\(Facoltativo\) Scarica librerie e strumenti](#)

Registrati per AWS

Quando ti registri ad Amazon Web Services (AWS), il tuo AWS account viene automaticamente registrato per tutti i servizi in AWS, incluso Amazon Data Firehose. Ti vengono addebitati solo i servizi che utilizzi.

Se hai già un AWS account, passa all'attività successiva. Se non disponi di un account AWS , utilizza la seguente procedura per crearne uno.

Per creare 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 o un messaggio di testo e ti verrà chiesto di 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 Servizi AWS 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](#).

(Facoltativo) Scarica librerie e strumenti

Le seguenti librerie e strumenti ti aiuteranno a lavorare con Amazon Data Firehose a livello di codice e dalla riga di comando:

- [Firehose API Operations è il set di operazioni](#) di base supportato da Amazon Data Firehose.

- Le versioni AWS SDKs per [Go](#), [Java](#), [.NET](#), [Node.js](#), [Python](#) e [Ruby](#) **includono** il supporto e gli esempi di Amazon Data Firehose.

Se la tua versione di AWS SDK per Java non include esempi per Amazon Data Firehose, puoi anche scaricare l' AWS SDK più recente da [GitHub](#)

- [AWS Command Line Interface](#)Supporta Amazon Data Firehose. Ti AWS CLI consente di controllare più AWS servizi dalla riga di comando e di automatizzarli tramite script.

Tutorial: Creare uno stream Firehose dalla console

È possibile utilizzare Console di gestione AWS o un AWS SDK per creare uno stream Firehose verso la destinazione prescelta.

Puoi aggiornare la configurazione del tuo stream Firehose in qualsiasi momento dopo la creazione, utilizzando la console Amazon Data Firehose o [UpdateDestination](#). Lo stream Firehose rimane nello `Active` stato durante l'aggiornamento della configurazione e puoi continuare a inviare dati. Di norma la configurazione aggiornata entra in vigore entro pochi minuti. Il numero di versione di uno stream Firehose viene aumentato di un valore di 1 dopo l'aggiornamento della configurazione. Questo numero viene riportato nel nome oggetto Amazon S3 distribuito. Per ulteriori informazioni, consulta [Configurazione del formato dei nomi degli oggetti Amazon S3](#).

Eseguite i passaggi descritti nei seguenti argomenti per creare uno stream Firehose.

Argomenti

- [Scegli la fonte e la destinazione per il tuo stream Firehose](#)
- [Configurazione delle impostazioni di origine](#)
- [\(Facoltativo\) Configurare la trasformazione dei record e la conversione del formato](#)
- [Configurare le impostazioni di destinazione](#)
- [Configurare le impostazioni di backup](#)
- [Configurare le impostazioni avanzate](#)

Scegli la fonte e la destinazione per il tuo stream Firehose

1. Aprire la console Firehose all'indirizzo. <https://console.aws.amazon.com/firehose/>
2. Scegli Crea un flusso Firehose.
3. Nella pagina Crea stream Firehose, scegli una fonte per il tuo stream Firehose tra una delle seguenti opzioni.
 - **Direct PUT:** scegliete questa opzione per creare uno stream Firehose su cui le applicazioni di produzione scrivono direttamente. Di seguito è riportato un elenco di AWS servizi, agenti e servizi open source che si integrano con Direct PUT in Amazon Data Firehose. Questo elenco non è esaustivo e potrebbero esserci servizi aggiuntivi che possono essere utilizzati per inviare dati direttamente a Firehose.

- AWS SDK
- AWS Lambda
- AWS CloudWatch Tronchi
- AWS CloudWatch Eventi
- AWS Flussi metrici su cloud
- AWS IoT
- AWS Eventbridge
- Amazon Simple Email Service
- Amazon SNS
- AWS Registri ACL Web WAF
- Gateway Amazon API: log di accesso
- Amazon Pinpoint
- Log di broker Amazon MSK
- Log di query di risolutore Amazon Route 53
- AWS Registri degli avvisi del Network Firewall
- AWS Registri di flusso del Network Firewall
- Amazon Elasticache Redis SLOWLOG
- Kinesis Agent (Linux)
- Kinesis Tap (Windows)
- Fluentbit
- Fluentd
- Apache Nifi
- Snowflake
- Amazon Kinesis Data Streams: scegli questa opzione per configurare un flusso Firehose che utilizza un flusso di dati Kinesis come origine dati. È quindi possibile utilizzare Firehose per leggere facilmente i dati da un flusso di dati Kinesis esistente e caricarli nelle destinazioni. Per ulteriori informazioni sull'utilizzo di Kinesis Data Streams come origine dati, [consulta Invio di dati a un flusso Firehose con Kinesis](#) Data Streams.
- Amazon MSK: scegli questa opzione per configurare uno stream Firehose che utilizza Amazon MSK come origine dati. È quindi possibile utilizzare Firehose per leggere facilmente i dati da

un cluster Amazon MSK esistente e caricarli in bucket S3 specifici. Per ulteriori informazioni, consulta [Invio di dati a uno stream Firehose con Amazon MSK](#).

4. Scegliete una destinazione per il vostro stream Firehose tra una delle seguenti destinazioni supportate da Firehose.
 - OpenSearch Servizio Amazon
 - Amazon OpenSearch Serverless
 - Amazon Redshift
 - Amazon S3
 - Tabelle Apache Iceberg
 - Coralogix
 - Datadog
 - Dynatrace
 - Elastic
 - Endpoint HTTP
 - Honeycomb
 - Logic Monitor
 - Logz.io
 - MongoDB Cloud
 - New Relic
 - Splunk
 - Splunk Observability Cloud
 - Sumo Logic
 - Snowflake
5. Per il nome dello stream Firehose, puoi utilizzare il nome che la console genera per te o aggiungere uno stream Firehose a tua scelta.

Configurazione delle impostazioni di origine

È possibile configurare le impostazioni della sorgente in base alla fonte scelta per inviare informazioni a uno stream Firehose dalla console. Puoi configurare le impostazioni di origine per Amazon MSK e

Amazon Kinesis Data Streams come origine. Non sono disponibili impostazioni di origine per Direct PUT come origine.

Configurazione delle impostazioni di origine per Amazon MSK

Quando scegli Amazon MSK per inviare informazioni a uno stream Firehose, puoi scegliere tra cluster con provisioning MSK e cluster MSK-Serverless. È quindi possibile utilizzare Firehose per leggere facilmente i dati da un cluster e un argomento Amazon MSK specifici e caricarli nella destinazione S3 specificata.

Nella sezione Impostazioni di origine della pagina, fornisci i valori per i seguenti campi.

Connettività dei cluster Amazon MSK

Scegli l'opzione Broker bootstrap privati (consigliata) o Broker bootstrap pubblici in base alla configurazione del cluster. I broker bootstrap sono ciò che il client Apache Kafka utilizza come punto di partenza per connettersi al cluster. I broker bootstrap pubblici sono destinati all'accesso pubblico dall'esterno AWS, mentre i broker bootstrap privati sono destinati all'accesso dall'interno. AWS Per ulteriori informazioni su Amazon MSK, consulta [Streaming gestito da Amazon per Apache Kafka](#).

Per connetterti a un cluster Amazon MSK con provisioning o serverless tramite broker bootstrap privati, il cluster deve soddisfare tutti i seguenti requisiti:

- Il cluster deve essere attivo.
- Il cluster deve avere IAM come uno dei metodi di controllo dell'accesso.
- La connettività privata multi-VPC deve essere abilitata per il metodo di controllo dell'accesso IAM.
- È necessario aggiungere a questo cluster una policy basata sulle risorse che conceda al responsabile del servizio Firehose l'autorizzazione a richiamare l'operazione dell'API Amazon MSK. `CreateVpcConnection`

Per connetterti a un cluster Amazon MSK con provisioning tramite broker bootstrap pubblici, il cluster deve soddisfare tutti i seguenti requisiti.

- Il cluster deve essere attivo.
- Il cluster deve avere IAM come uno dei metodi di controllo dell'accesso.
- Il cluster deve essere accessibile pubblicamente.

Account del cluster MSK

Puoi scegliere l'account in cui risiede il cluster Amazon MSK. Questo può essere uno dei seguenti.

- **Account corrente:** consente di inserire i dati da un cluster MSK nell'account corrente AWS . A tale scopo, è necessario specificare l'ARN del cluster Amazon MSK da cui lo stream Firehose leggerà i dati.
- **Cross-account:** consente di importare dati da un cluster MSK in un altro account. AWS Per ulteriori informazioni, consulta [Consegna su più account da Amazon MSK](#).

Argomento

Specificate l'argomento di Apache Kafka da cui desiderate che lo stream Firehose inserisca i dati. Non è possibile aggiornare questo argomento dopo il completamento della creazione dello stream Firehose.

Note

Firehose decompresse automaticamente i messaggi di Apache Kafka.

Configurazione delle impostazioni di origine per Amazon Kinesis Data Streams

Configura le impostazioni di origine per Amazon Kinesis Data Streams per inviare informazioni a un flusso Firehose come segue.

Important

Se utilizzi la Kinesis Producer Library (KPL) per scrivere i dati su un flusso di dati Kinesis, puoi utilizzare l'aggregazione per abbinare i record che scrivi al flusso di dati Kinesis. Se poi utilizzi quel flusso di dati come fonte per il tuo flusso Firehose, Amazon Data Firehose disaggrega i record prima di consegnarli alla destinazione. Se configuri il flusso Firehose per trasformare i dati, Amazon Data Firehose disaggrega i record prima di inviarli a. AWS Lambda Per ulteriori informazioni, consulta [Sviluppo di producer di flussi di dati Amazon Kinesis tramite la Kinesis Producer Library](#) e [Aggregazione](#).

Nelle impostazioni di origine, scegli uno stream esistente nell'elenco dei flussi di dati Kinesis o inserisci un flusso di dati ARN nel formato. `arn:aws:kinesis:[Region]:[AccountId]:stream/[StreamName]`

Se non disponi di un flusso di dati esistente, scegli Crea per crearne uno nuovo dalla console Amazon Kinesis. Potrebbe essere necessario un ruolo IAM con l'autorizzazione necessaria sullo stream Kinesis. Per ulteriori informazioni, consulta [???](#). Dopo aver creato un nuovo stream, scegli l'icona di aggiornamento per aggiornare l'elenco degli stream Kinesis. Se disponi di un numero elevato di flussi, filtra l'elenco utilizzando Filter by name (Filtra per nome).

Note

Quando configuri un flusso di dati Kinesis come origine di un flusso Firehose, Amazon Data Firehose e le operazioni sono disabilitate. `PutRecord` `PutRecordBatch` In questo caso, per aggiungere dati allo stream Firehose, utilizza Kinesis Data Streams and operations. `PutRecord` `PutRecords`

Amazon Data Firehose inizia a leggere i dati dalla LATEST posizione dello stream Kinesis. Per ulteriori informazioni sulle posizioni di Kinesis Data Streams, vedere. [GetShardIterator](#)

Amazon Data Firehose chiama l'operazione Kinesis Data [GetRecords](#)Streams una volta al secondo per ogni shard. Tuttavia, quando il backup completo è abilitato, Firehose chiama l'operazione Kinesis Data `GetRecords` Streams due volte al secondo per ogni shard, una per la destinazione di consegna principale e l'altra per il backup completo.

È possibile leggere più stream Firehose dallo stesso stream Kinesis. Anche altre applicazioni Kinesis (consumer) possono leggere dallo stesso flusso. Ogni chiamata da uno stream Firehose o da un'altra applicazione consumer viene conteggiata ai fini del limite di throttling complessivo per lo shard. Per evitare la limitazione, pianificare con attenzione le applicazioni. Per ulteriori informazioni sui limiti di Kinesis Data Streams, consulta [Limiti di Amazon Kinesis Streams](#).

Procedi al passaggio successivo per configurare la trasformazione dei record e la conversione del formato.

(Facoltativo) Configurare la trasformazione dei record e la conversione del formato

Configura Amazon Data Firehose per trasformare e convertire i dati dei tuoi record.

Se scegli Amazon MSK come sorgente per il tuo stream Firehose.

Nella sezione Trasforma i record di origine con AWS Lambda, fornisci i valori per il campo seguente.

1. Trasformazione dei dati

Per creare uno stream Firehose che non trasformi i dati in entrata, non selezionare la casella di controllo Abilita la trasformazione dei dati.

Per specificare una funzione Lambda da richiamare e utilizzare da Firehose per trasformare i dati in entrata prima di consegnarli, seleziona la casella di controllo Abilita la trasformazione dei dati. Puoi configurare una nuova funzione Lambda utilizzando uno degli schemi Lambda o scegliere una funzione Lambda esistente. La funzione Lambda deve contenere il modello di stato richiesto da Firehose. Per ulteriori informazioni, consulta [Trasforma i dati di origine in Amazon Data Firehose](#).

2. Nella sezione Convert record format (Converti formato record) fornire i valori per il seguente campo:

Record format conversion (Conversione del formato record)

Per creare uno stream Firehose che non converta il formato dei record di dati in entrata, scegliete Disabilitato.

Per convertire il formato dei record in entrata, scegli Enabled (Abilitato), quindi specifica il formato di output desiderato. È necessario specificare una AWS Glue tabella che contenga lo schema che si desidera che Firehose utilizzi per convertire il formato di record. Per ulteriori informazioni, consulta [Convertire il formato dei dati di input](#).

Per un esempio di come impostare la conversione del formato di record con CloudFormation, vedi [AWS::KinesisFirehose: DeliveryStream](#).

Se scegli Amazon Kinesis Data Streams o Direct PUT come origine per il tuo flusso Firehose

Nella sezione Impostazioni sorgente, fornisci i seguenti campi.

1. In Trasforma record, scegli una delle seguenti opzioni:

- a. Se la tua destinazione è Amazon S3 o Splunk, nella sezione Decomprimi i record di origine di CloudWatch Amazon Logs, scegli Attiva la decompressione.
- b. Nella sezione Trasforma i record di origine con AWS Lambda, fornisci i valori per il campo seguente:

Trasformazione dei dati

Per creare uno stream Firehose che non trasformi i dati in entrata, non selezionare la casella di controllo Abilita la trasformazione dei dati.

Per specificare una funzione Lambda che Amazon Data Firehose possa richiamare e utilizzare per trasformare i dati in entrata prima di consegnarli, seleziona la casella di controllo Abilita la trasformazione dei dati. Puoi configurare una nuova funzione Lambda utilizzando uno degli schemi Lambda o scegliere una funzione Lambda esistente. La tua funzione Lambda deve contenere il modello di stato richiesto da Amazon Data Firehose.

Per ulteriori informazioni, consulta [Trasforma i dati di origine in Amazon Data Firehose](#).

2. Nella sezione Convert record format (Converti formato record) fornire i valori per il seguente campo:

Record format conversion (Conversione del formato record)

Per creare uno stream Firehose che non converta il formato dei record di dati in entrata, scegliete Disabilitato.

Per convertire il formato dei record in entrata, scegli Enabled (Abilitato), quindi specifica il formato di output desiderato. È necessario specificare una AWS Glue tabella che contenga lo schema che desideri che Amazon Data Firehose utilizzi per convertire il formato di record. Per ulteriori informazioni, consulta [Convertire il formato dei dati di input](#).

Per un esempio di come impostare la conversione del formato di record con CloudFormation, vedi [AWS::KinesisFirehose: DeliveryStream](#).

Configurare le impostazioni di destinazione

Questa sezione descrive le impostazioni da configurare per lo stream Firehose in base alla destinazione selezionata.

Argomenti

- [Configurazione delle impostazioni di destinazione per Amazon S3](#)
- [Configura le impostazioni di destinazione per Apache Iceberg Tables](#)
- [Configurazione delle impostazioni di destinazione per Amazon Redshift](#)
- [Configurare OpenSearch le impostazioni di destinazione per il servizio](#)
- [Configura le impostazioni di destinazione per Serverless OpenSearch](#)
- [Configura le impostazioni di destinazione per HTTP Endpoint](#)
- [Configura le impostazioni di destinazione per Datadog](#)
- [Configura le impostazioni di destinazione per Honeycomb](#)
- [Configura le impostazioni di destinazione per Coralogix](#)
- [Configura le impostazioni di destinazione per Dynatrace](#)
- [Configura le impostazioni di destinazione per LogicMonitor](#)
- [Configura le impostazioni di destinazione per Logz.io](#)
- [Configurare le impostazioni di destinazione per MongoDB Atlas](#)
- [Configura le impostazioni di destinazione per New Relic](#)
- [Configura le impostazioni di destinazione per Snowflake](#)
- [Configura le impostazioni di destinazione per Splunk](#)
- [Configura le impostazioni di destinazione per Splunk Observability Cloud](#)
- [Configura le impostazioni di destinazione per Sumo Logic](#)
- [Configura le impostazioni di destinazione per Elastic](#)

Configurazione delle impostazioni di destinazione per Amazon S3

Per utilizzare Amazon S3 come destinazione per il flusso di Firehose, è necessario specificare le seguenti impostazioni:

- Inserisci i valori per i seguenti campi.

Bucket S3

Scegliere un bucket S3 di proprietà dove devono essere distribuiti i dati in streaming. Puoi creare un nuovo bucket S3 o sceglierne uno esistente.

Nuovo delimitatore di riga

Puoi configurare lo stream Firehose per aggiungere un nuovo delimitatore di riga tra i record negli oggetti che vengono consegnati ad Amazon S3. Per farlo, scegli **Abilitato**. Per non aggiungere un nuovo delimitatore di riga tra i record negli oggetti distribuiti ad Amazon S3, scegli **Disabilitato**. Se prevedi di utilizzare Athena per interrogare oggetti S3 con record aggregati, abilita questa opzione.

Partizionamento dinamico

Scegli **Abilitato** per abilitare e configurare il partizionamento dinamico.

Disaggregazione di più record

Si tratta del processo di analisi dei record nello stream Firehose e di separazione degli stessi in base a un codice JSON valido o al nuovo delimitatore di riga specificato.

Se si aggregano più eventi, registri o record in un'unica chiamata PutRecordBatch API, è comunque possibile abilitare PutRecord e configurare il partizionamento dinamico. Con i dati aggregati, quando abiliti il partizionamento dinamico, Amazon Data Firehose analizza i record e cerca più oggetti JSON validi all'interno di ogni chiamata API. Quando il flusso Firehose è configurato con Kinesis Data Stream come sorgente, puoi anche utilizzare l'aggregazione integrata nella Kinesis Producer Library (KPL). La funzionalità di partizione dei dati viene eseguita dopo la disaggregazione dei dati. Pertanto, ogni record di ogni chiamata API può essere inviato a diversi prefissi Amazon S3. Puoi anche sfruttare l'integrazione della funzione Lambda per eseguire qualsiasi altra deaggregazione o qualsiasi altra trasformazione prima della funzionalità di partizionamento dei dati.

Important

Se i dati sono aggregati, il partizionamento dinamico può essere applicato solo dopo aver eseguito la disaggregazione dei dati. Quindi, se abiliti il partizionamento dinamico dei dati aggregati, devi scegliere **Abilitato** per abilitare la disaggregazione di più record.

Firehose stream esegue le seguenti fasi di elaborazione nel seguente ordine: deaggregazione KPL (protobuf), deaggregazione JSON o delimiter, elaborazione Lambda, partizionamento dei dati, conversione del formato dei dati e distribuzione di Amazon S3.

Tipo di deaggregazione multi-record

Se è stata abilitata la deaggregazione di più record, è necessario specificare il metodo di disaggregazione dei dati da parte di Firehose. Utilizza il menu a discesa per scegliere JSON o Delimitata.

Analisi in linea

Questo è uno dei meccanismi supportati per partizionare in modo dinamico i dati destinati ad Amazon S3. Per utilizzare l'analisi in linea per il partizionamento dinamico dei dati, devi specificare i parametri del record di dati da utilizzare come chiavi di partizionamento e fornire un valore per ogni chiave di partizionamento specificata. Scegli Abilitato per abilitare e configurare l'analisi in linea.

Important

Se hai specificato una funzione AWS Lambda nei passaggi precedenti per trasformare i record di origine, puoi usare questa funzione per partizionare dinamicamente i dati associati a S3 e puoi comunque creare le tue chiavi di partizionamento con l'analisi in linea. Con il partizionamento dinamico, puoi utilizzare l'analisi in linea o la funzione AWS Lambda per creare le tue chiavi di partizionamento. Oppure puoi utilizzare contemporaneamente l'analisi in linea e la funzione AWS Lambda per creare le tue chiavi di partizionamento.

Chiavi di partizionamento dinamico

Puoi utilizzare i campi Chiave e Valore per specificare i parametri del record di dati da usare come chiavi di partizionamento dinamico e le query jq per generare valori delle chiavi di partizionamento dinamico. Firehose supporta solo jq 1.6. È possibile specificare fino a 50 chiavi di partizionamento dinamico. È necessario inserire espressioni jq valide per i valori della chiave di partizionamento dinamico per configurare correttamente il partizionamento dinamico per il flusso Firehose.

Prefisso del bucket S3

Quando abiliti e configuri il partizionamento dinamico, devi specificare i prefissi dei bucket S3 a cui Amazon Data Firehose deve fornire i dati partizionati.

Affinché il partizionamento dinamico sia configurato correttamente, il numero di prefissi del bucket S3 deve essere identico al numero delle chiavi di partizionamento specificate.

Puoi partizionare i dati di origine con l'analisi in linea o con la funzione AWS Lambda specificata. Se hai specificato una funzione AWS Lambda per creare chiavi di partizionamento per i tuoi dati di origine, devi digitare manualmente i valori del prefisso del bucket S3 utilizzando il seguente formato: "lambda:keyID». partitionKeyFrom Se utilizzi l'analisi in linea per specificare le chiavi di partizionamento per i tuoi dati di origine, puoi digitare manualmente i valori di anteprima del bucket S3 utilizzando il seguente formato: "partitionKeyFromquery:keyID» oppure puoi scegliere il pulsante Applica chiavi di partizionamento dinamico per utilizzare le coppie di partizionamento dinamico per generare automaticamente i prefissi dei bucket S3. key/value Durante il partizionamento dei dati con analisi in linea o AWS Lambda, puoi anche utilizzare le seguenti forme di espressione nel prefisso del bucket S3: {namespace:value}, dove lo spazio dei nomi può essere Query o Lambda. partitionKeyFrom partitionKeyFrom

Bucket S3 e fuso orario del prefisso di output di errore S3

Scegli un fuso orario che desideri utilizzare per la data e l'ora nei [prefissi personalizzati per gli oggetti Amazon S3](#). Per impostazione predefinita, Firehose aggiunge un prefisso orario in UTC. È possibile modificare il fuso orario utilizzato nei prefissi S3 se si desidera utilizzare un fuso orario diverso.

Suggerimenti per il buffering

Firehose memorizza i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Compressione S3

Scegli la compressione dei dati GZIP, Snappy, Zip o Snappy compatibile con Hadoop oppure nessuna compressione dei dati. La compressione Snappy, il formato zip e Snappy compatibile con Hadoop non è disponibile per i flussi Firehose con Amazon Redshift come destinazione.

Formato di estensione del file S3 (opzionale)

Specificare un formato di estensione di file per gli oggetti consegnati al bucket di destinazione Amazon S3. Se abiliti questa funzionalità, l'estensione di file specificata sostituirà le estensioni di file predefinite aggiunte dalle funzionalità di compressione Data Format Conversion o S3 come .parquet o .gz. Assicurati di aver configurato l'estensione di file

corretta quando usi questa funzionalità con Data Format Conversion o la compressione S3. L'estensione del file deve iniziare con un punto (.) e può contenere caratteri consentiti: 0-9a-z!-_*.' (). L'estensione del file non può superare i 128 caratteri.

Crittografia S3

Firehose supporta la crittografia lato server di Amazon S3 AWS Key Management Service con (SSE-KMS) per crittografare i dati forniti in Amazon S3. Puoi scegliere di utilizzare il tipo di crittografia predefinito specificato nel bucket S3 di destinazione o di crittografare con una chiave dall'elenco di chiavi di tua proprietà. AWS KMS Se crittografi i dati con le AWS KMS chiavi, puoi utilizzare la chiave AWS gestita predefinita (aws/s3) o una chiave gestita dal cliente. Per ulteriori informazioni, consulta [Protezione dei dati mediante la crittografia lato server con AWS chiavi gestite da KMS \(SSE-KMS\)](#).

Configura le impostazioni di destinazione per Apache Iceberg Tables

Firehose supporta Apache Iceberg Tables come destinazione in tutte le regioni tranne [Regioni AWS](#) Cina AWS GovCloud (US) Regions, Asia Pacifico (Taipei), Asia Pacifico (Malesia), Asia Pacifico (Nuova Zelanda) e Messico (Centrale).

Per ulteriori informazioni su Apache Iceberg Tables come destinazione, consulta [Distribuisci dati ad Apache Iceberg Tables con Amazon Data Firehose](#)

Configurazione delle impostazioni di destinazione per Amazon Redshift

Questa sezione descrive le impostazioni per l'utilizzo di Amazon Redshift come destinazione dello stream Firehose.

Scegli una delle procedure seguenti a seconda che tu disponga di un cluster con provisioning di Amazon Redshift o di un gruppo di lavoro Amazon Redshift serverless.

- [Cluster con provisioning di Amazon Redshift](#)
- [Configura le impostazioni di destinazione per il gruppo di lavoro Amazon Redshift Serverless](#)

Note

Firehose non è in grado di scrivere su cluster Amazon Redshift che utilizzano un routing VPC avanzato.

Cluster con provisioning di Amazon Redshift

Questa sezione descrive le impostazioni per l'utilizzo del cluster con provisioning di Amazon Redshift come destinazione dello stream Firehose.

- Immetti i valori per i seguenti campi:

Cluster

Il cluster Amazon Redshift sul quale vengono copiati i dati del bucket S3. Configura il cluster Amazon Redshift in modo che sia accessibile al pubblico e sblocca gli indirizzi IP di Amazon Data Firehose. Per ulteriori informazioni, consulta [Concedi a Firehose l'accesso a una destinazione Amazon Redshift](#).

Autenticazione

Puoi scegliere di accedere username/password direttamente o recuperare il segreto da cui accedere Gestione dei segreti AWS al cluster Amazon Redshift.

- Nome utente

Specificare un utente Amazon Redshift con le autorizzazioni per accedere al cluster Amazon Redshift. Tale utente deve disporre dell'autorizzazione INSERT di Amazon Redshift per copiare i dati dal bucket S3 al cluster Amazon Redshift.

- Password

Specificare la password per l'utente che dispone delle autorizzazioni per accedere al cluster.

- Secret

Seleziona un campo segreto Gestione dei segreti AWS che contenga le credenziali per il cluster Amazon Redshift. Se non vedi il tuo segreto nell'elenco a discesa, creane uno Gestione dei segreti AWS per le tue credenziali Amazon Redshift. Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Database

Il database Amazon Redshift su cui vengono copiati i dati.

Tabella

~~La tabella Amazon Redshift su cui vengono copiati i dati.~~

Colonne

(Opzionale) Le colonne specifiche della tabella su cui vengono copiati i dati. Utilizza questa opzione se il numero di colonne definite negli oggetti Amazon S3 è inferiore al numero delle colonne nella tabella Amazon Redshift.

Destinazione S3 intermedia

Firehose invia prima i dati al bucket S3 e poi emette un COPY comando Amazon Redshift per caricare i dati nel cluster Amazon Redshift. Specificare un bucket S3 di proprietà dove devono essere distribuiti i dati in streaming. Crea un nuovo bucket S3 o sceglie uno esistente di proprietà.

Firehose non elimina i dati dal bucket S3 dopo averli caricati nel cluster Amazon Redshift. Puoi gestire i dati nel bucket S3 utilizzando una configurazione del ciclo di vita. Per ulteriori informazioni, consulta [Gestione del ciclo di vita degli oggetti](#) nella Guida per l'utente di Amazon Simple Storage Service.

Prefisso S3 intermedio

(Facoltativo) Per utilizzare il prefisso predefinito per gli oggetti Amazon S3, lascia vuota questa opzione. Firehose utilizza automaticamente un prefisso in formato orario "YYYY/MM/dd/HH" UTC per gli oggetti Amazon S3 consegnati. Puoi aggiungerlo all'inizio di questo prefisso. Per ulteriori informazioni, consulta [Configurazione del formato dei nomi degli oggetti Amazon S3](#).

COPY options (Opzioni COPY)

Parametri che puoi specificare nel comando COPY di Amazon Redshift. Questi potrebbero essere necessari per la configurazione. Ad esempio, "GZIP" è necessario se la compressione dei dati di Amazon S3 è abilitata. «REGION» è obbligatorio se il bucket S3 non si trova nella stessa AWS regione del cluster Amazon Redshift. Per ulteriori informazioni, consulta [COPY](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

COPY command (Comando COPY)

Il comando COPY di Amazon Redshift. Per ulteriori informazioni, consulta [COPY](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Retry duration (Durata nuovi tentativi)

Periodo di tempo (0—7200 secondi) entro il quale Firehose riprova in caso di errore dei dati del cluster COPY Amazon Redshift. Firehose riprova ogni 5 minuti fino al termine del

nuovo tentativo. Se si imposta la durata del nuovo tentativo su 0 (zero) secondi, Firehose non riprova in caso COPY di errore del comando.

Suggerimenti per il buffering

Firehose memorizza i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Compressione S3

Scegli la compressione dei dati GZIP, Snappy, Zip o Snappy compatibile con Hadoop oppure nessuna compressione dei dati. La compressione Snappy, il formato zip e Snappy compatibile con Hadoop non è disponibile per i flussi Firehose con Amazon Redshift come destinazione.

Formato di estensione del file S3 (opzionale)

Formato di estensione file S3 (opzionale): specifica un formato di estensione di file per gli oggetti consegnati al bucket di destinazione Amazon S3. Se abiliti questa funzionalità, l'estensione di file specificata sostituirà le estensioni di file predefinite aggiunte dalle funzionalità di compressione Data Format Conversion o S3 come .parquet o .gz. Assicurati di aver configurato l'estensione di file corretta quando usi questa funzionalità con Data Format Conversion o la compressione S3. L'estensione del file deve iniziare con un punto (.) e può contenere caratteri consentiti: 0-9a-z! -_.*' (). L'estensione del file non può superare i 128 caratteri.

Crittografia S3

Firehose supporta la crittografia lato server di Amazon S3 AWS Key Management Service con (SSE-KMS) per crittografare i dati forniti in Amazon S3. Puoi scegliere di utilizzare il tipo di crittografia predefinito specificato nel bucket S3 di destinazione o di crittografare con una chiave dall'elenco di chiavi di tua proprietà. AWS KMS Se crittografi i dati con le AWS KMS chiavi, puoi utilizzare la chiave AWS gestita predefinita (aws/s3) o una chiave gestita dal cliente. Per ulteriori informazioni, consulta [Protezione dei dati mediante la crittografia lato server con AWS chiavi gestite da KMS \(SSE-KMS\)](#).

Configura le impostazioni di destinazione per il gruppo di lavoro Amazon Redshift Serverless

Questa sezione descrive le impostazioni per l'utilizzo del gruppo di lavoro Amazon Redshift Serverless come destinazione del flusso Firehose.

- Immetti i valori per i seguenti campi:

Workgroup name (Nome del gruppo di lavoro)

Il gruppo di lavoro Amazon Redshift serverless in cui vengono copiati i dati del bucket S3. Configura il gruppo di lavoro Amazon Redshift Serverless in modo che sia accessibile al pubblico e sblocca gli indirizzi IP Firehose. Per ulteriori informazioni, consulta la sezione [Connessione a un'istanza Amazon Redshift serverless accessibile pubblicamente](#) in [Connessione ad Amazon Redshift serverless](#) e anche [Concedi a Firehose l'accesso a una destinazione Amazon Redshift](#).

Autenticazione

Puoi scegliere di accedere username/password direttamente o recuperare il codice segreto Gestione dei segreti AWS per accedere al gruppo di lavoro Amazon Redshift Serverless.

- Nome utente

Specificare un utente Amazon Redshift con le autorizzazioni per accedere al gruppo di lavoro Amazon Redshift Serverless. Questo utente deve disporre dell'autorizzazione INSERT di Amazon Redshift per copiare i dati dal bucket S3 al gruppo di lavoro Amazon Redshift serverless.

- Password

Specificare la password per l'utente che dispone delle autorizzazioni per accedere al gruppo di lavoro Amazon Redshift Serverless.

- Secret

Seleziona un campo segreto Gestione dei segreti AWS che contenga le credenziali per il gruppo di lavoro Serverless Amazon Redshift. Se non vedi il tuo segreto nell'elenco a discesa, creane uno Gestione dei segreti AWS per le tue credenziali Amazon Redshift. Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Database

Il database Amazon Redshift su cui vengono copiati i dati.

Tabella

La tabella Amazon Redshift su cui vengono copiati i dati.

Colonne

(Opzionale) Le colonne specifiche della tabella su cui vengono copiati i dati. Utilizza questa opzione se il numero di colonne definite negli oggetti Amazon S3 è inferiore al numero delle colonne nella tabella Amazon Redshift.

Destinazione S3 intermedia

Amazon Data Firehose invia prima i dati al bucket S3 e poi emette un COPY comando Amazon Redshift per caricare i dati nel tuo gruppo di lavoro Serverless Amazon Redshift. Specificare un bucket S3 di proprietà dove devono essere distribuiti i dati in streaming. Crea un nuovo bucket S3 o scegline uno esistente di proprietà.

Firehose non elimina i dati dal bucket S3 dopo averli caricati nel gruppo di lavoro Amazon Redshift Serverless. Puoi gestire i dati nel bucket S3 utilizzando una configurazione del ciclo di vita. Per ulteriori informazioni, consulta [Gestione del ciclo di vita degli oggetti](#) nella Guida per l'utente di Amazon Simple Storage Service.

Prefisso S3 intermedio

(Facoltativo) Per utilizzare il prefisso predefinito per gli oggetti Amazon S3, lascia vuota questa opzione. Firehose utilizza automaticamente un prefisso in formato orario "YYYY/MM/dd/HH" UTC per gli oggetti Amazon S3 consegnati. Puoi aggiungerlo all'inizio di questo prefisso. Per ulteriori informazioni, consulta [Configurazione del formato dei nomi degli oggetti Amazon S3](#).

COPY options (Opzioni COPY)

Parametri che puoi specificare nel comando COPY di Amazon Redshift. Questi potrebbero essere necessari per la configurazione. Ad esempio, "GZIP" è necessario se la compressione dei dati di Amazon S3 è abilitata. «REGION» è obbligatorio se il bucket S3 non si trova nella stessa AWS regione del gruppo di lavoro Serverless Amazon Redshift. Per ulteriori informazioni, consulta [COPY](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

COPY command (Comando COPY)

Il comando COPY di Amazon Redshift. Per ulteriori informazioni, consulta [COPY](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Retry duration (Durata nuovi tentativi)

Periodo di tempo (0—7200 secondi) entro il quale Firehose riprova in caso di errore dei dati del gruppo di lavoro COPY Amazon Redshift Serverless. Firehose riprova ogni 5 minuti fino al

termine del nuovo tentativo. Se si imposta la durata del nuovo tentativo su 0 (zero) secondi, Firehose non riprova in caso COPY di errore del comando.

Suggerimenti per il buffering

Firehose memorizza i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Compressione S3

Scegli la compressione dei dati GZIP, Snappy, Zip o Snappy compatibile con Hadoop oppure nessuna compressione dei dati. La compressione Snappy, il formato zip e Snappy compatibile con Hadoop non è disponibile per i flussi Firehose con Amazon Redshift come destinazione.

Formato di estensione del file S3 (opzionale)

Formato di estensione file S3 (opzionale): specifica un formato di estensione di file per gli oggetti consegnati al bucket di destinazione Amazon S3. Se abiliti questa funzionalità, l'estensione di file specificata sostituirà le estensioni di file predefinite aggiunte dalle funzionalità di compressione Data Format Conversion o S3 come .parquet o .gz. Assicurati di aver configurato l'estensione di file corretta quando usi questa funzionalità con Data Format Conversion o la compressione S3. L'estensione del file deve iniziare con un punto (.) e può contenere caratteri consentiti: 0-9a-z! -_.*' (). L'estensione del file non può superare i 128 caratteri.

Crittografia S3

Firehose supporta la crittografia lato server di Amazon S3 AWS Key Management Service con (SSE-KMS) per crittografare i dati forniti in Amazon S3. Puoi scegliere di utilizzare il tipo di crittografia predefinito specificato nel bucket S3 di destinazione o di crittografare con una chiave dall'elenco di chiavi di tua proprietà. AWS KMS Se crittografi i dati con le AWS KMS chiavi, puoi utilizzare la chiave AWS gestita predefinita (aws/s3) o una chiave gestita dal cliente. Per ulteriori informazioni, consulta [Protezione dei dati mediante la crittografia lato server con AWS chiavi gestite da KMS \(SSE-KMS\)](#).

Configurare OpenSearch le impostazioni di destinazione per il servizio

Firehose supporta le versioni di Elasticsearch: 1.5, 2.3, 5.1, 5.3, 5.5, 5.6 e tutte le versioni 6.*, 7.* e 8.*. Firehose supporta Amazon OpenSearch Service 2.x e 3.x.

Questa sezione descrive le opzioni per utilizzare OpenSearch Service per la destinazione.

- Immetti i valori per i seguenti campi:

OpenSearch Dominio di servizio

Il dominio del OpenSearch servizio a cui vengono consegnati i dati.

Indice

Il nome dell'indice del OpenSearch servizio da utilizzare per l'indicizzazione dei dati nel cluster di OpenSearch servizio.

Index rotation (Rotazione indice)

Scegli se e con quale frequenza ruotare l'indice del OpenSearch servizio. Se la rotazione dell'indice è abilitata, Amazon Data Firehose aggiunge il timestamp corrispondente al nome dell'indice specificato ed esegue la rotazione. Per ulteriori informazioni, consulta [Configura la rotazione dell'indice per Service OpenSearch](#).

Tipo

Il nome del tipo di OpenSearch servizio da utilizzare per l'indicizzazione dei dati nel cluster di servizio. OpenSearch Per Elasticsearch 7.x e OpenSearch 1.x, può esserci un solo tipo per indice. Se provi a specificare un nuovo tipo per un indice esistente che ha già un altro tipo, Firehose restituisce un errore in fase di runtime.

Per Elasticsearch 7.x, lasciare vuoto questo campo.

Retry duration (Durata nuovi tentativi)

Intervallo di tempo entro il quale Firehose deve riprovare se una richiesta di indice fallisce. OpenSearch Per la durata dei nuovi tentativi, è possibile impostare qualsiasi valore compreso tra 0 e 7200 secondi. La durata predefinita dei nuovi tentativi è 300 secondi. Firehose riproverà più volte con il back up esponenziale disattivato fino alla scadenza della durata del nuovo tentativo.

Una volta scaduta la durata del nuovo tentativo, Firehose invia i dati a Dead Letter Queue (DLQ), un bucket di errori S3 configurato. Per i dati consegnati a DLQ, è necessario reindirizzare i dati dal bucket di errore S3 configurato alla destinazione. OpenSearch

Se desideri impedire allo stream di Firehose di fornire dati a DLQ a causa di tempi di inattività o di manutenzione dei OpenSearch cluster, puoi configurare la durata dei nuovi tentativi su un valore più alto in secondi. [È possibile aumentare il valore della durata del nuovo tentativo fino a 7200 secondi contattando l'assistenza.AWS](#)

Tipo di ID documento

Indica il metodo per impostare l'ID documento. I metodi supportati sono ID documento generato da FireHose e ID documento generato dal OpenSearch servizio. L'ID documento generato da FireHose è l'opzione predefinita quando il valore dell'ID del documento non è impostato. OpenSearch L'ID documento generato dal servizio è l'opzione consigliata perché supporta operazioni che richiedono molta scrittura, tra cui l'analisi dei log e l'osservabilità, consumando meno risorse della CPU nel dominio del OpenSearch servizio e quindi migliorando le prestazioni.

Destination VPC connectivity (Connettività VPC di destinazione)

Se il tuo dominio di OpenSearch servizio si trova in un VPC privato, utilizza questa sezione per specificare quel VPC. Specificate anche le sottoreti e i sottogruppi che desiderate che Amazon Data Firehose utilizzi quando invia dati al tuo dominio di servizio. OpenSearch Puoi utilizzare gli stessi gruppi di sicurezza utilizzati dal dominio OpenSearch Service. Se specifichi gruppi di sicurezza diversi, assicurati che consentano il traffico HTTPS in uscita al gruppo di sicurezza del dominio del OpenSearch servizio. Assicuratevi inoltre che il gruppo di sicurezza del dominio di OpenSearch servizio consenta il traffico HTTPS proveniente dai gruppi di sicurezza specificati durante la configurazione dello stream Firehose. Se utilizzi lo stesso gruppo di sicurezza sia per lo stream Firehose che per il dominio di OpenSearch servizio, assicurati che la regola in entrata del gruppo di sicurezza consenta il traffico HTTPS. Per ulteriori informazioni sulle regole dei gruppi di sicurezza, consulta [Regole del gruppo di sicurezza](#) nella documentazione di Amazon VPC.

Important

Quando specifichi delle sottoreti per la consegna dei dati alla destinazione in un VPC privato, assicurati di avere un numero sufficiente di indirizzi IP liberi nelle sottoreti scelte. Se non è disponibile un indirizzo IP gratuito in una sottorete specificata, Firehose non può creare o ENIs aggiungere dati per la consegna dei dati nel VPC privato e la consegna verrà compromessa o avrà esito negativo.

Suggerimenti sul buffer

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Configura le impostazioni di destinazione per Serverless OpenSearch

Questa sezione descrive le opzioni per l'utilizzo di OpenSearch Serverless per la destinazione.

- Immetti i valori per i seguenti campi:

OpenSearch Collezione Serverless

L'endpoint per un gruppo di indici OpenSearch Serverless a cui vengono distribuiti i dati.

Indice

Il nome dell'indice OpenSearch Serverless da utilizzare per l'indicizzazione dei dati nella raccolta Serverless. OpenSearch

Destination VPC connectivity (Connettività VPC di destinazione)

Se la tua raccolta OpenSearch Serverless si trova in un VPC privato, usa questa sezione per specificare quel VPC. Specificate anche le sottoreti e i sottogruppi che desiderate che Amazon Data Firehose utilizzi quando invia dati alla tua raccolta Serverless. OpenSearch

Important

Quando specifichi delle sottoreti per la consegna dei dati alla destinazione in un VPC privato, assicurati di avere un numero sufficiente di indirizzi IP liberi nelle sottoreti scelte. Se non è disponibile un indirizzo IP gratuito in una sottorete specificata, Firehose non può creare o ENIs aggiungere dati per la consegna dei dati nel VPC privato e la consegna verrà compromessa o avrà esito negativo.

Retry duration (Durata nuovi tentativi)

Intervallo di tempo entro il quale Firehose deve riprovare se una richiesta di indicizzazione a OpenSearch Serverless fallisce. Per la durata dei nuovi tentativi, è possibile impostare qualsiasi valore compreso tra 0 e 7200 secondi. La durata predefinita dei nuovi tentativi è 300 secondi. Firehose riproverà più volte con il back up esponenziale disattivato fino alla scadenza della durata del nuovo tentativo.

Una volta scaduta la durata del nuovo tentativo, Firehose invia i dati a Dead Letter Queue (DLQ), un bucket di errori S3 configurato. Per i dati consegnati a DLQ, è necessario reindirizzare i dati dal bucket di errore S3 configurato alla destinazione Serverless. OpenSearch

Se desideri impedire allo stream Firehose di fornire dati a DLQ a causa di tempi di inattività o di manutenzione di cluster OpenSearch Serverless, puoi configurare la durata dei tentativi su un valore più alto in secondi. [È possibile aumentare il valore della durata del nuovo tentativo portandolo a 7200 secondi contattando l'assistenza.AWS](#)

Suggerimenti sul buffer

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Configura le impostazioni di destinazione per HTTP Endpoint

Questa sezione descrive le opzioni per l'utilizzo di un endpoint HTTP come destinazione.

Important

Se scegli un endpoint HTTP come destinazione, consulta e segui le istruzioni riportate in [Comprendi le specifiche di richiesta e risposta di consegna degli endpoint HTTP](#).

- Fornisci i valori per i seguenti campi:

Nome dell'endpoint HTTP: facoltativo

Specifica un nome intuitivo per l'endpoint HTTP. Ad esempio, `My HTTP Endpoint Destination`.

URL dell'endpoint HTTP

Specifica l'URL per l'endpoint HTTP nel seguente formato: `https://xyz.httpendpoint.com`. L'URL deve essere un URL HTTPS.

Autenticazione

Puoi scegliere di inserire direttamente la chiave di accesso o recuperare il segreto da cui accedere Gestione dei segreti AWS all'endpoint HTTP.

- (Facoltativo) Chiave di accesso

Contatta il proprietario dell'endpoint se hai bisogno di ottenere la chiave di accesso per abilitare la consegna dei dati al suo endpoint da Firehose.

- Secret

Seleziona un campo segreto Gestione dei segreti AWS che contenga la chiave di accesso per l'endpoint HTTP. Se non vedi il tuo segreto nell'elenco a discesa, creane uno Gestione dei segreti AWS per la chiave di accesso. Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Codifica del contenuto

Amazon Data Firehose utilizza la codifica del contenuto per comprimere il corpo di una richiesta prima di inviarla alla destinazione. Scegli GZIP o Disabilitato per la codifica enable/disable del contenuto della tua richiesta.

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati all'endpoint HTTP selezionato.

Dopo l'invio dei dati, Amazon Data Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi.

Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati all'endpoint HTTP (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di conferma e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Important

Per le destinazioni degli endpoint HTTP, se visualizzi 413 codici di risposta dall'endpoint di destinazione in CloudWatch Logs, riduci la dimensione del suggerimento di buffering sullo stream Firehose e riprova.

Configura le impostazioni di destinazione per Datadog

Questa sezione descrive le opzioni per l'utilizzo di Datadog come destinazione. [Per ulteriori informazioni su Datadog, consulta amazon_web_services/. https://docs.datadoghq.com/integrations/](#)

- Fornisci valori per i seguenti campi.

URL dell'endpoint HTTP

Scegli dove vuoi inviare i dati da una delle seguenti opzioni nel menu a discesa.

- Registri Datadog - US1
- Registri Datadog - US3
- Registri Datadog - US5
- Registri Datadog - AP1
- Registri Datadog - UE
- Registri Datadog - GOV
- Parametri Datadog - USA
- Metriche Datadog - US5
- Metriche Datadog - AP1
- Parametri Datadog - UE
- Configurazioni Datadog - US1
- Configurazioni Datadog - US3
- Configurazioni Datadog - US5
- Configurazioni Datadog - AP1
- Configurazioni Datadog - EU
- Configurazioni Datadog - US GOV

Autenticazione

Puoi scegliere di inserire direttamente la chiave API o recuperare il segreto da cui accedere a Datadog. Gestione dei segreti AWS

- Chiave API

Contatta Datadog per ottenere la chiave API necessaria per abilitare la consegna dei dati a questo endpoint da Firehose.

- Secret

Seleziona un campo segreto Gestione dei segreti AWS che contenga la chiave API per Datadog. Se non vedi il tuo segreto nell'elenco a discesa, creane uno in. Gestione dei segreti AWS Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Codifica del contenuto

Amazon Data Firehose utilizza la codifica del contenuto per comprimere il corpo di una richiesta prima di inviarla alla destinazione. Scegli GZIP o Disabilitato per la codifica enable/disable del contenuto della tua richiesta.

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati all'endpoint HTTP selezionato.

Dopo l'invio dei dati, Amazon Data Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati all'endpoint HTTP (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di conferma e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Configura le impostazioni di destinazione per Honeycomb

Questa sezione descrive le opzioni per l'utilizzo di Honeycomb come destinazione. [Per ulteriori informazioni su Honeycomb, https://docs.honeycom consulta b. -cloudwatch-metrics/. io/getting-data-in/metrics/aws](https://docs.honeycom.consulta b. -cloudwatch-metrics/. io/getting-data-in/metrics/aws)

- Fornisci i valori per i seguenti campi:

Endpoint Honeycomb Kinesis

Specificate l'URL per l'endpoint HTTP nel seguente formato: `b.io/1/kinesis_events/ {{dataset}}`
`https://api.honeycom`

Autenticazione

Puoi scegliere di inserire direttamente la chiave API o recuperare il segreto da cui accedere a Honeycomb. [Gestione dei segreti AWS](#)

- Chiave API

Contatta Honeycomb per ottenere la chiave API necessaria per abilitare la consegna dei dati a questo endpoint da Firehose.

- Secret

Seleziona un campo segreto [Gestione dei segreti AWS](#) che contenga la chiave API per Honeycomb. Se non vedi il tuo segreto nell'elenco a discesa, creane uno in. [Gestione dei segreti AWS](#) Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Codifica del contenuto

Amazon Data Firehose utilizza la codifica del contenuto per comprimere il corpo di una richiesta prima di inviarla alla destinazione. Scegli GZIP per abilitare la codifica del contenuto della richiesta. Questa è l'opzione consigliata per la destinazione Honeycomb.

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati all'endpoint HTTP selezionato.

Dopo l'invio dei dati, Amazon Data Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. ~~Se si verifica un errore o se il riconoscimento non arriva entro il periodo~~

di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati all'endpoint HTTP (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di conferma e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Configura le impostazioni di destinazione per Coralogix

Questa sezione descrive le opzioni per l'utilizzo di Coralogix come destinazione. [Per ulteriori informazioni su Coralogix, consulta Introduzione a Coralogix.](#)

- Fornisci i valori per i seguenti campi:

URL dell'endpoint HTTP

Scegli l'URL dell'endpoint HTTP tra le seguenti opzioni nel menu a discesa:

- Coralogix - STATI UNITI

- Coralogix - SINGAPORE
- Coralogix - IRLANDA
- Coralogix - INDIA
- Coralogix - STOCCOLMA

Autenticazione

Puoi scegliere di inserire direttamente la chiave privata o recuperare il codice segreto per accedere a Coralogix. Gestione dei segreti AWS

- Chiave privata

Contatta Coralogix per ottenere la chiave privata necessaria per abilitare la consegna dei dati a questo endpoint da Firehose.

- Secret

Seleziona una cartella segreta Gestione dei segreti AWS che contenga la chiave privata per Coralogix. Se non vedi il tuo segreto nell'elenco a discesa, creane uno in. Gestione dei segreti AWS Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Codifica del contenuto

Amazon Data Firehose utilizza la codifica del contenuto per comprimere il corpo di una richiesta prima di inviarla alla destinazione. Scegli GZIP per abilitare la codifica del contenuto della richiesta. Questa è l'opzione consigliata per la destinazione Coralogix.

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati all'endpoint HTTP selezionato.

Dopo l'invio dei dati, Amazon Data Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati all'endpoint HTTP (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di conferma e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

- `applicationName`: l'ambiente in cui viene eseguito Data Firehose
- `subsystemName`: il nome dell'integrazione Data Firehose
- `computerName`: il nome del flusso Firehose in uso

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia in base al fornitore di servizi.

Configura le impostazioni di destinazione per Dynatrace

Questa sezione descrive le opzioni per l'utilizzo di Dynatrace come destinazione. [Per ulteriori informazioni, consulta https://www.dynatrace.com/support/help/technology-support/cloud-platforms/amazon-web-services/integrations/cloudwatch-metric-streams/](https://www.dynatrace.com/support/help/technology-support/cloud-platforms/amazon-web-services/integrations/cloudwatch-metric-streams/).

- Scegli le opzioni per utilizzare Dynatrace come destinazione per il tuo stream Firehose.

Tipo di ingestione

Scegliete se desiderate fornire metriche o log (impostazione predefinita) in Dynatrace per ulteriori analisi ed elaborazioni.

URL dell'endpoint HTTP

Scegli l'URL dell'endpoint HTTP (Dynatrace US, Dynatrace EU o Dynatrace Global) dal menu a discesa.

Autenticazione

Puoi scegliere di inserire direttamente il token API o recuperare il codice segreto per accedere a Dynatrace. Gestione dei segreti AWS

- Token API

Genera il token API Dynatrace necessario per abilitare la consegna dei dati a questo endpoint da Firehose. Per ulteriori informazioni, consulta API [Dynatrace](#) - Tokens and authentication.

- Secret

Seleziona un campo segreto Gestione dei segreti AWS che contenga il token API per Dynatrace. Se non vedi il tuo segreto nell'elenco a discesa, creane uno in. Gestione dei segreti AWS Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

URL API

Fornisci l'URL API dell'ambiente Dynatrace.

Codifica del contenuto

Scegli se vuoi abilitare la codifica del contenuto per comprimere il corpo della richiesta. Amazon Data Firehose utilizza la codifica del contenuto per comprimere il corpo di una richiesta prima di inviarla alla destinazione. Se abilitata, il contenuto viene compresso nel formato GZIP.

Retry duration (Durata nuovi tentativi)

Specificate per quanto tempo Firehose riprova a inviare dati all'endpoint HTTP selezionato.

Dopo l'invio dei dati, Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati nel bucket Amazon S3.

Ogni volta che Firehose invia dati all'endpoint HTTP, durante il tentativo iniziale o dopo un nuovo tentativo, riavvia il contatore del timeout di riconoscimento e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Firehose attende comunque la conferma fino a quando non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desiderate che Firehose tenti di inviare nuovamente i dati, impostate questo valore su 0.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. I suggerimenti sul buffer includono la dimensione e l'intervallo del buffer per i tuoi stream. La dimensione del buffer consigliata per la destinazione varia in base al fornitore di servizi.

Configura le impostazioni di destinazione per LogicMonitor

Questa sezione descrive le opzioni per l'utilizzo di LogicMonitor come destinazione. Per ulteriori informazioni, consulta <https://www.logicmonitor.com>.

- Fornisci i valori per i seguenti campi:

URL dell'endpoint HTTP

Specificare l'URL per l'endpoint HTTP nel formato seguente.

```
https://ACCOUNT.logicmonitor.com
```

Autenticazione

Puoi scegliere di inserire direttamente la chiave API o recuperare il codice segreto Gestione dei segreti AWS per accedere. LogicMonitor

- Chiave API

Contattateci LogicMonitor per ottenere la chiave API necessaria per abilitare la consegna dei dati a questo endpoint da Firehose.

- Secret

Seleziona un campo segreto Gestione dei segreti AWS che contenga la chiave API per. LogicMonitor Se non vedi il tuo segreto nell'elenco a discesa, creane uno in. Gestione dei segreti AWS Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Codifica del contenuto

Amazon Data Firehose utilizza la codifica del contenuto per comprimere il corpo di una richiesta prima di inviarla alla destinazione. Scegli GZIP o Disabilitato per la codifica enable/disable del contenuto della tua richiesta.

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati all'endpoint HTTP selezionato.

Dopo l'invio dei dati, Amazon Data Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati all'endpoint HTTP (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di conferma e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Configura le impostazioni di destinazione per Logz.io

Questa sezione descrive le opzioni per l'utilizzo di Logz.io come destinazione. [Per ulteriori informazioni, vedere https://logz.io/](#).

Note

Nella regione Europa (Milano), Logz.io non è supportato come destinazione di Amazon Data Firehose.

- Fornisci i valori per i seguenti campi:

URL dell'endpoint HTTP

Specificate l'URL per l'endpoint HTTP nel formato seguente. L'URL deve essere un HTTPS URL.

```
https://listener-aws-metrics-stream-<region>.logz.io/
```

Ad esempio

```
https://listener-aws-metrics-stream-us.logz.io/
```

Autenticazione

Puoi scegliere di inserire direttamente il token di spedizione o recuperare il codice segreto Gestione dei segreti AWS per accedere a Logz.io.

- Token di spedizione

Contatta Logz.io per ottenere il token di spedizione necessario per abilitare la consegna dei dati a questo endpoint da Firehose.

- Secret

Seleziona un codice segreto Gestione dei segreti AWS che contenga il token di spedizione per Logz.io. Se non vedi il tuo segreto nell'elenco a discesa, creane uno in [Gestione dei segreti AWS](#) Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati a Logz.io.

Dopo l'invio dei dati, Amazon Data Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati all'endpoint HTTP (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di conferma e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Configurare le impostazioni di destinazione per MongoDB Atlas

Questa sezione descrive le opzioni per l'utilizzo di MongoDB Atlas per la tua destinazione. Per ulteriori informazioni, consulta [MongoDB Atlas su Amazon Web Services](#).

- Fornisci i valori per i seguenti campi:

URL del gateway API

Specificate l'URL per l'endpoint HTTP nel seguente formato.

```
https://xxxxx.execute-api.region.amazonaws.com/stage
```

L'URL deve essere un HTTPS URL.

Autenticazione

Puoi scegliere di inserire direttamente la chiave API o recuperare il codice segreto Gestione dei segreti AWS per accedere a MongoDB Atlas.

- Chiave API

Segui le istruzioni in [MongoDB Atlas su Amazon Web Services](#) per ottenere ciò che ti serve per abilitare `APIKeyValue` la consegna dei dati a questo endpoint da Firehose.

- Secret

Seleziona un campo segreto Gestione dei segreti AWS che contenga la chiave API per API Gateway supportata da Lambda che interagisce con MongoDB Atlas. Se non vedi il tuo segreto nell'elenco a discesa, creane uno in. Gestione dei segreti AWS Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Codifica del contenuto

Amazon Data Firehose utilizza la codifica del contenuto per comprimere il corpo di una richiesta prima di inviarla alla destinazione. Scegli GZIP o Disabilitato per la codifica enable/disable del contenuto della tua richiesta.

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati al provider terzo selezionato.

Dopo l'invio dei dati, Amazon Data Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati all'endpoint HTTP (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di conferma e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se

la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

Configura le impostazioni di destinazione per New Relic

Questa sezione descrive le opzioni per l'utilizzo di New Relic come destinazione. Per ulteriori informazioni, consulta <https://newrelic.com>.

- Fornisci i valori per i seguenti campi:

URL dell'endpoint HTTP

Scegli l'URL dell'endpoint HTTP tra le seguenti opzioni nell'elenco a discesa.

- Log di New Relic - USA
- Parametri di New Relic - USA
- Parametri di New Relic - UE

Autenticazione

Puoi scegliere di inserire direttamente la chiave API o recuperare il codice segreto per accedere Gestione dei segreti AWS a New Relic.

- Chiave API

Inserisci la tua chiave di licenza, che è una stringa esadecimale di 40 caratteri, dalle impostazioni del tuo account New Relic One. È necessaria questa chiave API per abilitare la consegna dei dati a questo endpoint da Firehose.

- Secret

Seleziona un campo segreto Gestione dei segreti AWS che contenga la chiave API per New Relic. Se non vedi il tuo segreto nell'elenco a discesa, creane uno in [Gestione dei segreti AWS](#) Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Codifica del contenuto

Amazon Data Firehose utilizza la codifica del contenuto per comprimere il corpo di una richiesta prima di inviarla alla destinazione. Scegli GZIP o Disabilitato per la codifica enable/disable del contenuto della tua richiesta.

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati all'endpoint HTTP New Relic.

Dopo l'invio dei dati, Amazon Data Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati all'endpoint HTTP (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di conferma e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Configura le impostazioni di destinazione per Snowflake

Questa sezione descrive le opzioni per l'utilizzo di Snowflake per la destinazione.

Note

L'integrazione di Firehose con Snowflake è disponibile negli Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Europa (Irlanda), Stati Uniti orientali (Ohio), Asia Pacifico (Tokyo), Europa (Francoforte), Asia Pacifico (Singapore), Asia Pacifico (Seoul) e Asia Pacifico (Sydney), Asia Pacifico (Mumbai), Europa (Londra), Sud America (San Paolo), Canada (Centrale), Europa (Parigi), Asia Pacifico (Osaka), Europa (Stoccolma), Asia Pacifico (Giacarta). Regioni AWS

Impostazioni di connessione

- Fornisci i valori per i seguenti campi:

URL dell'account Snowflake

Specificate l'URL di un account Snowflake. Ad esempio: `xy12345.us-east-1.aws.snowflakecomputing.com`. Consulta la [documentazione di Snowflake](#) su come determinare l'URL del tuo account. Tieni presente che non devi specificare il numero di porta, mentre il protocollo (`https://`) è facoltativo.

Autenticazione

Puoi scegliere di inserire manualmente userlogin, chiave privata e passphrase oppure recuperare il codice segreto per accedere a Snowflake. Gestione dei segreti AWS

- Login utente

Specificare l'utente Snowflake da utilizzare per il caricamento dei dati. Assicurati che l'utente abbia accesso per inserire i dati nella tabella Snowflake.

- Chiave privata

Specificate la chiave privata per l'autenticazione con Snowflake nel formato PKCS8. Inoltre, non includete l'intestazione e il piè di pagina PEM come parte della chiave privata. Se la chiave è divisa su più righe, rimuovi le interruzioni di riga. Di seguito è riportato un esempio di come deve essere la tua chiave privata.

```
-----BEGIN PRIVATE KEY-----  
KEY_CONTENT  
-----END PRIVATE KEY-----
```

Rimuovi lo spazio all'interno KEY_CONTENT e forniscilo a Firehose. Sono richiesti caratteri netti header/footer o di nuova riga.

- Passphrase

Specifica la passphrase per decrittografare la chiave privata crittografata. Puoi lasciare vuoto questo campo se la chiave privata non è crittografata. Per informazioni, consulta [Utilizzo dell'autenticazione a coppie di chiavi e della rotazione delle chiavi](#).

- Secret

Seleziona un campo segreto Gestione dei segreti AWS che contenga le credenziali per Snowflake. Se non vedi il tuo segreto nell'elenco a discesa, creane uno in Gestione dei segreti AWS. Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Configurazione dei ruoli

Usa il ruolo Snowflake predefinito: se questa opzione è selezionata, Firehose non passerà alcun ruolo a Snowflake. Si presume che il ruolo predefinito sia il caricamento dei dati. Assicurati che il ruolo predefinito disponga dell'autorizzazione per inserire dati nella tabella Snowflake.

Usa il ruolo Snowflake personalizzato: inserisci un ruolo Snowflake non predefinito che verrà assunto da Firehose durante il caricamento dei dati nella tabella Snowflake.

Connettività Snowflake

Le opzioni sono Privato o Pubblico.

ID VPCE privato (opzionale)

L'ID VPCE per consentire a Firehose di connettersi privatamente con Snowflake. Il formato ID è `com.amazonaws.vpce.[regione].vpce-svc-[id]`. [Per ulteriori informazioni, vedere & Snowflake.AWS PrivateLink](#)

Note

Se il tuo cluster Snowflake è abilitato al collegamento privato, utilizza una policy di rete `AwsVpceIds` basata su una politica di rete per consentire i dati di Amazon Data Firehose. Firehose non richiede la configurazione di una politica di rete basata su IP nel tuo account Snowflake. L'attivazione di una policy di rete basata su IP potrebbe interferire con la connettività Firehose. [Se hai un caso limite che richiede una policy basata su IP, contatta il team di Firehose inviando un ticket di supporto.](#) Per un elenco dei VPCE IDs che puoi utilizzare, consulta. [Accesso a Snowflake in VPC](#)

Configurazione del database

- Per utilizzare Snowflake come destinazione per il flusso di Firehose, è necessario specificare le seguenti impostazioni:
 - Database Snowflake: tutti i dati in Snowflake vengono mantenuti nei database.
 - Schema Snowflake: ogni database è costituito da uno o più schemi, che sono raggruppamenti logici di oggetti del database, come tabelle e viste
 - Tabella Snowflake: tutti i dati in Snowflake vengono archiviati in tabelle di database, strutturate logicamente come raccolte di colonne e righe.

Opzioni di caricamento dei dati per la tabella Snowflake

- Usa le chiavi JSON come nomi di colonna
- Usa le colonne VARIANT
 - Nome della colonna di contenuto: specifica il nome di una colonna nella tabella, in cui devono essere caricati i dati grezzi.

- Nome della colonna di metadati (opzionale): specifica un nome di colonna nella tabella, in cui devono essere caricate le informazioni sui metadati. Quando abiliti questo campo, vedrai la colonna seguente nella tabella Snowflake in base al tipo di fonte.

Per Direct PUT come sorgente

```
{
  "firehoseDeliveryStreamName" : "streamname",
  "IngestionTime" : "timestamp"
}
```

Per Kinesis Data Stream come sorgente

```
{
  "kinesisStreamName" : "streamname",
  "kinesisShardId" : "Id",
  "kinesisPartitionKey" : "key",
  "kinesisSequenceNumber" : "1234",
  "subsequenceNumber" : "2334",
  "IngestionTime" : "timestamp"
}
```

Retry duration (Durata nuovi tentativi)

Intervallo di tempo (0—7200 secondi) entro cui Firehose riprova se l'apertura del canale o la consegna a Snowflake falliscono a causa di problemi del servizio Snowflake. Firehose riprova con un backoff esponenziale fino al termine della durata del nuovo tentativo. Se si imposta la durata del nuovo tentativo su 0 (zero) secondi, Firehose non riprova in caso di errori Snowflake e indirizza i dati al bucket di errore di Amazon S3.

Suggerimenti sul buffer

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro. Per ulteriori informazioni, consulta [Configura i suggerimenti per il buffering](#).

Configura le impostazioni di destinazione per Splunk

Questa sezione descrive le opzioni per l'utilizzo di Splunk come destinazione.

Note

Firehose fornisce dati ai cluster Splunk configurati con Classic Load Balancer o Application Load Balancer.

- Fornisci i valori per i seguenti campi:

Splunk cluster endpoint (Endpoint del cluster Splunk)

Per determinare l'endpoint, consulta [Configurare Amazon Data Firehose per inviare dati alla piattaforma Splunk nella documentazione Splunk](#).

Splunk endpoint type (Tipo endpoint Splunk)

Selezionare Raw endpoint nella maggior parte dei casi, Scegli Event endpoint se hai preelaborato i dati utilizzando AWS Lambda per inviare dati a diversi indici in base al tipo di evento. Per informazioni su quale endpoint utilizzare, consulta l'argomento relativo alla [configurazione di Amazon Data Firehose per l'invio di dati alla piattaforma Splunk](#) nella documentazione di Splunk.

Autenticazione

Puoi scegliere di inserire direttamente il token di autenticazione o recuperare il segreto da Gestione dei segreti AWS cui accedere a Splunk.

- Authentication token (Token di autenticazione)

Per configurare un endpoint Splunk in grado di ricevere dati da Amazon Data Firehose, consulta [Panoramica sull'installazione e la configurazione del componente aggiuntivo Splunk per Amazon Data Firehose](#) nella documentazione di Splunk. Salva il token che ottieni da Splunk quando configuri l'endpoint per questo stream Firehose e aggiungilo qui.

- Secret

Seleziona un codice segreto Gestione dei segreti AWS che contenga il token di autenticazione per Splunk. Se non vedi il tuo segreto nell'elenco a discesa, creane uno in Gestione dei segreti AWS Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

HEC acknowledgement timeout (Timeout riconoscimento HEC)

Specificate per quanto tempo Amazon Data Firehose attende la conferma dell'indice da parte di Splunk. Se Splunk non invia la conferma prima del raggiungimento del timeout, Amazon Data Firehose lo considera un errore di consegna dei dati. Amazon Data Firehose quindi riprova o esegue il backup dei dati nel bucket Amazon S3, a seconda del valore della durata dei tentativi impostato.

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati a Splunk.

Dopo l'invio dei dati, Amazon Data Firehose attende prima un riconoscimento da parte di Splunk. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati a Splunk (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di riconoscimento e attende una conferma da parte di Splunk.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia in base al fornitore di servizi.

Configura le impostazioni di destinazione per Splunk Observability Cloud

Questa sezione descrive le opzioni per l'utilizzo di Splunk Observability Cloud come destinazione. Per ulteriori informazioni, consulta [https://docs.splunk.com/observability/en/gdi/get-data-in/connect/aws/aws-apiconfig.html# -api connect-to-aws-using.the-splunk-observability-cloud](https://docs.splunk.com/observability/en/gdi/get-data-in/connect/aws/aws-apiconfig.html#-api-connect-to-aws-using.the-splunk-observability-cloud)

- Fornisci i valori per i seguenti campi:

URL dell'endpoint di inserimento del cloud

L'URL di inserimento dati in tempo reale di Splunk Observability Cloud si trova in Profilo > Organizzazioni > Endpoint di inserimento dati in tempo reale nella console di Splunk Observability.

Autenticazione

Puoi scegliere di inserire direttamente il token di accesso o recuperare il codice segreto per accedere a Splunk Observability Cloud. Gestione dei segreti AWS

- Token di accesso

Copia il token di accesso Splunk Observability con l'ambito di autorizzazione INGEST da Token di accesso in Impostazioni della console Splunk Observability.

- Secret

Seleziona un segreto Gestione dei segreti AWS che contenga il token di accesso per Splunk Observability Cloud. Se non vedi il tuo segreto nell'elenco a discesa, creane uno in Gestione dei segreti AWS Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Codifica del contenuto

Amazon Data Firehose utilizza la codifica del contenuto per comprimere il corpo di una richiesta prima di inviarla alla destinazione. Scegli GZIP o Disabilitato per la codifica enable/disable del contenuto della tua richiesta.

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati all'endpoint HTTP selezionato.

Dopo l'invio dei dati, Amazon Data Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati all'endpoint HTTP (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di conferma e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione varia da un fornitore di servizi all'altro.

Configura le impostazioni di destinazione per Sumo Logic

Questa sezione descrive le opzioni per l'utilizzo di Sumo Logic come destinazione. Per ulteriori informazioni, consulta <https://www.sumologic.com>.

- Fornisci i valori per i seguenti campi:

URL dell'endpoint HTTP

Specifica l'URL per l'endpoint HTTP nel seguente formato: `https://deployment.name.sumologic.net/receiver/v1/kinesis/dataType/access token`. L'URL deve essere un URL HTTPS.

Codifica del contenuto

Amazon Data Firehose utilizza la codifica del contenuto per comprimere il corpo di una richiesta prima di inviarla alla destinazione. Scegli GZIP o Disabilitato per la codifica `enable/disable` del contenuto della tua richiesta.

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati a Sumo Logic.

Dopo l'invio dei dati, Amazon Data Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati all'endpoint HTTP (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di conferma e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione Elastic varia da un fornitore di servizi all'altro.

Configura le impostazioni di destinazione per Elastic

Questa sezione descrive le opzioni per l'utilizzo di Elastic come destinazione.

- Fornisci i valori per i seguenti campi:

URL dell'endpoint Elastic

Specifica l'URL per l'endpoint HTTP nel seguente formato: `https://<cluster-id>.es.<region>.aws.elastic-cloud.com`. L'URL deve essere un URL HTTPS.

Autenticazione

Puoi scegliere di inserire direttamente la chiave API o recuperare il codice segreto Gestione dei segreti AWS per accedere a Elastic.

- Chiave API

Contatta Elastic per ottenere da Firehose la chiave API necessaria per abilitare la consegna dei dati al suo servizio.

- Secret

Seleziona un campo segreto Gestione dei segreti AWS che contenga la chiave API per Elastic. Se non vedi il tuo segreto nell'elenco a discesa, creane uno in [Gestione dei segreti AWS](#). Per ulteriori informazioni, consulta [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#).

Codifica del contenuto

Amazon Data Firehose utilizza la codifica del contenuto per comprimere il corpo di una richiesta prima di inviarla alla destinazione. Scegli GZIP (che è quello selezionato per impostazione predefinita) o Disabilitato per la codifica enable/disable del contenuto della richiesta.

Retry duration (Durata nuovi tentativi)

Specificare per quanto tempo Amazon Data Firehose riprova a inviare dati a Elastic.

Dopo l'invio dei dati, Amazon Data Firehose attende innanzitutto un riconoscimento dall'endpoint HTTP. Se si verifica un errore o se il riconoscimento non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata dei nuovi tentativi. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati sul bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati all'endpoint HTTP (il tentativo iniziale o un nuovo tentativo), riavvia il contatore del timeout di conferma e attende una conferma dall'endpoint HTTP.

Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque la conferma finché non la riceve o non viene raggiunto il periodo di timeout per la conferma. Se la conferma scade, Amazon Data Firehose determina se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Se non desideri che Amazon Data Firehose tenti di inviare nuovamente i dati, imposta questo valore su 0.

Parametri: facoltativo

Amazon Data Firehose include queste coppie chiave-valore in ogni chiamata HTTP. Questi parametri consentono di identificare e organizzare le destinazioni.

Suggerimenti per il buffering

Amazon Data Firehose memorizza nel buffer i dati in entrata prima di consegnarli alla destinazione specificata. La dimensione del buffer consigliata per la destinazione Elastic è di 1 MiB.

Configurare le impostazioni di backup

Amazon Data Firehose utilizza Amazon S3 per eseguire il backup di tutti i dati (o solo quelli non riusciti) che tenta di consegnare alla destinazione prescelta.

⚠ Important

- Le impostazioni di backup sono supportate solo se l'origine del flusso Firehose è Direct PUT o Kinesis Data Streams.
- La funzionalità di zero buffering è disponibile solo per le destinazioni delle applicazioni e non è disponibile per la destinazione di backup Amazon S3.

È possibile specificare le impostazioni di backup S3 per lo stream Firehose se si è effettuata una delle seguenti scelte.

- Se imposti Amazon S3 come destinazione per il tuo stream Firehose e scegli di specificare una funzione AWS Lambda per trasformare i record di dati o se scegli di convertire i formati di record di dati per il tuo flusso Firehose.
- Se imposti Amazon Redshift come destinazione per il tuo stream Firehose e scegli di specificare una funzione AWS Lambda per trasformare i record di dati.
- Se imposti uno dei seguenti servizi come destinazione per il tuo stream Firehose: Amazon OpenSearch Service, Datadog, Dynatrace, HTTP Endpoint, LogicMonitor MongoDB Cloud, New Relic, Splunk o Sumo Logic, Snowflake, Apache Iceberg Tables.

Di seguito sono riportate le impostazioni di backup per lo stream Firehose.

- Backup dei record di origine in Amazon S3: se S3 o Amazon Redshift è la destinazione selezionata, questa impostazione indica se desideri abilitare il backup dei dati di origine o mantenerlo disabilitato. Se qualsiasi altro servizio supportato (diverso da S3 o da Amazon Redshift) è impostato come destinazione selezionata, questa impostazione indica se desideri eseguire il backup di tutti i dati di origine o solo dei dati non riusciti.
- Bucket di backup S3: questo è il bucket S3 in cui Amazon Data Firehose esegue il backup dei dati.
- Prefisso del bucket di backup S3: questo è il prefisso con cui Amazon Data Firehose esegue il backup dei dati.
- Prefisso di output degli errori del bucket di backup S3: il backup di tutti i dati non riusciti viene eseguito nel prefisso di output degli errori di questo bucket S3.
- Suggerimenti per il buffering, compressione e crittografia per il backup: Amazon Data Firehose utilizza Amazon S3 per eseguire il backup di tutti o solo i dati che tenta di consegnare alla destinazione prescelta. Amazon Data Firehose memorizza nel buffer i dati in entrata prima di

consegnarli (eseguendone il backup) su Amazon S3. Puoi scegliere una dimensione del buffer di 1—128 e un intervallo di buffer di 60—900 secondi MiBs . La condizione che viene soddisfatta per prima attiva la distribuzione dei dati ad Amazon S3. Se abiliti la trasformazione dei dati, l'intervallo di buffer si applica dal momento in cui i dati trasformati vengono ricevuti da Amazon Data Firehose alla consegna dei dati ad Amazon S3. Se la consegna dei dati alla destinazione è inferiore alla scrittura dei dati nel flusso Firehose, Amazon Data Firehose aumenta la dimensione del buffer in modo dinamico per recuperare il ritardo. Questa azione aiuta a garantire che tutti i dati vengano consegnati alla destinazione.

- **Compressione S3:** scegli la compressione dei dati Snappy con GZIP, Snappy, Zip o Snappy compatibile con Hadoop oppure nessuna compressione dei dati. La compressione Snappy compatibile con Snappy, Zip e Hadoop non è disponibile per lo stream Firehose con Amazon Redshift come destinazione.
- **Formato di estensione file S3 (opzionale):** specifica un formato di estensione di file per gli oggetti consegnati al bucket di destinazione Amazon S3. Se abiliti questa funzionalità, l'estensione di file specificata sostituirà le estensioni di file predefinite aggiunte dalle funzionalità di compressione Data Format Conversion o S3 come .parquet o .gz. Assicurati di aver configurato l'estensione di file corretta quando usi questa funzionalità con Data Format Conversion o la compressione S3. L'estensione del file deve iniziare con un punto (.) e può contenere caratteri consentiti: 0-9a-z! - _.*' (). L'estensione del file non può superare i 128 caratteri.
- **Firehose supporta la crittografia lato server di Amazon S3 AWS Key Management Service con (SSE-KMS) per crittografare i dati forniti in Amazon S3.** Puoi scegliere di utilizzare il tipo di crittografia predefinito specificato nel bucket S3 di destinazione o di crittografare con una chiave dall'elenco di chiavi di tua proprietà. AWS KMS Se crittografi i dati con le AWS KMS chiavi, puoi utilizzare la chiave AWS gestita predefinita (aws/s3) o una chiave gestita dal cliente. Per ulteriori informazioni, consulta [Protezione dei dati mediante la crittografia lato server con AWS chiavi gestite da KMS \(SSE-KMS\)](#).

Configura i suggerimenti per il buffering

Amazon Data Firehose memorizza i dati di streaming in entrata fino a una certa dimensione (dimensione di buffering) e per un determinato periodo di tempo (intervallo di buffering) prima di consegnarli alle destinazioni specificate. I suggerimenti di buffering possono essere utilizzati quando si desidera distribuire file di dimensioni ottimali ad Amazon S3 e ottenere prestazioni migliori dalle applicazioni di elaborazione dati o per adattare la velocità di consegna di Firehose alla velocità di destinazione.

È possibile configurare la dimensione e l'intervallo di buffer durante la creazione di nuovi flussi Firehose o aggiornare la dimensione e l'intervallo di buffering sui flussi Firehose esistenti. La dimensione del buffering viene misurata in e l'intervallo di buffering viene misurato in secondi. MBs Tuttavia, se specifichi un valore per uno di essi, devi fornire un valore per l'altro. La prima condizione del buffer soddisfatta attiva Firehose per fornire i dati. Se non si configurano i valori di buffering, vengono utilizzati i valori predefiniti.

È possibile configurare i suggerimenti di buffering di Firehose tramite, o. Console di gestione AWS AWS Command Line Interface AWS SDKs Per gli stream esistenti, è possibile riconfigurare i suggerimenti di buffering con un valore adatto ai casi d'uso utilizzando l'opzione Modifica nella console o utilizzando l'API. [UpdateDestination](#) Per i nuovi stream, puoi configurare i suggerimenti di buffering come parte della creazione di nuovi stream utilizzando la console o l'API. [CreateDeliveryStream](#) Per regolare la dimensione del buffering, imposta `SizeInMBs` e `IntervalInSeconds` inserisci il `DestinationConfiguration` parametro specifico di destinazione dell'API or. [CreateDeliveryStreamUpdateDestination](#)

Note

- I suggerimenti sul buffer vengono applicati a livello di shard o di partizione, mentre i suggerimenti sul buffer di partizionamento dinamico vengono applicati a livello di stream o topic.
- Per soddisfare le latenze più basse dei casi d'uso in tempo reale, puoi utilizzare un hint a intervallo di buffering zero. Quando si configura l'intervallo di buffering su zero secondi, Firehose non memorizzerà i dati nel buffer e li consegnerà entro pochi secondi. Prima di modificare i suggerimenti di buffering con un valore inferiore, rivolgiti al fornitore per conoscere i suggerimenti di buffering consigliati da Firehose per le relative destinazioni.
- La funzionalità di zero buffering è disponibile solo per le destinazioni delle applicazioni e non è disponibile per la destinazione di backup Amazon S3.
- La funzionalità Zero Buffering non è disponibile per il partizionamento dinamico.
- Firehose utilizza il caricamento in più parti per la destinazione S3 quando si configura un intervallo di tempo del buffer inferiore a 60 secondi per offrire latenze inferiori. A causa del caricamento in più parti per la destinazione S3, noterai un certo aumento dei costi dell'PUTAPI S3 se scegli un intervallo di tempo di buffer inferiore a 60 secondi.

Per gli intervalli di suggerimenti per il buffering specifici della destinazione e i valori predefiniti, consulta la seguente tabella:

Destinazione	Dimensione del buffering in MB (impostazione predefinita tra parentesi)	Intervallo di buffering in secondi (impostazione predefinita tra parentesi)
Simple Storage Service (Amazon S3)	1-128 (5)	0-900 (300)
Tavoli Apache Iceberg	1-128 (5)	0-900 (300)
Amazon Redshift	1-128 (5)	0-900 (300)
OpenSearch Senza server	1-100 (5)	0-900 (300)
OpenSearch	1-100 (5)	0-900 (300)
Splunk	1-5 (5)	0-60 (60)
Datadog	1-4 (4)	0-900 (60)
Coralogix	1-64 (6)	0-900 (60)
Dynatrace	1-64 (5)	0-900 (60)
Elastic	1	0-900 (60)
Honeycomb	1-64 (15)	0-900 (60)
Endpoint HTTP	1-64 (5)	0-900 (60)
LogicMonitor	1-64 (5)	0-900 (60)
Loggiato	1-64 (5)	0-900 (60)

Destinazione	Dimensione del buffering in MB (impostazione predefinita tra parentesi)	Intervallo di buffering in secondi (impostazione predefinita tra parentesi)
MongoDB	1-16 (5)	0-900 (60)
Nuova reliquia	1-64 (5)	0-900 (60)
SumoLogic	1-64 (1)	0-900 (60)
Splunk Observability Cloud	1-64 (1)	0-900 (60)
Snowflake	1 - 128 (1)	0 - 900 (0)

Configurare le impostazioni avanzate

La sezione seguente contiene dettagli sulle impostazioni avanzate per lo stream Firehose.

- **Crittografia lato server:** Amazon Data Firehose supporta la crittografia lato server Amazon S3 con AWS Key Management Service (AWS KMS) per crittografare i dati forniti in Amazon S3. Per ulteriori informazioni, consulta [Protezione dei dati tramite crittografia lato server con chiavi gestite da KMS \(SSE-KMS\)](#). AWS
- **Registrazione degli errori:** Amazon Data Firehose registra gli errori relativi all'elaborazione e alla consegna. Inoltre, quando la trasformazione dei dati è abilitata, può registrare le chiamate Lambda e inviare errori di consegna dei dati ai registri. CloudWatch Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose utilizzando i log CloudWatch](#).

Important

Sebbene facoltativo, si consiglia vivamente di abilitare la registrazione degli errori di Amazon Data Firehose durante la creazione di stream Firehose. Questa pratica garantisce la possibilità di accedere ai dettagli degli errori in caso di errori di elaborazione o distribuzione dei record.

- **Autorizzazioni:** Amazon Data Firehose utilizza i ruoli IAM per tutte le autorizzazioni necessarie allo stream Firehose. Puoi scegliere di creare un nuovo ruolo in cui le autorizzazioni richieste vengono assegnate automaticamente o scegliere un ruolo esistente creato per Amazon Data Firehose. Il ruolo viene utilizzato per concedere a Firehose l'accesso a vari servizi, tra cui il bucket S3, la chiave AWS KMS (se la crittografia dei dati è abilitata) e la funzione Lambda (se la trasformazione dei dati è abilitata). La console potrebbe creare un ruolo con segnaposto. Per ulteriori informazioni, consulta [Cos'è IAM?](#).

Note

Il ruolo IAM (inclusi i placeholder) viene creato in base alla configurazione scelta durante la creazione di uno stream Firehose. Se si apportano modifiche all'origine o alla destinazione del flusso Firehose, è necessario aggiornare manualmente il ruolo IAM.

- **Tag:** puoi aggiungere tag per organizzare AWS le risorse, tenere traccia dei costi e controllare l'accesso.

Se specifichi tag nell'`CreateDeliveryStreamazione`, Amazon Data Firehose esegue un'autorizzazione aggiuntiva sull'`firehose:TagDeliveryStreamazione` per verificare se gli utenti dispongono delle autorizzazioni per creare tag. Se non si fornisce questa autorizzazione, le richieste di creazione di nuovi flussi Firehose con tag di risorse IAM falliranno con uno degli `AccessDeniedException` esempi seguenti.

```
AccessDeniedException
```

```
User: arn:aws:sts::x:assumed-role/x/x is not authorized to perform:
  firehose:TagDeliveryStream on resource: arn:aws:firehose:us-east-1:x:deliverystream/
  x with an explicit deny in an identity-based policy.
```

L'esempio seguente illustra una politica che consente agli utenti di creare uno stream Firehose e applicare i tag.

Dopo aver scelto le impostazioni di backup e avanzate, rivedi le tue scelte, quindi scegli `Create Firehose stream`.

Il nuovo stream Firehose impiega alcuni istanti nello stato `Creating` prima di essere disponibile. Dopo che lo stream Firehose è in stato `Attivo`, puoi iniziare a inviargli dati dal tuo produttore.

Test del flusso Firehose con dati di esempio

È possibile utilizzarli Console di gestione AWS per importare dati simulati sulle quotazioni azionarie. La console esegue uno script nel browser per inserire record di esempio nello stream Firehose. Ciò consente di testare la configurazione dello stream Firehose senza dover generare i propri dati di test.

Di seguito un esempio dei dati simulati:

```
{"TICKER_SYMBOL": "QXZ", "SECTOR": "HEALTHCARE", "CHANGE": -0.05, "PRICE": 84.51}
```

Tieni presente che le tariffe standard di Amazon Data Firehose si applicano quando lo stream Firehose trasmette i dati, ma non è previsto alcun addebito quando i dati vengono generati. Per arrestare l'addebito di questi costi, puoi interrompere il flusso di esempio dalla console in qualsiasi momento.

Prerequisiti

Prima di iniziare, create uno stream Firehose. Per ulteriori informazioni, consulta [Tutorial: Creare uno stream Firehose dalla console](#).

Prova con Amazon S3

Utilizza la seguente procedura per testare lo stream Firehose con Amazon Simple Storage Service (Amazon S3) come destinazione.

Per testare uno stream Firehose utilizzando Amazon S3

1. Aprire la console Firehose all'indirizzo. <https://console.aws.amazon.com/firehose/>
2. Scegliete uno stream Firehose attivo. Lo stream Firehose deve essere in stato Attivo prima di poter iniziare a inviare dati.
3. In Test with demo data (Test con dati di demo), selezionare Start sending demo data (Inizia l'invio di dati di demo) per generare dati su ticket di titoli di esempio.
4. Seguire le istruzioni sullo schermo per verificare che i dati vengano distribuiti sul bucket S3. Alcuni oggetti potrebbero impiegare qualche minuto per comparire nel bucket, in base alla configurazione di buffering del bucket.

5. Al termine del test, selezionare Stop sending demo data (Arresta l'invio di dati di demo) per interrompere l'addebito dei costi di utilizzo.

Esegui test con Amazon Redshift

Utilizza la seguente procedura per testare il tuo stream Firehose con Amazon Redshift come destinazione.

Per testare uno stream Firehose utilizzando Amazon Redshift

1. Lo stream Firehose prevede la presenza di una tabella nel cluster Amazon Redshift. [Connettersi ad Amazon Redshift tramite un'interfaccia SQL](#) ed eseguire la seguente istruzione per creare una tabella in grado di accettare i dati di esempio.

```
create table firehose_test_table
(
  TICKER_SYMBOL varchar(4),
  SECTOR varchar(16),
  CHANGE float,
  PRICE float
);
```

2. Aprire la console Firehose all'indirizzo. <https://console.aws.amazon.com/firehose/>
3. Scegliete uno stream Firehose attivo. Lo stream Firehose deve essere in stato Attivo prima di poter iniziare a inviare dati.
4. Modifica i dettagli della destinazione dello stream Firehose in modo che punti alla tabella appena creata `firehose_test_table`.
5. In Test with demo data (Test con dati di demo), selezionare Start sending demo data (Inizia l'invio di dati di demo) per generare dati su ticket di titoli di esempio.
6. Seguire le istruzioni sullo schermo per verificare che i dati vengano distribuiti sulla tabella. Alcune righe potrebbero impiegare qualche minuto per comparire nella tabella in base alla configurazione di buffering.
7. Al termine del test, selezionare Stop sending demo data (Arresta l'invio di dati di demo) per interrompere l'addebito dei costi di utilizzo.
8. Modifica i dettagli della destinazione dello stream Firehose in modo che punti a un'altra tabella.
9. (Opzionale) Eliminare la tabella `firehose_test_table`.

Esegui il test con Service OpenSearch

Utilizza la seguente procedura per testare lo stream Firehose utilizzando Amazon OpenSearch Service come destinazione.

Per testare uno stream Firehose utilizzando Service OpenSearch

1. Aprire la console Firehose all'indirizzo. <https://console.aws.amazon.com/firehose/>
2. Scegliete uno stream Firehose attivo. Lo stream Firehose deve essere in stato Attivo prima di poter iniziare a inviare dati.
3. In Test with demo data (Test con dati di demo), selezionare Start sending demo data (Inizia l'invio di dati di demo) per generare dati su ticket di titoli di esempio.
4. Segui le istruzioni sullo schermo per verificare che i dati vengano recapitati al tuo dominio di OpenSearch servizio. Per ulteriori informazioni, consulta [Searching Documents in an OpenSearch Service Domain](#) nella Amazon OpenSearch Service Developer Guide.
5. Al termine del test, selezionare Stop sending demo data (Arresta l'invio di dati di demo) per interrompere l'addebito dei costi di utilizzo.

Prova con Splunk

Usa la seguente procedura per testare lo stream Firehose usando Splunk come destinazione.

Per testare uno stream Firehose usando Splunk

1. Aprire la console Firehose all'indirizzo. <https://console.aws.amazon.com/firehose/>
2. Scegliete uno stream Firehose attivo. Lo stream Firehose deve essere in stato Attivo prima di poter iniziare a inviare dati.
3. In Test with demo data (Test con dati di demo), selezionare Start sending demo data (Inizia l'invio di dati di demo) per generare dati su ticket di titoli di esempio.
4. Controllare se i dati vengono distribuiti all'indice Splunk. Esempi di termini di ricerca in Splunk sono `sourcetype="aws:firehose:json"` e `index="name-of-your-splunk-index"`. Per ulteriori informazioni su come cercare eventi in Splunk, consulta l'argomento [Ricerca manuale](#) nella documentazione di Splunk.

Se i dati di test non compaiono nell'indice Splunk, verifica nel bucket Amazon S3 gli eventi non andati a buon fine. Consulta anche [Dati non distribuiti su Splunk](#).

5. Al termine del test, selezionare Stop sending demo data (Arresta l'invio di dati di demo) per interrompere l'addebito dei costi di utilizzo.

Prova con Apache Iceberg Tables

Utilizzate la seguente procedura per testare lo stream Firehose con Apache Iceberg Tables come destinazione.

Per testare uno stream Firehose utilizzando Apache Iceberg Tables

1. Aprire la console Firehose all'indirizzo. <https://console.aws.amazon.com/firehose/>
2. Scegliete uno stream Firehose attivo. Lo stream Firehose deve essere in stato Attivo prima di poter iniziare a inviare dati.
3. In Test with demo data (Test con dati di demo), selezionare Start sending demo data (Inizia l'invio di dati di demo) per generare dati su ticket di titoli di esempio.
4. Segui le istruzioni sullo schermo per verificare che i dati vengano consegnati alle tue tabelle Apache Iceberg. Tieni presente che potrebbero essere necessari alcuni minuti prima che nuovi oggetti appaiano nel bucket, in base alla sua configurazione di buffering.
5. Se i dati del test non vengono visualizzati nelle tabelle Apache Iceberg, verifica la presenza di eventi non riusciti nel bucket Amazon S3.
6. Al termine del test, selezionare Stop sending demo data (Arresta l'invio di dati di demo) per interrompere l'addebito dei costi di utilizzo.

Inviare dati a uno stream Firehose

Questa sezione descrive come utilizzare diverse fonti di dati per inviare dati allo stream Firehose. Se non conosci Amazon Data Firehose, prenditi del tempo per acquisire familiarità con i concetti e la terminologia presentati in [Cos'è Amazon Data Firehose?](#)

Note

Alcuni AWS servizi possono inviare messaggi ed eventi solo a uno stream Firehose che si trova nella stessa regione. Se lo stream Firehose non viene visualizzato come opzione quando configuri un target per Amazon CloudWatch Logs, CloudWatch Events oppure AWS IoT, verifica che lo stream Firehose si trovi nella stessa regione degli altri servizi. Per informazioni sugli endpoint di servizio per ciascuna regione, consulta gli endpoint di [Amazon Data Firehose](#).

È possibile inviare dati al proprio stream Firehose dalle seguenti fonti di dati.

Argomenti

- [Configurare l'agente Kinesis per l'invio di dati](#)
- [Inviare dati con AWS SDK](#)
- [Invia CloudWatch log a Firehose](#)
- [Invia CloudWatch eventi a Firehose](#)
- [AWS IoT Configurare l'invio di dati a Firehose](#)

Configurare l'agente Kinesis per l'invio di dati

L'agente Amazon Kinesis è un'applicazione software Java autonoma che funge da implementazione di riferimento per mostrare come raccogliere e inviare dati a Firehose. L'agente monitora continuamente un set di file e invia nuovi dati allo stream Firehose. L'agente mostra come gestire la rotazione dei file, il checkpoint e riprovare in caso di errore. Mostra come è possibile fornire i dati in modo affidabile, tempestivo e semplice. Mostra anche come è possibile emettere CloudWatch metriche per monitorare e risolvere meglio il processo di streaming. [Per saperne di più, awslabs/.amazon-kinesis-agent](#)

Come impostazione predefinita, i record vengono analizzati da ciascun file in base alla nuova riga di caratteri ('\n'). Tuttavia, l'agente può anche essere configurato per analizzare record a più righe (consulta [Specificare le impostazioni di configurazione dell'agente](#)).

Puoi installare l'agente su ambienti server basati su Linux, come server Web, server di log e server di database. Dopo aver installato l'agente, configuralo specificando i file da monitorare e il flusso Firehose per i dati. Una volta configurato, l'agente raccoglie in modo duraturo i dati dai file e li invia in modo affidabile al flusso Firehose.

Prerequisiti

Prima di iniziare a utilizzare Kinesis Agent, assicurati di soddisfare i seguenti prerequisiti.

- Il sistema operativo deve essere Amazon Linux o Red Hat Enterprise Linux versione 7 o successiva.
- La versione 2.0.0 o successiva dell'agente viene eseguita utilizzando la versione JRE 1.8 o successiva. La versione 1.1.x dell'agente viene eseguita utilizzando JRE 1.7 o una versione successiva.
- Se utilizzi Amazon EC2 per eseguire l'agente, avvia l'istanza EC2.
- Il ruolo o AWS le credenziali IAM che specifichi devono essere autorizzati a eseguire l'operazione Amazon Data [PutRecordBatch](#) Firehose affinché l'agente possa inviare dati al tuo flusso Firehose. Se abiliti il CloudWatch monitoraggio per l'agente, è necessaria anche l'autorizzazione a eseguire l' CloudWatch [PutMetricData](#) operazione. Per ulteriori informazioni [Controllo dell'accesso con Amazon Data Firehose](#) Monitora lo stato di Kinesis Agent, consulta [Autenticazione e controllo degli accessi per Amazon CloudWatch](#).

Gestisci le AWS credenziali

Gestisci AWS le tue credenziali utilizzando uno dei seguenti metodi:

- Crea un fornitore di credenziali personalizzate. Per informazioni dettagliate, vedi [the section called "Crea provider di credenziali personalizzati"](#).
- Specifica un ruolo IAM quando avvii l'istanza EC2.
- Specificate AWS le credenziali quando configurate l'agente (consultate le voci relative `awsAccessKeyId` e `awsSecretAccessKey` nella tabella di configurazione riportata sotto [the section called "Specificare le impostazioni di configurazione dell'agente"](#)).

- Modifica `/etc/sysconfig/aws-kinesis-agent` per specificare la AWS regione e le chiavi di AWS accesso.
- Se la tua istanza EC2 si trova in un AWS account diverso, crea un ruolo IAM per fornire l'accesso al servizio Amazon Data Firehose. [Specificate quel ruolo quando configurate l'agente \(vedete `AssumeroLearn` e `IdassumeRoleExternal`\)](#). Utilizzate uno dei metodi precedenti per specificare le AWS credenziali di un utente nell'altro account che dispone del permesso di assumere questo ruolo.

Crea provider di credenziali personalizzati

Puoi creare un fornitore di credenziali personalizzate e assegnare il nome della classe e il percorso jar all'agente Kinesis nelle seguenti impostazioni di configurazione: `userDefinedCredentialsProvider.classname` e `userDefinedCredentialsProvider.location`. Per le descrizioni di queste due impostazioni di configurazione, consulta [the section called "Specificare le impostazioni di configurazione dell'agente"](#).

Per creare un fornitore di credenziali personalizzate, definisci una classe che implementa l'interfaccia `AWS CredentialsProvider`, come quella nell'esempio seguente.

```
import com.amazonaws.auth.AWSCredentials;
import com.amazonaws.auth.AWSCredentialsProvider;
import com.amazonaws.auth.BasicAWSCredentials;

public class YourClassName implements AWSCredentialsProvider {
    public YourClassName() {
    }

    public AWSCredentials getCredentials() {
        return new BasicAWSCredentials("key1", "key2");
    }

    public void refresh() {
    }
}
```

La classe deve avere un costruttore che non accetti argomenti.

AWS richiama periodicamente il metodo di aggiornamento per ottenere credenziali aggiornate. Se desideri che il fornitore di credenziali fornisca credenziali diverse per tutta la sua durata, includi il

codice per aggiornare le credenziali con questo metodo. In alternativa, puoi lasciare vuoto questo metodo se desideri un fornitore di credenziali che offra credenziali statiche (non modificabili).

Scarica e installa l'agente

Innanzitutto connettiti all'istanza, Per ulteriori informazioni, consulta [Connect to Your Instance](#) nella Amazon EC2 User Guide. In caso di problemi di connessione, consulta [Risoluzione dei problemi di connessione alla tua istanza](#) nella Guida per l'utente di Amazon EC2.

Quindi, installa l'agente utilizzando uno dei seguenti metodi.

- Configurazione dell'agente dai repository Amazon Linux

Questo metodo funziona solo per le istanze Amazon Linux. Utilizzando il seguente comando:

```
sudo yum install -y aws-kinesis-agent
```

Agent v 2.0.0 o successivo è installato su computer con sistema operativo Amazon Linux 2 (AL2). Questa versione dell'agente richiede Java 1.8 o la versione successiva. Se la versione Java richiesta non è ancora presente, viene installata durante il processo di installazione dell'agente. Per ulteriori informazioni su Amazon Linux 2, consulta <https://aws.amazon.com/amazon-linux-2/>.

- Configurazione dell'agente dal repository Amazon S3

Questo metodo funziona per Red Hat Enterprise Linux e per le istanze di Amazon Linux 2 perché installa l'agente dal repository disponibile pubblicamente. Utilizza il comando seguente per scaricare e installare la versione più recente dell'agente versione 2.x.x:

```
sudo yum install -y https://s3.amazonaws.com/streaming-data-agent/aws-kinesis-agent-latest.amzn2.noarch.rpm
```

Per installare una versione specifica dell'agente, specifica il numero di versione nel comando. Ad esempio, il seguente comando installa l'agente 2.0.1.

```
sudo yum install -y https://streaming-data-agent.s3.amazonaws.com/aws-kinesis-agent-2.0.1-1.amzn1.noarch.rpm
```

Se disponi di Java 1.7 e non vuoi aggiornarlo, puoi scaricare la versione 1.x.x dell'agente, che è compatibile con Java 1.7. Ad esempio, per scaricare l'agente 1.1.6, puoi utilizzare il seguente comando:

```
sudo yum install -y https://s3.amazonaws.com/streaming-data-agent/aws-kinesis-agent-1.1.6-1.amzn1.noarch.rpm
```

Puoi scaricare l'agente più recente con il seguente comando

```
sudo yum install -y https://s3.amazonaws.com/streaming-data-agent/aws-kinesis-agent-latest.amzn2.noarch.rpm
```

- Per configurare l'agente dal GitHub repository
 1. Innanzitutto, assicurati che sia installata la versione Java richiesta, in base alla versione dell'agente.
 2. Scarica l'agente dal repository [awslabs/ amazon-kinesis-agent](#) GitHub .
 3. Installare l'agente spostandosi nella directory di download ed eseguendo il comando seguente:

```
sudo ./setup --install
```

- Configurazione dell'agente in un container Docker

L'agente Kinesis può essere eseguito anche in un container tramite la base container [amazonlinux](#). Utilizza il seguente Dockerfile e poi esegui `docker build`.

```
FROM amazonlinux

RUN yum install -y aws-kinesis-agent which findutils
COPY agent.json /etc/aws-kinesis/agent.json

CMD ["start-aws-kinesis-agent"]
```

Configura e avvia l'agente

Configurazione e avvio dell'agente

1. Aprire e modificare il file di configurazione (come superutente se vengono utilizzate le autorizzazioni predefinite di accesso al file): `/etc/aws-kinesis/agent.json`

In questo file di configurazione, specificate i file ("`filePattern`") da cui l'agente raccoglie i dati e il nome del flusso Firehose "`deliveryStream`" () a cui l'agente invia i dati. Il nome del file è un modello e l'agente riconosce le rotazioni dei file. Puoi ruotare i file o creare nuovi file non più di una volta al secondo. L'agente utilizza il timestamp di creazione dei file per determinare quali file tracciare e inserire nel flusso Firehose. La creazione di nuovi file o la rotazione di file più frequentemente di una volta al secondo non consente all'agente di distinguerli in modo corretto.

```
{
  "flows": [
    {
      "filePattern": "/tmp/app.log*",
      "deliveryStream": "yourdeliverystream"
    }
  ]
}
```

La AWS regione predefinita è `us-east-1`. Se utilizzi una regione diversa, aggiungi l'impostazione `firehose.endpoint` al file di configurazione, specificando l'endpoint della regione in uso. Per ulteriori informazioni, consulta [Specificare le impostazioni di configurazione dell'agente](#).

2. Avvia l'agente manualmente:

```
sudo service aws-kinesis-agent start
```

3. (Facoltativo) Configurare l'agente per iniziare l'avvio del sistema:

```
sudo chkconfig aws-kinesis-agent on
```

L'agente è ora in esecuzione come servizio di sistema in background. Monitora continuamente i file specificati e invia i dati al flusso Firehose specificato. L'attività dell'agente viene registrata in `/var/log/aws-kinesis-agent/aws-kinesis-agent.log`.

Specificare le impostazioni di configurazione dell'agente

L'agente supporta due impostazioni di configurazione obbligatorie, `filePattern` e `deliveryStream`, oltre a impostazioni di configurazione opzionali per funzionalità aggiuntive. Puoi specificare le impostazioni di configurazione obbligatoria e opzionale in `/etc/aws-kinesis/agent.json`.

Quando modifichi il file di configurazione, devi arrestare e avviare l'agente, utilizzando i comandi seguenti:

```
sudo service aws-kinesis-agent stop
sudo service aws-kinesis-agent start
```

In alternativa, potresti utilizzare il comando seguente:

```
sudo service aws-kinesis-agent restart
```


Seguono le impostazioni di configurazione generali.

Impostazione di configurazione	Description
<code>assumeRoleARN</code>	L'Amazon Resource Name (ARN) del ruolo che deve essere assunto dall'utente. Per ulteriori informazioni, consulta Delegare l'accesso tra AWS account utilizzando i ruoli IAM nella Guida per l'utente IAM.
<code>assumeRoleExternalId</code>	Si è verificato un identificatore opzionale che determina chi può assumere il ruolo. Per ulteriori informazioni, consulta Come utilizzare un ID esterno nella Guida per l'utente di IAM.
<code>awsAccessKeyId</code>	AWS ID della chiave di accesso che sostituisce le credenziali predefinite. Questa impostazione ha la precedenza su tutti gli altri provider di credenziali.
<code>awsSecretAccessKey</code>	AWS chiave segreta che sostituisce le credenziali predefinite. Questa impostazione ha la precedenza su tutti gli altri provider di credenziali.
<code>cloudwatch.emitMetrics</code>	Consente all'agente di emettere metriche su CloudWatch if set (true).

Impostazione di configurazione	Description
	Impostazione predefinita: true
<code>cloudwatch.endpoint</code>	L'endpoint regionale per CloudWatch Impostazione predefinita: <code>monitoring.us-east-1.amazonaws.com</code>
<code>firehose.endpoint</code>	L'endpoint regionale per Amazon Data Firehose. Impostazione predefinita: <code>firehose.us-east-1.amazonaws.com</code>
<code>sts.endpoint</code>	L'endpoint regionale per il servizio AWS Security Token. Impostazione predefinita: <code>https://sts.amazonaws.com</code>
<code>userDefinedCredentialsProvider.className</code>	Se definisci un fornitore di credenziali personalizzate, specifica il nome completo della classe utilizzando questa impostazione. Non includere <code>.class</code> alla fine del nome della classe.
<code>userDefinedCredentialsProvider.location</code>	Se definisci un fornitore di credenziali personalizzate, utilizza questa impostazione per specificare il percorso assoluto del jar contenente il fornitore di credenziali personalizzate. L'agente cerca anche il file jar nel seguente percorso: <code>/usr/share/aws-kinesis-agent/lib/</code> .

Seguono le impostazioni di configurazione del flusso.

Impostazione di configurazione	Description
<code>aggregateRecordSizeBytes</code>	Per fare in modo che l'agente aggregi i record e poi li inserisca nel flusso Firehose in un'unica operazione, specificate questa impostazione. Impostatelo sulla dimensione che desiderate che il record aggregato abbia prima che l'agente lo inserisca nel flusso Firehose. Predefinito: 0 (nessuna aggregazione)

Impostazione di configurazione	Description
<code>dataProcessingOptions</code>	L'elenco delle opzioni di elaborazione applicate a ciascun record analizzato prima di essere inviato allo stream Firehose. Le opzioni di elaborazione vengono eseguite nell'ordine specificato. Per ulteriori informazioni, consulta Preelabora i dati con gli agenti .
<code>deliveryStream</code>	[Obbligatorio] Il nome dello stream Firehose.
<code>filePattern</code>	<p>[Obbligatorio] Un glob per i file che devono essere monitorati dall'agente. Qualsiasi file che corrisponde a questo modello viene acquisito dall'agente automaticamente e monitorato. Per tutti i file corrispondenti a questo modello, concedere l'autorizzazione in lettura a <code>aws-kinesis-agent-user</code>. Per la directory contenente i file, concedere autorizzazioni in lettura ed esecuzione a <code>aws-kinesis-agent-user</code>.</p> <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Important</p> <p>L'agente raccoglie qualsiasi file che corrisponde a questo modello. Per assicurarsi che l'agente non raccolga record non previsti, scegliere questo modello con attenzione.</p> </div>
<code>initialPosition</code>	<p>La posizione iniziale dalla quale è iniziata l'analisi del file. I valori validi sono <code>START_OF_FILE</code> e <code>END_OF_FILE</code>.</p> <p>Impostazione predefinita: <code>END_OF_FILE</code></p>
<code>maxBufferAgeMillis</code>	<p>Il tempo massimo, in millisecondi, durante il quale l'agente memorizza i dati nel buffer prima di inviarli al flusso Firehose.</p> <p>Intervallo di valori: da 1.000 a 900.000 (da 1 secondo a 15 minuti)</p> <p>Impostazione predefinita: 60.000 (1 minuto)</p>

Impostazione di configurazione	Description
<code>maxBuffer SizeBytes</code>	<p>La dimensione massima, in byte, per la quale l'agente memorizza i dati nel buffer prima di inviarli al flusso Firehose.</p> <p>Intervallo di valori: da 1 a 4.194.304 (4 MB)</p> <p>Impostazione predefinita: 4.194.304 (4 MB)</p>
<code>maxBuffer SizeRecords</code>	<p>Il numero massimo di record per i quali l'agente memorizza i dati nel buffer prima di inviarli allo stream Firehose.</p> <p>Intervallo di valori: da 1 a 500</p> <p>Impostazione predefinita: 500</p>
<code>minTimeBe tweenFile PollsMillis</code>	<p>L'intervallo di tempo, in millisecondi, in cui l'agente esegue il polling e analizza i dati nuovi nei file monitorati.</p> <p>Intervallo valore: 1 o più</p> <p>Impostazione predefinita: 100</p>
<code>multiLine StartPattern</code>	<p>Il modello per identificare l'inizio di un record. Un record è composto da una riga corrispondente al modello e da tutte le righe successive non corrispondenti al modello. I valori validi sono espressioni regolari. Come impostazione predefinita, ogni nuova riga nei file di log viene analizzata come un record.</p>
<code>skipHeaderLines</code>	<p>Il numero di righe necessarie perché l'agente salti l'analisi all'inizio dei file monitorati.</p> <p>Intervallo valore: 0 o più</p> <p>Impostazione predefinita: 0 (zero)</p>

Impostazione di configurazione	Description
<code>truncatedRecordTerminator</code>	La stringa utilizzata dall'agente per troncare un record analizzato quando la dimensione del record supera il limite di dimensione del record di Amazon Data Firehose. (1.000 KB) Impostazione predefinita: <code>'\n'</code> (nuova riga)

Configura più directory e stream di file

Specificando più impostazioni di configurazione del flusso, puoi configurare l'agente in modo che monitori più directory di file e invii dati a più flussi. Nel seguente esempio di configurazione, l'agente monitora due directory di file e invia i dati rispettivamente a un flusso di dati Kinesis e a un flusso Firehose. Puoi specificare diversi endpoint per Kinesis Data Streams e Amazon Data Firehose in modo che il flusso di dati e il flusso Firehose non debbano necessariamente trovarsi nella stessa regione.

```
{
  "cloudwatch.emitMetrics": true,
  "kinesis.endpoint": "https://your/kinesis/endpoint",
  "firehose.endpoint": "https://your/firehose/endpoint",
  "flows": [
    {
      "filePattern": "/tmp/app1.log*",
      "kinesisStream": "yourkinesisstream"
    },
    {
      "filePattern": "/tmp/app2.log*",
      "deliveryStream": "yourfirehosedeliverystream"
    }
  ]
}
```

Per informazioni più dettagliate sull'utilizzo dell'agente con flusso di dati Amazon Kinesis, consulta [Writing to Amazon Kinesis Data Streams with Kinesis Agent](#).

Preelabora i dati con gli agenti

L'agente può preelaborare i record analizzati dai file monitorati prima di inviarli allo stream Firehose. È possibile abilitare questa funzionalità aggiungendo le impostazioni di configurazione `dataProcessingOptions` al flusso di file. Si possono aggiungere una o più opzioni di elaborazione, che verranno eseguite nell'ordine specificato.

L'agente supporta le seguenti opzioni di elaborazione. Poiché l'agente è open source, è possibile sviluppare ulteriormente e ampliare le opzioni di elaborazione. Puoi scaricare l'agente da [Kinesis Agent](#).

Opzioni di elaborazione

SINGLELINE

Converte un record a più righe in un record a riga singola rimuovendo i caratteri di nuova riga, gli spazi iniziali e finali.

```
{
  "optionName": "SINGLELINE"
}
```

CSVTOJSON

Converte un record da un formato delimitatore separato a un formato JSON.

```
{
  "optionName": "CSVTOJSON",
  "customFieldNames": [ "field1", "field2", ... ],
  "delimiter": "yourdelimiter"
}
```

`customFieldNames`

[Obbligatorio] I nomi di campo utilizzati come chiavi in ciascuna coppia chiave-valore JSON. Ad esempio, se specifichi `["f1", "f2"]`, il record `"v1, v2"` viene convertito in `{"f1": "v1", "f2": "v2"}`.

`delimiter`

La stringa utilizzata come delimitatore nel record. L'impostazione predefinita è una virgola (,).

LOGTOJSON

Converte un record da un formato log a un formato JSON. I formati di log supportati sono Apache Common Log, Apache Combined Log, Apache Error Log e RFC3164 Syslog.

```
{
  "optionName": "LOGTOJSON",
  "logFormat": "logformat",
  "matchPattern": "yourregexpattern",
  "customFieldNames": [ "field1", "field2", ... ]
}
```

logFormat

[Obbligatorio] Il formato di inserimento dei log. I seguenti sono i valori possibili:

- COMMONAPACHELOG - Il formato Apache Common Log. Ogni voce di log ha il seguente modello come impostazione predefinita: "%{host} %{ident} %{authuser} [%{datetime}] \"%{request}\" %{response} %{bytes}".
- COMBINEDAPACHELOG: il formato Apache Combined Log. Ogni voce di log ha il seguente modello come impostazione predefinita: "%{host} %{ident} %{authuser} [%{datetime}] \"%{request}\" %{response} %{bytes} %{referrer} %{agent}".
- APACHEERRORLOG: il formato Apache Error Log. Ogni voce di log ha il seguente modello come impostazione predefinita: "[%{timestamp}] [%{module}:%{severity}] [pid %{processid}:tid %{threadid}] [client: %{client}] %{message}".
- SYSLOG— Il formato Syslog. RFC3164 Ogni voce di log ha il seguente modello come impostazione predefinita: "%{timestamp} %{hostname} %{program} [%{processid}]: %{message}".

matchPattern

Ignora il modello predefinito per il formato di log specificato. Utilizza questa impostazione per estrarre valori dalle voci di log se utilizzano un formato personalizzato. Se si specifica `matchPattern`, è necessario specificare anche `customFieldNames`.

customFieldNames

I nomi di campo obbligatori utilizzati come chiavi in ciascuna coppia chiave-valore JSON. Puoi utilizzare questa impostazione per definire i nomi dei campi per i valori estratti da `matchPattern` oppure sovrascrivere i nomi dei campi predefiniti dei formati di log predefiniti.

Example: configurazione LOGTOJSON

Questo è un esempio di una configurazione LOGTOJSON per una voce Apache Common Log convertita in formato JSON:

```
{
  "optionName": "LOGTOJSON",
  "logFormat": "COMMONAPACHELOG"
}
```

Prima della conversione:

```
64.242.88.10 - - [07/Mar/2004:16:10:02 -0800] "GET /mailman/listinfo/hsdivision
HTTP/1.1" 200 6291
```

Dopo la conversione:

```
{"host":"64.242.88.10","ident":null,"authuser":null,"datetime":"07/
Mar/2004:16:10:02 -0800","request":"GET /mailman/listinfo/hsdivision
HTTP/1.1","response":"200","bytes":"6291"}
```

Example: configurazione LOGTOJSON con campi personalizzati

Ecco un altro esempio di configurazione LOGTOJSON:

```
{
  "optionName": "LOGTOJSON",
  "logFormat": "COMMONAPACHELOG",
  "customFieldNames": ["f1", "f2", "f3", "f4", "f5", "f6", "f7"]
}
```

Con questa impostazione di configurazione, la stessa voce Apache Common Log dall'esempio precedente viene convertita in formato JSON come segue:

```
{"f1":"64.242.88.10","f2":null,"f3":null,"f4":"07/Mar/2004:16:10:02 -0800","f5":"GET /
mailman/listinfo/hsdivision HTTP/1.1","f6":"200","f7":"6291"}
```

Example: convertire la voce Apache Common Log

La seguente configurazione di flusso converte una voce Apache Common Log in record a riga singola in formato JSON:

```
{
  "flows": [
    {
      "filePattern": "/tmp/app.log*",
      "deliveryStream": "my-delivery-stream",
      "dataProcessingOptions": [
        {
          "optionName": "LOGTOJSON",
          "logFormat": "COMMONAPACHELOG"
        }
      ]
    }
  ]
}
```

Example: convertire record a più righe

La seguente configurazione del flusso analizza i record a più righe la cui prima riga inizia con "[SEQUENCE=". Ogni record viene convertito in un record a riga singola. Quindi, i valori vengono estratti dal record in base a un delimitatore di schede. I valori estratti sono mappati in valori `customFieldNames` specificati per formare un record a riga singola in formato JSON.

```
{
  "flows": [
    {
      "filePattern": "/tmp/app.log*",
      "deliveryStream": "my-delivery-stream",
      "multilineStartPattern": "\\[SEQUENCE=",
      "dataProcessingOptions": [
        {
          "optionName": "SINGLELINE"
        },
        {
          "optionName": "CSVTOJSON",
          "customFieldNames": [ "field1", "field2", "field3" ],
          "delimiter": "\\t"
        }
      ]
    }
  ]
}
```

Example: configurazione LOGTOJSON con modello corrispondente

Questo è un esempio di una configurazione LOGTOJSON per una voce Apache Common Log convertita in formato JSON, con l'ultimo campo (byte) omesso:

```
{
  "optionName": "LOGTOJSON",
  "logFormat": "COMMONAPACHELOG",
  "matchPattern": "^(\\d\\.\\d\\.\\d) (\\S+) (\\S+) \\[[([\\w:/]+\\s[+\\-]\\d{4})\\] \\\"(.+?)\\\" (\\d{3})",
  "customFieldNames": ["host", "ident", "authuser", "datetime", "request",
    "response"]
}
```

Prima della conversione:

```
123.45.67.89 - - [27/Oct/2000:09:27:09 -0400] "GET /java/javaResources.html HTTP/1.0"
200
```

Dopo la conversione:

```
{"host":"123.45.67.89","ident":null,"authuser":null,"datetime":"27/Oct/2000:09:27:09
-0400","request":"GET /java/javaResources.html HTTP/1.0","response":"200"}
```

Usa i comandi CLI dell'agente comuni

La tabella seguente fornisce una serie di casi d'uso comuni e i comandi corrispondenti per lavorare con l'agente AWS Kinesis.

Caso d'uso	Comando
Avvia automaticamente l'agente all'avvio del sistema	<code>sudo chkconfig aws-kinesis-agent on</code>
Controlla lo stato dell'agente	<code>sudo service aws-kinesis-agent status</code>
Fermate l'agente	<code>sudo service aws-kinesis-agent stop</code>

Caso d'uso	Comando
Leggi il file di registro dell'agente da questa posizione	<code>/var/log/aws-kinesis-agent/aws-kinesis-agent.log</code>
Disinstalla l'agente	<code>sudo yum remove aws-kinesis-agent</code>

Risolvi i problemi relativi all'invio da Kinesis Agent

Questa tabella fornisce informazioni e soluzioni per la risoluzione dei problemi più comuni riscontrati durante l'utilizzo di Amazon Kinesis Agent.

Problema	Soluzione
Perché Kinesis Agent non funziona su Windows?	L'agente Kinesis per Windows è un software diverso dall'agente Kinesis per piattaforme Linux.
Perché l'agente Kinesis rallenta e/o <code>RecordSendErrors</code> aumenta?	<p>Di solito ciò è dovuto alla limitazione di Kinesis. Controlla la <code>WriteProvisionedThroughputExceeded</code> metrica per Kinesis Data Streams o la <code>ThrottledRecords</code> metrica per i flussi Firehose. Qualsiasi aumento rispetto a 0 di questi parametri indica che è necessario aumentare i limiti dei flussi. Per ulteriori informazioni, consulta i limiti di Kinesis Data Stream e i flussi Firehose.</p> <p>Una volta esclusa la limitazione, verifica se Kinesis Agent è configurato in modo da monitorare grandi quantità di file di piccole dimensioni. Si verifica un ritardo nel momento in cui Kinesis Agent esegue il tail di un nuovo file, quindi Kinesis Agent dovrebbe eseguire la coda su una piccola quantità di file più grandi. Prova a consolidare i tuoi file di log in file più grandi.</p>

Problema	Soluzione
Come risolvere le eccezioni <code>? java.lang.OutOfMemoryError</code>	Ciò accade quando Kinesis Agent non dispone di memoria sufficiente per gestire il carico di lavoro corrente. Prova ad aumentare, <code>JAVA_START_HEAP</code> inserire <code>/usr/bin/start-aws-kinesis-agent</code> e <code>JAVA_MAX_HEAP</code> riavviare l'agente.
Come risolvere le eccezioni? <code>IllegalStateException : connection pool shut down</code>	Kinesis Agent non dispone di connessioni sufficienti per gestire il carico di lavoro corrente. Prova ad aumentare <code>maxConnections</code> e <code>maxSendingThreads</code> a inserire le impostazioni generali della configurazione dell'agente su <code>/etc/aws-kinesis/agent.json</code> Il valore predefinito per questi campi è 12 volte superiore ai processori di runtime disponibili. Consulta AgentConfiguration.java per ulteriori informazioni sulle impostazioni avanzate delle configurazioni degli agenti.
Come posso eseguire il debug di un altro problema con Kinesis Agent?	DEBUG log di livello possono essere abilitati in <code>/etc/aws-kinesis/log4j.xml</code>
Come devo configurare Kinesis Agent?	Più piccolo è <code>maxBufferSizeBytes</code> , più frequentemente Kinesis Agent invierà i dati. Ciò può essere utile in quanto riduce i tempi di consegna dei record, ma aumenta anche le richieste al secondo a Kinesis.
Perché Kinesis Agent invia record duplicati?	Ciò si verifica a causa di un'errata configurazione nella coda dei file. Assicurati che ognuno corrisponda <code>fileFlow's filePattern</code> a un solo file. Ciò può verificarsi anche se la <code>logrotate</code> modalità utilizzata è <code>copytruncate</code> attiva. Prova a passare alla modalità predefinita o crea per evitare duplicazioni. Per ulteriori informazioni sulla gestione dei record duplicati, vedere Gestione dei record duplicati .

Inviare dati con AWS SDK

[Puoi utilizzare l'API Amazon Data Firehose per inviare dati a uno stream Firehose utilizzando l'SDK for AWS Java, .NET, Node.js, Python o Ruby.](#) Se non conosci Amazon Data Firehose, prenditi del tempo per acquisire familiarità con i concetti e la terminologia presentati in [Cos'è Amazon Data Firehose?](#) Per ulteriori informazioni, consulta [Come iniziare a usare Amazon Web Services.](#)

Questi esempi non rappresentano codici pronti per la produzione, poiché non eseguono un controllo per tutte le possibili eccezioni o spiegano tutte le possibili considerazioni relative alle prestazioni e alla sicurezza.

L'API Amazon Data Firehose offre due operazioni per l'invio di dati al tuo stream Firehose: e. [PutRecordPutRecordBatch](#) `PutRecord()` invia un record di dati in una chiamata e `PutRecordBatch()` può inviare più record di dati in una sola chiamata.

Operazioni di scrittura singole utilizzando PutRecord

L'inserimento dei dati richiede solo il nome del flusso Firehose e un buffer di byte (<=1000 KB). Poiché Amazon Data Firehose raggruppa più record prima di caricare il file in Amazon S3, potresti voler aggiungere un separatore di record. Per inserire i dati un record alla volta in un flusso Firehose, utilizzate il codice seguente:

```
PutRecordRequest putRecordRequest = new PutRecordRequest();
putRecordRequest.setDeliveryStreamName(deliveryStreamName);

String data = line + "\n";

Record record = new Record().withData(ByteBuffer.wrap(data.getBytes()));
putRecordRequest.setRecord(record);

// Put record into the DeliveryStream
firehoseClient.putRecord(putRecordRequest);
```

Per ulteriori informazioni sul codice, consulta il codice di esempio incluso nell' AWS SDK. Per informazioni sulla sintassi di richiesta e risposta, consultate l'argomento pertinente in [Firehose API Operations](#).

Operazioni di scrittura in batch utilizzando PutRecordBatch

L'inserimento dei dati richiede solo il nome dello stream Firehose e un elenco di record. Poiché Amazon Data Firehose raggruppa più record prima di caricare il file in Amazon S3, potresti voler aggiungere un separatore di record. Per inserire i record di dati in batch in un flusso Firehose, utilizzate il codice seguente:

```
PutRecordBatchRequest putRecordBatchRequest = new PutRecordBatchRequest();
putRecordBatchRequest.setDeliveryStreamName(deliveryStreamName);
putRecordBatchRequest.setRecords(recordList);

// Put Record Batch records. Max No.Of Records we can put in a
// single put record batch request is 500
firehoseClient.putRecordBatch(putRecordBatchRequest);

recordList.clear();
```

Per ulteriori informazioni sul codice, consulta il codice di esempio incluso nell' AWS SDK. Per informazioni sulla sintassi di richiesta e risposta, consultate l'argomento pertinente in [Firehose API Operations](#).

Invia CloudWatch log a Firehose

CloudWatch Gli eventi di registro possono essere inviati a Firehose CloudWatch utilizzando i filtri di abbonamento. Per ulteriori informazioni, consulta [Filtri di abbonamento con Amazon Data Firehose](#).

CloudWatch Gli eventi di registro vengono inviati a Firehose in formato gzip compresso. Se si desidera inviare eventi di registro decompressi alle destinazioni Firehose, è possibile utilizzare la funzionalità di decompressione di Firehose per decomprimere automaticamente i log. CloudWatch

Important

Attualmente, Firehose non supporta l'invio di CloudWatch log alla destinazione di Amazon OpenSearch Service perché Amazon CloudWatch combina più eventi di registro in un unico record Firehose e OpenSearch Amazon Service non può accettare più eventi di registro in un unico record. In alternativa, puoi prendere in considerazione [l'utilizzo del filtro di abbonamento per Amazon OpenSearch Service in CloudWatch Logs](#).

Decomprimi i log CloudWatch

[Se si utilizza Firehose per inviare CloudWatch i log e si desidera inviare dati decompressi alla destinazione del flusso Firehose, utilizzare Firehose Data Format Conversion \(Parquet, ORC\) o il partizionamento dinamico.](#) È necessario abilitare la decompressione per lo stream Firehose.

È possibile abilitare la decompressione utilizzando, o. Console di gestione AWS AWS Command Line Interface AWS SDKs

Note

Se abiliti la funzionalità di decompressione su uno stream, usa quel flusso esclusivamente per i filtri CloudWatch degli abbonamenti Logs e non per i Vided Logs. Se si abilita la funzionalità di decompressione su uno stream utilizzato per importare sia CloudWatch Logs che Vending Logs, l'importazione di Vending Logs in Firehose non riesce. Questa funzione CloudWatch di decompressione è disponibile solo per i log.

Estrai il messaggio dopo la decompressione dei registri CloudWatch

Quando abiliti la decompressione, hai la possibilità di abilitare anche l'estrazione dei messaggi. Quando si utilizza l'estrazione dei messaggi, Firehose filtra tutti i metadati, come owner, loggroup, logstream e altri dai record CloudWatch Logs decompressi e fornisce solo il contenuto all'interno dei campi del messaggio. Se stai inviando dati a una destinazione Splunk, devi attivare l'estrazione dei messaggi affinché Splunk analizzi i dati. Di seguito sono riportati alcuni esempi di output dopo la decompressione con e senza estrazione dei messaggi.

Fig 1: Esempio di output dopo la decompressione senza estrazione del messaggio:

```
{
  "owner": "111111111111",
  "logGroup": "CloudTrail/logs",
  "logStream": "111111111111_CloudTrail/logs_us-east-1",
  "subscriptionFilters": [
    "Destination"
  ],
  "messageType": "DATA_MESSAGE",
  "logEvents": [
    {
      "id": "31953106606966983378809025079804211143289615424298221568",
```

```

"timestamp": 1432826855000,
"message": "{\"eventVersion\":\"1.03\", \"userIdentity\":{\"type\":\"Root1\"}}",
},
{
"timestamp": 1432826855000,
"message": "{\"eventVersion\":\"1.03\", \"userIdentity\":{\"type\":\"Root2\"}}",
},
{
"timestamp": 1432826855000,
"message": "{\"eventVersion\":\"1.03\", \"userIdentity\":{\"type\":\"Root3\"}}",
}
]
}

```

Fig 2: Esempio di output dopo la decompressione con estrazione del messaggio:

```

{"eventVersion":"1.03", "userIdentity":{"type":"Root1"}}
{"eventVersion":"1.03", "userIdentity":{"type":"Root2"}}
{"eventVersion":"1.03", "userIdentity":{"type":"Root3"}}

```

Abilitare la decompressione su un nuovo stream Firehose dalla console

Per abilitare la decompressione su un nuovo flusso Firehose utilizzando il Console di gestione AWS

1. [Accedi Console di gestione AWS e apri la console Kinesis all'indirizzo https://console.aws.amazon.com /kinesis.](https://console.aws.amazon.com/kinesis)
2. Scegli Amazon Data Firehose nel pannello di navigazione.
3. Scegli Crea un flusso Firehose.
4. In Scegli origine e destinazione

Origine

La fonte del tuo stream Firehose. Scegli una delle seguenti fonti:

- Direct PUT: scegliete questa opzione per creare uno stream Firehose su cui le applicazioni di produzione scrivono direttamente. Per un elenco di AWS servizi e agenti e servizi open source integrati con Direct PUT in Firehose, consulta [questa](#) sezione.
- Kinesis stream: scegliete questa opzione per configurare un flusso Firehose che utilizza un flusso di dati Kinesis come origine dati. È quindi possibile utilizzare Firehose per leggere

facilmente i dati da un flusso di dati Kinesis esistente e caricarli nelle destinazioni. Per ulteriori informazioni, consulta [Scrittura su Firehose con Kinesis Data Streams](#)

Destinazione

La destinazione del tuo stream Firehose. Seleziona una delle seguenti opzioni:

- Simple Storage Service (Amazon S3)
- Splunk

5. In Firehose stream name, inserisci un nome per lo stream.
6. (Facoltativo) In Transform records:
 - Nella sezione Decomprimi i record di origine da Amazon CloudWatch Logs, scegli Attiva la decompressione.
 - Se desideri utilizzare l'estrazione dei messaggi dopo la decompressione, scegli Attiva l'estrazione dei messaggi.

Abilitare la decompressione su un flusso Firehose esistente

Questa sezione fornisce istruzioni per abilitare la decompressione sui flussi Firehose esistenti. Copre due scenari: flussi con elaborazione Lambda disabilitata e flussi con elaborazione Lambda già abilitata. Le seguenti sezioni descrivono step-by-step le procedure per ogni caso, tra cui la creazione o la modifica di funzioni Lambda, l'aggiornamento delle impostazioni di Firehose e le metriche di CloudWatch monitoraggio per garantire una corretta implementazione della funzionalità di decompressione integrata Firehose.

Abilitazione della decompressione quando l'elaborazione Lambda è disabilitata

Per abilitare la decompressione su un flusso Firehose esistente con l'elaborazione Lambda disabilitata, è necessario prima abilitare l'elaborazione Lambda. Questa condizione è valida solo per gli stream esistenti. I passaggi seguenti mostrano come abilitare la decompressione su flussi esistenti che non hanno l'elaborazione Lambda abilitata.

1. Creazione di una funzione Lambda. È possibile creare un passthrough di record fittizio o utilizzare questo [blueprint](#) per creare una nuova funzione Lambda.
2. Aggiorna lo stream Firehose corrente per abilitare l'elaborazione Lambda e usa la funzione Lambda che hai creato per l'elaborazione.

3. Dopo aver aggiornato lo stream con la nuova funzione Lambda, torna alla console Firehose e attiva la decompressione.
4. Disabilita l'elaborazione Lambda abilitata nel passaggio 1. Ora puoi eliminare la funzione che hai creato nel passaggio 1.

Abilitazione della decompressione quando l'elaborazione Lambda è abilitata

Se disponi già di uno stream Firehose con una funzione Lambda, per eseguire la decompressione puoi sostituirlo con la funzionalità di decompressione Firehose. Prima di procedere, esamina il codice della funzione Lambda per confermare che esegua solo la decompressione o l'estrazione dei messaggi. L'output della funzione Lambda dovrebbe essere simile agli esempi mostrati in [Fig 1](#) o [Fig 2](#). Se l'output è simile, puoi sostituire la funzione Lambda utilizzando i passaggi seguenti.

1. [Sostituisci la tua attuale funzione Lambda con questo modello](#). La nuova funzione Lambda Blueprint rileva automaticamente se i dati in entrata sono compressi o decompressi. Eseguendo la decompressione solo se i dati di input sono compressi.
2. Attiva la decompressione utilizzando l'opzione Firehose integrata per la decompressione.
3. Abilita le CloudWatch metriche per il tuo stream Firehose se non è già abilitato. Monitora la metrica `CloudWatchProcessorLambda_IncomingCompressedData` e attendi che questa metrica diventi zero. Ciò conferma che tutti i dati di input inviati alla funzione Lambda sono decompressi e che la funzione Lambda non è più necessaria.
4. Rimuovi la trasformazione dei dati Lambda perché non ti serve più per decomprimere lo stream.

Disattiva la decompressione sullo stream Firehose

Per disabilitare la decompressione su un flusso di dati utilizzando il Console di gestione AWS

1. [Accedi Console di gestione AWS e apri la console Kinesis all'indirizzo https://console.aws.amazon.com/kinesis](https://console.aws.amazon.com/kinesis).
2. Scegli Amazon Data Firehose nel pannello di navigazione.
3. Scegli lo stream Firehose che desideri modificare.
4. Nella pagina dei dettagli dello stream Firehose, selezionare la scheda Configurazione.
5. Nella sezione Trasforma e converti i record, scegli Modifica.

6. In Decomprimi i record di origine da Amazon CloudWatch Logs, deseleziona Attiva la decompressione, quindi scegli Salva modifiche.

Risoluzione dei problemi di decompressione in Firehose

La tabella seguente mostra come Firehose gestisce gli errori durante la decompressione e l'elaborazione dei dati, tra cui l'invio di record a un bucket S3 con errori, la registrazione degli errori e l'emissione di metriche. Spiega inoltre il messaggio di errore restituito per le operazioni di immissione di dati non autorizzate.

Problema	Soluzione
Cosa succede ai dati di origine in caso di errore durante la decompressione?	Se Amazon Data Firehose non è in grado di decomprimere il record, il record viene consegnato così com'è (in formato compresso) al bucket di errore S3 specificato durante la creazione dello stream Firehose. Oltre al record, l'oggetto consegnato include anche il codice di errore e il messaggio di errore e questi oggetti verranno recapitati a un prefisso del bucket S3 chiamato <code>decompression-failed</code> . Firehose continuerà a elaborare altri record dopo una decompressione non riuscita di un record.
Cosa succede ai dati di origine in caso di errore nella pipeline di elaborazione dopo una decompressione riuscita?	Se Amazon Data Firehose presenta errori nelle fasi di elaborazione dopo la decompressione, ad esempio il partizionamento dinamico e la conversione del formato dei dati, il record viene fornito in formato compresso nel bucket di errore S3 specificato durante la creazione dello stream Firehose. Oltre al record, l'oggetto consegnato include anche il codice di errore e il messaggio di errore.
Come siete informati in caso di errore o eccezione?	In caso di errore o eccezione durante la decompressione, se si configurano i log, Firehose registrerà i messaggi di errore in CloudWatch Logs. CloudWatch Inoltre, Firehose invia metriche a CloudWatch metriche che è possibile monitorare. Facoltativamente, puoi anche creare allarmi in base alle metriche emesse da Firehose.

Problema	Soluzione
Cosa succede quando put le operazioni non provengono dai log? CloudWatch	Quando il cliente puts non proviene da CloudWatch Logs, viene restituito il seguente messaggio di errore: <pre>Put to Firehose failed for AccountId: <accountID>, FirehoseName: <firehosename> because the request is not originating from allowed source types.</pre>
Quali metriche emette Firehose per la funzione di decompressione?	Firehose emette metriche per la decompressione di ogni record. È necessario selezionare il periodo (1 minuto), la statistica (somma) e l'intervallo di date per ottenere il numero di risultati non riusciti o <code>DecompressedRecords</code> riusciti o non riusciti. <code>DecompressedBytes</code> Per ulteriori informazioni, consulta CloudWatch Registra le metriche di decompressione .

Invia CloudWatch eventi a Firehose

Puoi configurare Amazon CloudWatch per inviare eventi a uno stream Firehose aggiungendo una destinazione a una regola CloudWatch Events.

Per creare una destinazione per una regola CloudWatch Events che invia eventi a un flusso Firehose esistente

1. Accedi a Console di gestione AWS e apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Scegli Crea regola.
3. Nella pagina Passaggio 1: creazione della regola, per Target, selezionare Aggiungi destinazione, quindi scegliere Firehose stream.
4. Scegliete uno stream Firehose esistente.

Per ulteriori informazioni sulla creazione di regole per CloudWatch gli eventi, consulta [Getting Started with Amazon CloudWatch Events](#).

AWS IoT Configurare l'invio di dati a Firehose

È possibile configurare AWS IoT l'invio di informazioni a uno stream Firehose aggiungendo un'azione.

Per creare un'azione che invii eventi a un flusso Firehose esistente

1. Quando crei una regola nella AWS IoT console, nella pagina Crea una regola, in Imposta una o più azioni, scegli Aggiungi azione.
2. Scegli Invia messaggi a un flusso Amazon Kinesis Firehose.
3. Selezionare Configure action (Configura operazione).
4. Per Stream name, scegliete uno stream Firehose esistente.
5. Per Separator (Separatore), selezionare un carattere del separatore da inserire tra i record.
6. Per Nome ruolo IAM, scegli un ruolo IAM esistente oppure scegli Crea un nuovo ruolo.
7. Selezionare Add action (Aggiungi operazione).

Per ulteriori informazioni sulla creazione di AWS IoT regole, consulta [AWS IoT Rule Tutorials](#).

Trasforma i dati di origine in Amazon Data Firehose

Amazon Data Firehose può richiamare la funzione Lambda per trasformare i dati di origine in entrata e consegnarli alle destinazioni. Puoi abilitare la trasformazione dei dati di Amazon Data Firehose quando crei il tuo stream Firehose.

Comprendi il flusso di trasformazione dei dati

Quando si abilita la trasformazione dei dati Firehose, Firehose memorizza nel buffer i dati in entrata. Il suggerimento sulla dimensione del buffering varia tra 0,2 MB e 3 MB. Il suggerimento predefinito sulla dimensione del buffering Lambda è 1 MB per tutte le destinazioni, tranne Splunk e Snowflake. Per Splunk e Snowflake, l'hint di buffering predefinito è 256 KB. Il suggerimento sull'intervallo di buffering Lambda è compreso tra 0 e 900 secondi. Il suggerimento predefinito per l'intervallo di buffering Lambda è di sessanta secondi per tutte le destinazioni tranne Snowflake. Per Snowflake, l'intervallo di suggerimento di buffering predefinito è di 30 secondi. Per regolare la dimensione del buffering, imposta il [ProcessingConfiguration](#) parametro dell'API [CreateDeliveryStream](#) o [UpdateDestination](#) con il comando chiamato `and. ProcessorParameter BufferSizeInMBs IntervalInSeconds` Firehose richiama quindi la funzione Lambda specificata in modo sincrono con ogni batch bufferizzato utilizzando la modalità di chiamata sincrona. AWS Lambda I dati trasformati vengono inviati da Lambda a Firehose. Firehose lo invia quindi alla destinazione quando viene raggiunta la dimensione o l'intervallo di buffering di destinazione specificati, a seconda dell'evento che si verifica per primo.

Important

La modalità di invocazione sincrona di Lambda ha un limite di dimensione del payload di 6 MB sia per la richiesta che per la risposta. Verifica che la dimensione del buffer per l'invio della richiesta alla funzione sia minore o uguale a 6 MB. Verifica anche che la risposta restituita dalla funzione non superi i 6 MB.

Durata della chiamata Lambda

Amazon Data Firehose supporta un tempo di chiamata Lambda fino a 5 minuti. Se la funzione Lambda impiega più di 5 minuti per essere completata, viene visualizzato il seguente errore: Firehose ha riscontrato errori di timeout durante la chiamata a Lambda. AWS Il timeout massimo della funzione supportato è di 5 minuti.

Per informazioni su cosa fa Amazon Data Firehose se si verifica un errore di questo tipo, consulta [the section called “Gestisci gli errori nella trasformazione dei dati”](#)

Parametri richiesti per la trasformazione dei dati

Tutti i record trasformati da Lambda devono contenere i seguenti parametri, altrimenti Amazon Data Firehose li rifiuta e li considera un errore di trasformazione dei dati.

For Kinesis Data Streams and Direct PUT

I seguenti parametri sono necessari per tutti i record trasformati da Lambda.

- `recordId`— L'ID del record viene passato da Amazon Data Firehose a Lambda durante la chiamata. Il record trasformato deve contenere lo stesso ID record. Ogni mancata corrispondenza tra l'ID del record originale e l'ID del record trasformato viene trattato come un errore di trasformazione dei dati.
- `result`— Lo stato della trasformazione dei dati del record. I valori possibili sono: `Ok` (il record è stato trasformato correttamente), `Dropped` (il record è stato rimosso intenzionalmente dalla logica di elaborazione) e `ProcessingFailed` (non è stato possibile trasformare il record). Se un record ha lo stato di `Ok` o `Dropped`, Amazon Data Firehose lo considera elaborato correttamente. In caso contrario, Amazon Data Firehose lo considera elaborato senza successo.
- `data`— Il payload dei dati trasformato, dopo la codifica in base64.

Di seguito è riportato un esempio di risultato Lambda:

```
{
  "recordId": "<recordId from the Lambda input>",
  "result": "Ok",
  "data": "<Base64 encoded Transformed data>"
}
```

For Amazon MSK

I seguenti parametri sono necessari per tutti i record trasformati da Lambda.

- `recordId`— L'ID del record viene passato da Firehose a Lambda durante la chiamata. Il record trasformato deve contenere lo stesso ID record. Ogni mancata corrispondenza tra l'ID del

record originale e l'ID del record trasformato viene trattato come un errore di trasformazione dei dati.

- `result`— Lo stato della trasformazione dei dati del record. I valori possibili sono: `Ok` (il record è stato trasformato correttamente), `Dropped` (il record è stato rimosso intenzionalmente dalla logica di elaborazione) e `ProcessingFailed` (non è stato possibile trasformare il record). Se un record ha lo stato `Ok` o `Dropped`, Firehose lo considera elaborato correttamente. In caso contrario, Firehose lo considera elaborato senza successo.
- `KafkaRecordValue`— Il payload dei dati trasformato, dopo la codifica in base64.

Di seguito è riportato un esempio di risultato Lambda:

```
{
  "recordId": "<recordId from the Lambda input>",
  "result": "Ok",
  "kafkaRecordValue": "<Base64 encoded Transformed data>"
}
```

Blueprint Lambda supportati

Questi blueprint dimostrano come è possibile creare e utilizzare funzioni AWS Lambda per trasformare i dati nei flussi di dati di Amazon Data Firehose.

Per vedere i blueprint disponibili nella console AWS Lambda

1. Accedi a Console di gestione AWS e apri la AWS Lambda console all'indirizzo <https://console.aws.amazon.com/lambda/>.
2. Scegliere Create function (Crea funzione), quindi scegliere Use a blueprint (Usa un piano).
3. Nel campo Blueprints, cerca la parola chiave per `firehose` trovare i blueprint Amazon Data Firehose Lambda.

Elenco degli schemi:

- Record di processo inviati allo stream Amazon Data Firehose (Node.js, Python)

Questo modello mostra un esempio di base di come elaborare i dati nel flusso di dati di Firehose utilizzando AWS Lambda.

Ultima data di rilascio: novembre 2016.

Note di rilascio: nessuna.

- CloudWatch Registri dei processi inviati a Firehose

Questo blueprint è obsoleto. Non utilizzare questo blueprint. Potrebbe comportare costi elevati quando i dati dei CloudWatch registri decompressi superano i 6 MB (limite Lambda). Per informazioni sull'elaborazione dei CloudWatch log inviati a Firehose, [vedere Writing to Firehose Using Logs](#). CloudWatch

- Convertire i record di flusso di Amazon Data Firehose in formato syslog in JSON (Node.js)

Questo modello mostra come convertire i record di input in formato Syslog in RFC3164 JSON.

Ultima data di rilascio: novembre 2016.

Note di rilascio: nessuna.

Per visualizzare i progetti disponibili in AWS Serverless Application Repository

1. Passa a [AWS Serverless Application Repository](#).
2. Scegli Sfoglia tutte le applicazioni.
3. Nel campo Applications (Applicazioni), cercare la parola chiave `firehose`.

Puoi inoltre creare una funzione Lambda senza utilizzare uno schema. Vedi [Guida introduttiva a AWS Lambda](#).

Gestisci gli errori nella trasformazione dei dati

Se la chiamata della funzione Lambda non riesce a causa di un timeout di rete o perché hai raggiunto il limite di invocazione Lambda, Amazon Data Firehose ritenta la chiamata tre volte per impostazione predefinita. Se la chiamata non riesce, Amazon Data Firehose salta quel batch di record. I record ignorati vengono considerati record con errori di elaborazione. Puoi specificare o sovrascrivere le opzioni di riprova utilizzando l'API or. [CreateDeliveryStreamUpdateDestination](#) Per questo tipo di errore, puoi registrare gli errori di chiamata su Amazon CloudWatch Logs. Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose utilizzando i log CloudWatch](#).

Se lo stato della trasformazione dei dati di un record è `ProcessingFailed`, Amazon Data Firehose considera il record come se fosse stato elaborato senza successo. Per questo tipo di errore, puoi inviare log di errore ad Amazon CloudWatch Logs dalla tua funzione Lambda. Per ulteriori informazioni, consulta [Accedere ad Amazon CloudWatch Logs AWS Lambda](#) nella AWS Lambda Developer Guide.

Se una trasformazione dei dati fallisce, i record elaborati senza successo vengono inviati al bucket S3 all'interno della cartella `processing-failed`. I record hanno il formato seguente:

```
{
  "attemptsMade": "count",
  "arrivalTimestamp": "timestamp",
  "errorCode": "code",
  "errorMessage": "message",
  "attemptEndingTimestamp": "timestamp",
  "rawData": "data",
  "lambdaArn": "arn"
}
```

`attemptsMade`

Il numero di richieste di invocazioni tentate.

`arrivalTimestamp`

L'ora in cui il record è stato ricevuto da Amazon Data Firehose.

`errorCode`

Il codice di errore HTTP restituito da Lambda.

`errorMessage`

Il messaggio di errore restituito da Lambda.

`attemptEndingTimestamp`

L'ora in cui Amazon Data Firehose ha smesso di tentare le chiamate Lambda.

`rawData`

I dati dei record codificati con base 64.

`lambdaArn`

Il nome della risorsa Amazon (ARN) della funzione Lambda.

Esegui il backup dei record di origine

Amazon Data Firehose è in grado di eseguire contemporaneamente il backup di tutti i record non trasformati nel bucket S3, consegnando i record trasformati alla destinazione. È possibile abilitare il backup dei record di origine quando si crea o si aggiorna lo stream Firehose. Non puoi disabilitare il backup dei record di origine dopo averlo abilitato.

Partizione dei dati di streaming in Amazon Data Firehose

Il partizionamento dinamico consente di partizionare continuamente i dati in streaming in Firehose utilizzando chiavi all'interno dei dati (ad esempio, `customer_id` o `transaction_id`) e quindi fornire i dati raggruppati da queste chiavi nei prefissi Amazon Simple Storage Service (Amazon S3) corrispondenti. Ciò semplifica l'esecuzione di analisi ad alte prestazioni ed economiche sui dati in streaming in Amazon S3 utilizzando vari servizi come Amazon Athena, Amazon EMR, Amazon Redshift Spectrum e Amazon. QuickSight Inoltre, AWS Glue può eseguire lavori di estrazione, trasformazione e caricamento (ETL) più sofisticati dopo che i dati di streaming partizionati dinamicamente sono stati consegnati ad Amazon S3, in casi d'uso in cui è richiesta un'ulteriore elaborazione.

Il partizionamento dei dati riduce al minimo la quantità di dati scansionati, ottimizza le prestazioni e riduce i costi delle query di analisi su Amazon S3. Inoltre, aumenta l'accesso granulare ai dati. I flussi Firehose vengono tradizionalmente utilizzati per acquisire e caricare dati in Amazon S3. Per partizionare un set di dati in streaming per l'analisi basata su Amazon S3, è necessario eseguire il partizionamento di applicazioni tra i bucket Amazon S3 prima di rendere i dati disponibili per l'analisi, operazione che potrebbe diventare complicata o costosa.

Con il partizionamento dinamico, Firehose raggruppa continuamente i dati in transito utilizzando chiavi dati definite dinamicamente o staticamente e fornisce i dati ai singoli prefissi Amazon S3 per chiave. `time-to-insight` Ciò si riduce di minuti o ore. Inoltre, riduce i costi e semplifica le architetture.

Argomenti

- [Abilita il partizionamento dinamico in Amazon Data Firehose](#)
- [Comprendi le chiavi di partizionamento](#)
- [Usa il prefisso del bucket Amazon S3 per fornire dati](#)
- [Applica il partizionamento dinamico ai dati aggregati](#)
- [Risolvi gli errori di partizionamento dinamico](#)
- [Dati buffer per il partizionamento dinamico](#)

Abilita il partizionamento dinamico in Amazon Data Firehose

Puoi configurare il partizionamento dinamico per i tuoi stream Firehose tramite la Console di gestione Amazon Data Firehose, la CLI o il. APIs

⚠ Important

È possibile abilitare il partizionamento dinamico solo quando si crea un nuovo flusso Firehose. Non è possibile abilitare il partizionamento dinamico per un flusso Firehose esistente per il quale il partizionamento dinamico non è già abilitato.

Per i passaggi dettagliati su come abilitare e configurare il partizionamento dinamico tramite la console di gestione Firehose durante la creazione di un nuovo flusso Firehose, consulta [Creazione di un flusso Amazon Firehose](#). Quando devi specificare la destinazione per il tuo stream Firehose, assicurati di seguire i passaggi indicati nella [Configurare le impostazioni di destinazione](#) sezione, poiché attualmente il partizionamento dinamico è supportato solo per i flussi Firehose che utilizzano Amazon S3 come destinazione.

Una volta abilitato il partizionamento dinamico su un flusso Firehose attivo, è possibile aggiornare la configurazione aggiungendo nuove chiavi di partizionamento o rimuovendo o aggiornando quelle esistenti e le espressioni del prefisso S3. Una volta aggiornato, Firehose inizia a utilizzare le nuove chiavi e le nuove espressioni del prefisso S3.

⚠ Important

Una volta abilitato il partizionamento dinamico su un flusso Firehose, non può essere disabilitato su questo flusso Firehose.

Comprendi le chiavi di partizionamento

Con il partizionamento dinamico, crei set di dati mirati dai dati S3 in streaming partizionandoli in base alle chiavi di partizionamento. Le chiavi di partizionamento consentono di filtrare i dati in streaming in base a valori specifici. Ad esempio, se è necessario filtrare i dati in base all'ID cliente e al paese, è possibile specificare il campo dati `customer_id` come una chiave di partizionamento e il campo dati `country` come un'altra chiave di partizionamento. Quindi, specificare le espressioni (utilizzando i formati supportati) per definire i prefissi dei bucket S3 a cui devono essere distribuiti i record di dati partizionati in modo dinamico.

È possibile creare chiavi di partizionamento con i seguenti metodi.

- **Analisi in linea:** questo metodo utilizza il meccanismo di supporto integrato di Firehose, un [parser jq](#), per estrarre le chiavi per il partizionamento dai record di dati in formato JSON. Al jq 1.6 momento, supportiamo solo la versione.
- **AWS Funzione Lambda:** questo metodo utilizza una AWS Lambda funzione specificata per estrarre e restituire i campi di dati necessari per il partizionamento.

⚠ Important

Quando abiliti il partizionamento dinamico, devi configurare almeno uno di questi metodi per partizionare i dati. Puoi configurare uno di questi metodi per specificare le chiavi di partizionamento o entrambi contemporaneamente.

Crea chiavi di partizionamento con analisi in linea

Per configurare l'analisi in linea come metodo di partizionamento dinamico per i dati di streaming, è necessario scegliere i parametri del record di dati da utilizzare come chiavi di partizionamento e fornire un valore per ogni chiave di partizionamento specificata.

Il seguente record di dati di esempio mostra come definire le relative chiavi di partizionamento con l'analisi in linea. Nota che i dati devono essere codificati nel formato Base64. Puoi anche fare riferimento all'esempio [CLI](#).

```
{
  "type": {
    "device": "mobile",
    "event": "user_clicked_submit_button"
  },
  "customer_id": "1234567890",
  "event_timestamp": 1565382027,    #epoch timestamp
  "region": "sample_region"
}
```

Ad esempio, puoi scegliere di partizionare i dati in base al parametro `customer_id` o al parametro `event_timestamp`. Ciò significa che desideri che il valore del parametro `customer_id` o del parametro `event_timestamp` in ogni record venga utilizzato per determinare il prefisso S3 a cui deve essere distribuito il record. Puoi anche scegliere un parametro nidificato, ad esempio `device`

con un'espressione `.type.device`. La logica di partizionamento dinamico può dipendere da più parametri.

Dopo aver selezionato i parametri dei dati per le chiavi di partizionamento, mappa ogni parametro a un'espressione jq valida. La tabella seguente mostra una tale mappatura dei parametri alle espressioni jq:

Parametro	espressione jq
<code>customer_id</code>	<code>.customer_id</code>
<code>device</code>	<code>.type.device</code>
<code>year</code>	<code>.event_timestamp strftime("%Y")</code>
<code>month</code>	<code>.event_timestamp strftime("%m")</code>
<code>day</code>	<code>.event_timestamp strftime("%d")</code>
<code>hour</code>	<code>.event_timestamp strftime("%H")</code>

In fase di esecuzione, Firehose utilizza la colonna destra in alto per valutare i parametri in base ai dati di ogni record.

Crea chiavi di partizionamento con una funzione AWS Lambda

Per i record di dati compressi o crittografati o i dati in qualsiasi formato di file diverso da JSON, puoi utilizzare la AWS Lambda funzione integrata con il tuo codice personalizzato per decomprimere, decrittografare o trasformare i record al fine di estrarre e restituire i campi di dati necessari per il partizionamento. Si tratta di un'espansione della funzione di trasformazione Lambda esistente oggi disponibile con Firehose. Puoi quindi trasformare, analizzare e restituire i campi di dati da utilizzare quindi per il partizionamento dinamico usando la stessa funzione Lambda.

Di seguito è riportato un esempio di funzione Lambda di elaborazione del flusso Firehose in Python che riproduce ogni record letto dall'input all'output ed estrae le chiavi di partizionamento dai record.

```
from __future__ import print_function
import base64
import json
```

```
import datetime

# Signature for all Lambda functions that user must implement
def lambda_handler(firehose_records_input, context):
    print("Received records for processing from DeliveryStream: " +
        firehose_records_input['deliveryStreamArn']
        + ", Region: " + firehose_records_input['region']
        + ", and InvocationId: " + firehose_records_input['invocationId'])

    # Create return value.
    firehose_records_output = {'records': []}

    # Create result object.
    # Go through records and process them

    for firehose_record_input in firehose_records_input['records']:
        # Get user payload
        payload = base64.b64decode(firehose_record_input['data'])
        json_value = json.loads(payload)

        print("Record that was received")
        print(json_value)
        print("\n")
        # Create output Firehose record and add modified payload and record ID to it.
        firehose_record_output = {}
        event_timestamp = datetime.datetime.fromtimestamp(json_value['eventTimestamp'])
        partition_keys = {"customerId": json_value['customerId'],
            "year": event_timestamp.strftime('%Y'),
            "month": event_timestamp.strftime('%m'),
            "day": event_timestamp.strftime('%d'),
            "hour": event_timestamp.strftime('%H'),
            "minute": event_timestamp.strftime('%M')}
        }

        # Create output Firehose record and add modified payload and record ID to it.
        firehose_record_output = {'recordId': firehose_record_input['recordId'],
            'data': firehose_record_input['data'],
            'result': 'Ok',
            'metadata': { 'partitionKeys': partition_keys }}

        # Must set proper record ID
        # Add the record to the list of output records.

        firehose_records_output['records'].append(firehose_record_output)
```

```
# At the end return processed records
return firehose_records_output
```

Di seguito è riportato un esempio di funzione Lambda di elaborazione del flusso Firehose in Go che riproduce ogni record letto dall'input all'output ed estrae le chiavi di partizionamento dai record.

```
package main

import (
    "fmt"
    "encoding/json"
    "time"
    "strconv"

    "github.com/aws/aws-lambda-go/events"
    "github.com/aws/aws-lambda-go/lambda"
)

type DataFirehoseEventRecordData struct {
    CustomerId string `json:"customerId"`
}

func handleRequest(evnt events.DataFirehoseEvent) (events.DataFirehoseResponse, error) {
    {
        fmt.Printf("InvocationID: %s\n", evnt.InvocationID)
        fmt.Printf("DeliveryStreamArn: %s\n", evnt.DeliveryStreamArn)
        fmt.Printf("Region: %s\n", evnt.Region)

        var response events.DataFirehoseResponse

        for _, record := range evnt.Records {
            fmt.Printf("RecordID: %s\n", record.RecordID)
            fmt.Printf("ApproximateArrivalTimestamp: %s\n", record.ApproximateArrivalTimestamp)

            var transformedRecord events.DataFirehoseResponseRecord
            transformedRecord.RecordID = record.RecordID
            transformedRecord.Result = events.DataFirehoseTransformedStateOk
            transformedRecord.Data = record.Data

            var metaData events.DataFirehoseResponseRecordMetadata
```

```
var recordData DataFirehoseEventRecordData
partitionKeys := make(map[string]string)

currentTime := time.Now()
json.Unmarshal(record.Data, &recordData)
partitionKeys["customerId"] = recordData.CustomerId
partitionKeys["year"] = strconv.Itoa(currentTime.Year())
partitionKeys["month"] = strconv.Itoa(int(currentTime.Month()))
partitionKeys["date"] = strconv.Itoa(currentTime.Day())
partitionKeys["hour"] = strconv.Itoa(currentTime.Hour())
partitionKeys["minute"] = strconv.Itoa(currentTime.Minute())
metaData.PartitionKeys = partitionKeys
transformedRecord.Metadata = metaData

response.Records = append(response.Records, transformedRecord)
}

return response, nil
}

func main() {
    lambda.Start(handleRequest)
}
```

Usa il prefisso del bucket Amazon S3 per fornire dati

Quando crei uno stream Firehose che utilizza Amazon S3 come destinazione, devi specificare un bucket Amazon S3 a cui Firehose deve fornire i tuoi dati. I prefissi del bucket Amazon S3 vengono utilizzati per organizzare i dati archiviati nei bucket Amazon S3. Un prefisso del bucket Amazon S3 è simile a una directory che consente di raggruppare oggetti simili.

Con il partizionamento dinamico, i dati partizionati vengono distribuiti nei prefissi Amazon S3 specificati. Se non abiliti il partizionamento dinamico, è facoltativo specificare un prefisso del bucket S3 per il flusso Firehose. Tuttavia, se si sceglie di abilitare il partizionamento dinamico, è necessario specificare i prefissi dei bucket S3 a cui Firehose fornisce i dati partizionati.

In ogni flusso Firehose in cui è abilitato il partizionamento dinamico, il valore del prefisso del bucket S3 è costituito da espressioni basate sulle chiavi di partizionamento specificate per quel flusso Firehose. Utilizzando nuovamente l'esempio di record di dati precedente, puoi creare il seguente valore di prefisso S3 che consiste in espressioni basate sulle chiavi di partizionamento definite sopra:

```
"ExtendedS3DestinationConfiguration": {  
  "BucketARN": "arn:aws:s3:::my-logs-prod",  
  "Prefix": "customer_id={!partitionKeyFromQuery:customer_id}/  
    device={!partitionKeyFromQuery:device}/  
    year={!partitionKeyFromQuery:year}/  
    month={!partitionKeyFromQuery:month}/  
    day={!partitionKeyFromQuery:day}/  
    hour={!partitionKeyFromQuery:hour}/"  
}
```

Firehose valuta l'espressione precedente in fase di esecuzione. Raggruppa i record che corrispondono alla stessa espressione di prefisso S3 valutata in un unico set di dati. Firehose invia quindi ogni set di dati al prefisso S3 valutato. La frequenza di consegna del set di dati a S3 è determinata dall'impostazione del buffer di flusso Firehose. Di conseguenza, il record in questo esempio viene distribuito alla seguente chiave oggetto S3:

```
s3://my-logs-prod/customer_id=1234567890/device=mobile/year=2019/month=08/day=09/  
hour=20/my-delivery-stream-2019-08-09-23-55-09-a9fa96af-e4e4-409f-bac3-1f804714faaa
```

Per il partizionamento dinamico, è necessario utilizzare il seguente formato di espressione nel prefisso del bucket S3: `!{namespace:value}`, dove lo spazio dei nomi può essere `partitionKeyFromQuery`, `partitionKeyFromLambda` o entrambi. Se si utilizza l'analisi in linea per creare le chiavi di partizionamento per i dati di origine, è necessario specificare un valore del prefisso del bucket S3 costituito da espressioni specificate nel seguente formato: `"partitionKeyFromQuery:keyID"`. Se si utilizza una funzione AWS Lambda per creare chiavi di partizionamento per i dati di origine, è necessario specificare un valore di prefisso del bucket S3 costituito da espressioni specificate nel seguente formato: `"partitionKeyFromLambda:keyID"`.

Note

È inoltre possibile specificare il valore del prefisso del bucket S3 utilizzando il formato in stile hive, ad esempio `customer_id=! partitionKeyFrom{query:customer_id}`.

Per ulteriori informazioni, consulta «Scegli Amazon S3 per la tua destinazione» in [Creazione di uno stream Amazon Firehose](#) e [prefissi personalizzati per oggetti Amazon S3](#).

Aggiungi un nuovo delimitatore di riga durante la distribuzione di dati ad Amazon S3

Puoi abilitare New Line Delimiter per aggiungere un nuovo delimitatore di riga tra i record negli oggetti che vengono consegnati ad Amazon S3. Ciò può essere utile per analizzare gli oggetti in Amazon S3. Ciò è particolarmente utile anche quando il partizionamento dinamico viene applicato a dati aggregati, poiché la deaggregazione multi-record (che deve essere applicata ai dati aggregati prima di poter essere partizionati dinamicamente) rimuove nuove righe dai record come parte del processo di analisi.

Applica il partizionamento dinamico ai dati aggregati

È possibile applicare il partizionamento dinamico ai dati aggregati (ad esempio, più eventi, log o record aggregati in un'unica chiamata API PutRecord e PutRecordBatch), ma questi dati devono prima essere disaggregati. È possibile disaggregare i dati abilitando la deaggregazione di più record, il processo di analisi dei record nel flusso Firehose e la loro separazione.

La disaggregazione di più record può essere di JSON tipo diverso, il che significa che la separazione dei record si basa su oggetti JSON consecutivi. La disaggregazione può anche essere di questo tipo Delimited, vale a dire che la separazione dei record viene eseguita in base a un delimitatore personalizzato specificato. Questo delimitatore personalizzato deve essere una stringa con codifica in base 64. Ad esempio, se si desidera utilizzare la stringa seguente come delimitatore personalizzato, è necessario specificarla nel formato codificato base-64####, che la traduce in. IyMjIw== La deaggregazione dei record per JSON o per delimitatore è limitata a 500 per record.


Note

Quando disaggregate i record JSON, assicuratevi che l'input sia ancora presentato nel formato JSON supportato. Gli oggetti JSON devono trovarsi su una singola riga senza delimitatori o devono essere delimitati solo da una nuova riga (JSONL). Una matrice di oggetti JSON non è un input valido.


Questi sono esempi di input corretto: `{"a":1}{ "a":2}` and `{"a":1}\n{"a":2}`

Questo è un esempio di immissione errata: `[{"a":1}, {"a":2}]`

Con i dati aggregati, quando si abilita il partizionamento dinamico, Firehose analizza i record e cerca oggetti JSON validi o record delimitati all'interno di ogni chiamata API in base al tipo di deaggregazione multi-record specificato.

 Important

Se i dati sono aggregati, il partizionamento dinamico può essere applicato solo se i dati vengono prima disaggregati.

 Important

Quando si utilizza la funzionalità di trasformazione dei dati in Firehose, la deaggregazione verrà applicata prima della trasformazione dei dati. I dati che entrano in Firehose verranno elaborati nel seguente ordine: Deaggregazione → Trasformazione dei dati tramite Lambda → Chiavi di partizionamento.

Risolvi gli errori di partizionamento dinamico

Se Amazon Data Firehose non è in grado di analizzare i record di dati nel tuo flusso Firehose o non riesce a estrarre le chiavi di partizionamento specificate o a valutare le espressioni incluse nel valore del prefisso S3, questi record di dati vengono inviati al prefisso del bucket di errore S3 che devi specificare quando crei il flusso Firehose in cui abiliti il partizionamento dinamico. Il prefisso del bucket di errore S3 contiene tutti i record che Firehose non è in grado di inviare alla destinazione S3 specificata. Questi record sono organizzati in base al tipo di errore. Oltre al record, l'oggetto distribuito include anche informazioni sull'errore per facilitarne la comprensione e la risoluzione.

È necessario specificare un prefisso del bucket di errore S3 per un flusso Firehose se si desidera abilitare il partizionamento dinamico per questo flusso Firehose. Se non si desidera abilitare il partizionamento dinamico per un flusso Firehose, è facoltativo specificare un prefisso del bucket di errore S3.

Dati buffer per il partizionamento dinamico

Amazon Data Firehose memorizza nel buffer i dati di streaming in entrata fino a una certa dimensione e per un determinato periodo di tempo prima di consegnarli alle destinazioni specificate. È possibile configurare la dimensione e l'intervallo del buffer durante la creazione di nuovi flussi Firehose o

aggiornare la dimensione e l'intervallo del buffer sui flussi Firehose esistenti. La dimensione del buffer viene misurata in e l'intervallo del buffer viene misurato in secondi. MBs

Note

La funzionalità Zero Buffering non è disponibile per il partizionamento dinamico.

Quando il partizionamento dinamico è abilitato, Firehose memorizza internamente i record che appartengono a una determinata partizione in base al suggerimento di buffering configurato (dimensione e ora) prima di consegnare questi record al bucket Amazon S3. Per fornire oggetti di dimensioni massime, Firehose utilizza internamente un buffering multistadio. Pertanto, il end-to-end ritardo di un batch di record potrebbe essere 1,5 volte il tempo di suggerimento per il buffering configurato. Ciò influisce sulla freschezza dei dati di un flusso Firehose.

Il conteggio delle partizioni attive corrisponde al numero totale di partizioni attive all'interno del buffer di distribuzione. Ad esempio, se la query di partizionamento dinamico costruisce 3 partizioni al secondo e disponi di una configurazione di suggerimento per il buffering che attiva la distribuzione ogni 60 secondi, in media si avranno 180 partizioni attive. Se Firehose non è in grado di consegnare i dati in una partizione a una destinazione, questa partizione viene contata come attiva nel buffer di consegna fino a quando non può essere consegnata.

Una nuova partizione viene creata quando un prefisso S3 viene valutato con un nuovo valore in base ai campi di dati del record e alle espressioni del prefisso S3. Un nuovo buffer viene creato per ogni partizione attiva. Ogni record successivo con lo stesso prefisso S3 valutato viene inviato a quel buffer.

Una volta che il buffer raggiunge il limite di dimensione del buffer o l'intervallo di tempo del buffer, Firehose crea un oggetto con i dati del buffer e lo invia al prefisso Amazon S3 specificato. Dopo la consegna dell'oggetto, il buffer per quella partizione e la partizione stessa vengono eliminati e rimossi dal conteggio delle partizioni attive.

Firehose fornisce ogni dato del buffer come oggetto singolo una volta soddisfatte le dimensioni o l'intervallo del buffer per ciascuna partizione separatamente. Una volta che il numero di partizioni attive raggiunge il limite di 500 per flusso Firehose, il resto dei record del flusso Firehose viene inviato al prefisso del bucket di errore S3 specificato (`.`). `activePartitionExceeded` Puoi utilizzare il [modulo Amazon Data Firehose Limits](#) per richiedere un aumento di questa quota fino a 5000 partizioni attive per un determinato flusso Firehose. Se sono necessarie più partizioni, è possibile creare più flussi Firehose e distribuire le partizioni attive su di essi.

Convertire il formato dei dati di input in Amazon Data Firehose

Amazon Data Firehose è in grado di convertire il formato dei dati di input da JSON ad [Apache Parquet o Apache ORC prima di archivarli](#) in Amazon S3. Parquet e ORC sono formati di dati colonnari che consentono di risparmiare spazio e consentono query più veloci rispetto ai formati orientati alle righe come JSON. Se desideri convertire un formato di input diverso da JSON, come valori separati da virgole (CSV) o testo strutturato, puoi prima trasformarlo in JSON. AWS Lambda Per ulteriori informazioni, consulta [Trasforma i dati di origine](#).

Puoi convertire il formato dei tuoi dati anche se aggregi i tuoi record prima di inviarli ad Amazon Data Firehose.

Amazon Data Firehose richiede i seguenti tre elementi per convertire il formato dei dati dei record:

Deserializer

Amazon Data Firehose richiede un deserializzatore per leggere il codice JSON dei dati di input. Puoi scegliere uno dei seguenti due tipi di deserializzatore.

Quando combini più documenti JSON nello stesso record, assicurati che l'input sia comunque presentato nel formato JSON supportato. Una matrice di documenti JSON non è un input valido.

Ad esempio, questo è l'input corretto: `{"a": 1}{ "b": 1}` e questo è l'input errato: `[{"a": 1}, {"a": 2}]`.

- [Apache Hive JSON SerDe](#)
- [OpenX JSON SerDe](#)

Scegli il deserializzatore JSON

Scegli [OpenX JSON SerDe se il tuo JSON](#) di input contiene timestamp nei seguenti formati:

- `yyyy-MM-dd'T'hh:mm:ss [.S] 'Z'`, dove la frazione può avere fino a 9 cifre, ad esempio, `2017-02-07T15:13:01.39256Z`
- `yyyy-[M]M-[d]d HH:mm:ss[.S]`, dove la frazione può avere fino a 9 cifre, ad esempio, `2017-02-07 15:13:01.14`.

- Secondi epoch: ad esempio, 1518033528.
- Millisecondi epoch: ad esempio, 1518033528123.
- Secondi epoch a virgola mobile: ad esempio, 1518033528.123.

OpenX JSON SerDe può convertire i punti (.) in caratteri di sottolineatura (_). _ Può anche convertire le chiavi JSON in minuscolo prima di deserializzarle. [Per ulteriori informazioni sulle opzioni disponibili con questo deserializzatore tramite Amazon Data Firehose, consulta Open. XJson SerDe](#)

Se non sei sicuro di quale deserializzatore scegliere, usa OpenX JSON SerDe, a meno che tu non abbia timestamp che non supporta.

[Se hai timestamp in formati diversi da quelli elencati in precedenza, usa Apache Hive JSON. SerDe](#)

Se scegli questo deserializzatore, puoi specificare i formati di timestamp da utilizzare. Per eseguire questa operazione, segui il modello di sintassi delle stringhe di formato `DateTimeFormat` Joda-Time. [Per ulteriori informazioni, consulta Class. DateTimeFormat](#)

Puoi anche utilizzare il valore speciale `millis` per analizzare timestamp in millisecondi Unix epoch. Se non specifichi un formato, Amazon Data Firehose lo utilizza `java.sql.Timestamp::valueOf` per impostazione predefinita.

Hive JSON SerDe non consente quanto segue:

- Punti (.) nei nomi di colonna.
- Campi il cui tipo è `uniontype`.
- Campi che dispongono di tipi di numerici nello schema, ma che sono stringhe in JSON. Ad esempio, se lo schema è (un `int`) e il JSON lo è `{"a": "123"}`, Hive SerDe restituisce un errore.

Hive SerDe non converte JSON annidato in stringhe. Ad esempio, se hai `{"a": {"inner": 1}}`, non tratta `{"inner": 1}` come stringa.

Schema

Amazon Data Firehose richiede uno schema per determinare come interpretare tali dati. Usa [AWS Glue](#) per creare uno schema in AWS Glue Data Catalog. Amazon Data Firehose fa quindi riferimento a tale schema e lo utilizza per interpretare i dati di input. Puoi utilizzare lo stesso schema per configurare sia Amazon Data Firehose che il tuo software di analisi. Per ulteriori informazioni, consulta [Populating the AWS Glue Data Catalog](#) nella AWS Glue Developer Guide.

Note

Lo schema creato in AWS Glue Data Catalog deve corrispondere alla struttura dei dati di input. In caso contrario, i dati convertiti non conterranno attributi non specificati nello schema. Se utilizzi il codice JSON nidificato, utilizza un tipo STRUCT nello schema che rispecchi la struttura dei tuoi dati JSON. Vedi [questo esempio](#) su come gestire il codice JSON nidificato con un tipo STRUCT.

Important

Per i tipi di dati che non specificano un limite di dimensione, esiste un limite pratico di 32 MBs per tutti i dati in una singola riga.

Se si specifica length per CHAR o VARCHAR, Firehose tronca le stringhe alla lunghezza specificata quando legge i dati di input. Se la stringa di dati sottostante è più lunga, rimane invariata.

Serializer

Firehose richiede un serializzatore per convertire i dati nel formato di archiviazione colonnare di destinazione (Parquet o ORC): è possibile scegliere uno dei due tipi di serializzatori seguenti.

- [ORC SerDe](#)
- [Parquet SerDe](#)

Scegli il serializzatore

Il serializzatore scelto dipende dalle esigenze aziendali. [Per ulteriori informazioni sulle due opzioni di serializzazione, consulta ORC e Parquet. SerDe SerDe](#)

Abilita la conversione del formato di registrazione

Se abiliti la conversione del formato di record, non puoi impostare la destinazione Amazon Data Firehose come Amazon OpenSearch Service, Amazon Redshift o Splunk. Con la conversione del formato abilitata, Amazon S3 è l'unica destinazione che puoi usare per il tuo stream Firehose. La sezione seguente mostra come abilitare la conversione del formato di registrazione dalle operazioni

della console e dell'API Firehose. Per un esempio di come impostare la conversione del formato di record con CloudFormation, vedi [AWS::DataFirehose: DeliveryStream](#).

Abilita la conversione del formato di registrazione dalla console

È possibile abilitare la conversione del formato dei dati sulla console quando si crea o si aggiorna uno stream Firehose. Con la conversione del formato dei dati abilitata, Amazon S3 è l'unica destinazione che puoi configurare per lo stream Firehose. Inoltre, la compressione Amazon S3 viene disabilitata quando abiliti la conversione del formato. Tuttavia, la compressione Snappy si verifica automaticamente come parte del processo di conversione. Il formato di framing per Snappy utilizzato da Amazon Data Firehose in questo caso è compatibile con Hadoop. Ciò significa che puoi utilizzare i risultati della compressione Snappy ed eseguire query su questi dati in Athena. [Per il formato di framing Snappy su cui si basa Hadoop, consulta `.java. BlockCompressorStream`](#)

Per abilitare la conversione del formato dei dati per un flusso di dati Firehose

1. Accedi a e apri Console di gestione AWS la console Amazon Data Firehose all'indirizzo. <https://console.aws.amazon.com/firehose/>
2. Scegli uno stream Firehose da aggiornare o crea un nuovo stream Firehose seguendo la procedura riportata di seguito. [Tutorial: Creare uno stream Firehose dalla console](#)
3. In Convert record format (Converti formato record), impostare Record format conversion (Conversione formato record) su Enabled (Abilitata).
4. Scegliere il formato di output desiderato. Per ulteriori informazioni sulle due opzioni, consulta [Apache Parquet](#) e [Apache ORC](#).
5. Scegliete una AWS Glue tabella per specificare uno schema per i record di origine. Impostare la regione, il database, la tabella e la versione della tabella.

Gestione della conversione del formato di record dall'API Firehose

[Se desideri che Amazon Data Firehose converta il formato dei dati di input da JSON a Parquet o ORC, specifica l'`DataFormatConversionConfiguration` elemento opzionale in `ExtendDS3` o `DestinationConfigurationExtendDS3`. `DestinationUpdate`](#) Se lo specifichi, si applicano le seguenti restrizioni. [DataFormatConversionConfiguration](#)

- In [BufferingHints](#), non è possibile impostare un valore inferiore `SizeInMBs` a 64 se si abilita la conversione del formato di record. Inoltre, se la conversione del formato non è abilitata, il valore predefinito è 5. Se la abiliti, il valore diventa 128.

- [È necessario impostare CompressionFormat in ExtendedS3 DestinationConfiguration o in ExtendedS3 su DestinationUpdate UNCOMPRESSED](#) Il valore predefinito per CompressionFormat è UNCOMPRESSED. [Pertanto, puoi anche lasciarlo non specificato in ExtendedS3 DestinationConfiguration](#) I dati vengono ancora compressi come parte del processo di serializzazione, utilizzando la compressione Snappy per impostazione predefinita. Il formato di framing per Snappy utilizzato da Amazon Data Firehose in questo caso è compatibile con Hadoop. Ciò significa che puoi utilizzare i risultati della compressione Snappy ed eseguire query su questi dati in Athena. [Per il formato di framing Snappy su cui si basa Hadoop, consulta .java.BlockCompressorStream](#) Quando configuri il serializzatore, puoi scegliere altri tipi di compressione.

Gestione degli errori per la conversione del formato dei dati

Quando Amazon Data Firehose non è in grado di analizzare o deserializzare un record (ad esempio, quando i dati non corrispondono allo schema), lo scrive su Amazon S3 con un prefisso di errore. Se questa scrittura non riesce, Amazon Data Firehose riprova per sempre, bloccando l'ulteriore consegna. Per ogni record non riuscito, Amazon Data Firehose scrive un documento JSON con lo schema seguente:

```
{
  "attemptsMade": long,
  "arrivalTimestamp": long,
  "errorCode": string,
  "errorMessage": string,
  "attemptEndingTimestamp": long,
  "rawData": string,
  "sequenceNumber": string,
  "subSequenceNumber": long,
  "dataCatalogTable": {
    "catalogId": string,
    "databaseName": string,
    "tableName": string,
    "region": string,
    "versionId": string,
    "catalogArn": string
  }
}
```

Comprendi la distribuzione dei dati in Amazon Data Firehose

Quando invii dati al tuo stream Firehose, questi vengono consegnati automaticamente alla destinazione prescelta. La tabella seguente spiega la consegna dei dati a diverse destinazioni.

Destinazione	Informazioni
Simple Storage Service (Amazon S3)	Per la distribuzione dei dati ad Amazon S3, Firehose concatena più record in entrata in base alla configurazione di buffering del flusso Firehose. Quindi distribuisce i record ad Amazon S3 come oggetto Amazon S3. Per impostazione predefinita, Firehose concatena i dati senza delimitatori. Se si desidera disporre di nuovi delimitatori di riga tra i record, è possibile aggiungere nuovi delimitatori di riga abilitando la funzionalità nella configurazione della console Firehose o nel parametro API. La consegna dei dati tra Firehose e la destinazione Amazon S3 è crittografata con TLS (HTTPS).
Amazon Redshift	Per la distribuzione dei dati ad Amazon Redshift, Firehose invia innanzitutto i dati in entrata al bucket S3 nel formato descritto in precedenza. Firehose emette quindi un comando Amazon COPY Redshift per caricare i dati dal bucket S3 al cluster con provisioning di Amazon Redshift o al gruppo di lavoro Serverless Amazon Redshift. Assicurati che, dopo che Amazon Data Firehose ha concatenato più record in entrata in un oggetto Amazon S3, l'oggetto Amazon S3 possa essere copiato nel cluster con provisioning di Amazon Redshift o nel gruppo di lavoro Amazon Redshift Serverless. Per ulteriori informazioni, vedi i parametri del formato dati del comando COPY di Amazon Redshift.
OpenSearch OpenSearch Service e Serverless	Per la distribuzione dei dati a OpenSearch Service e OpenSearch Serverless, Amazon Data Firehose memorizza nel buffer i record in entrata in base alla configurazione di buffering del flusso Firehose. Quindi genera una richiesta in blocco di OpenSearch Service o OpenSearch Serverless per indicizzare più record nel cluster di servizio o nella raccolta Serverless. OpenSearch Assicurati che il record sia codificato in UTF-8 e appiattito in un oggetto JSON a riga singola prima di inviarlo ad Amazon

Destinazione	Informazioni
	<p>Data Firehose. Inoltre, l'<code>rest.action.multi.allow_explicit_index</code> opzione per il cluster di OpenSearch servizio deve essere impostata su <code>true</code> (impostazione predefinita) per accettare richieste in blocco con un indice esplicito impostato per record. Per ulteriori informazioni, consulta OpenSearch Service Configure Advanced Options nella Amazon OpenSearch Service Developer Guide.</p>
Splunk	<p>Per la consegna dei dati a Splunk, Amazon Data Firehose concatena i byte inviati. Se nei dati vuoi dei delimitatori, come un carattere di nuova riga, devi inserirli manualmente. Verifica che Splunk sia configurato per analizzare questo tipo di delimitatori. Per reindirizzare a Splunk i dati che sono stati consegnati al bucket di errore S3 (backup S3), segui i passaggi indicati nella documentazione di Splunk.</p>
Endpoint HTTP	<p>Per la consegna dei dati a un endpoint HTTP di proprietà di un fornitore di servizi terzo supportato, puoi utilizzare il servizio integrato Amazon Lambda per creare una funzione per trasformare i record in entrata nel formato che corrisponde al formato previsto dall'integrazione del fornitore di servizi. Contatta il fornitore di servizi di terze parti di cui hai scelto l'endpoint HTTP come destinazione per saperne di più sul formato di record accettato.</p>

Destinazione	Informazioni
Snowflake	Per la consegna dei dati a Snowflake, Amazon Data Firehose memorizza internamente i dati nel buffer per un secondo e utilizza le operazioni dell'API di streaming Snowflake per inserire dati in Snowflake. Per impostazione predefinita, i record inseriti vengono cancellati e trasferiti nella tabella Snowflake ogni secondo. Dopo aver effettuato la chiamata di inserimento, Firehose emette una CloudWatch metrica che misura il tempo impiegato per il commit dei dati su Snowflake. Attualmente Firehose supporta solo un singolo elemento JSON come payload di record e non supporta gli array JSON. Assicurati che il payload di input sia un oggetto JSON valido e che sia ben formato senza virgolette, virgolette o caratteri di escape aggiuntivi.

Ogni destinazione Firehose ha una propria frequenza di consegna dei dati. Per ulteriori informazioni, consulta [Configura i suggerimenti per il buffering](#).

Duplicazione di record

Amazon Data Firehose utilizza la at-least-once semantica per la distribuzione dei dati. In alcune circostanze, ad esempio quando scadono i tempi di consegna dei dati, i nuovi tentativi di consegna da parte di Amazon Data Firehose potrebbero creare duplicati se la richiesta originale di consegna dei dati alla fine viene accolta. Questo vale per tutti i tipi di destinazione supportati da Amazon Data Firehose, ad eccezione delle destinazioni Amazon S3, Apache Iceberg Tables e Snowflake.

Argomenti

- [Comprendi la distribuzione tra account e regioni AWS](#)
- [Comprendi le specifiche di richiesta e risposta di consegna degli endpoint HTTP](#)
- [Gestisci gli errori di consegna dei dati](#)
- [Configurazione del formato dei nomi degli oggetti Amazon S3](#)
- [Configura la rotazione dell'indice per Service OpenSearch](#)
- [Sospendere e riprendere la consegna dei dati](#)

Comprendi la distribuzione tra account e regioni AWS

Amazon Data Firehose supporta la distribuzione di dati verso destinazioni endpoint HTTP tra diversi account. AWS Lo stream Firehose e l'endpoint HTTP che scegli come destinazione possono appartenere a diversi account. AWS

Amazon Data Firehose supporta anche la distribuzione di dati verso destinazioni endpoint HTTP in tutte le regioni. AWS È possibile inviare dati da un flusso Firehose in una AWS regione a un endpoint HTTP in un'altra regione. AWS È inoltre possibile inviare dati da un flusso Firehose a una destinazione endpoint HTTP al di fuori delle AWS regioni, ad esempio al proprio server locale impostando l'URL dell'endpoint HTTP sulla destinazione desiderata. Per questi scenari, ai costi di distribuzione si aggiungono ulteriori costi di trasferimento dati. Per ulteriori informazioni, consulta la sezione [Trasferimento dati](#) della pagina "Prezzi on demand".

Comprendi le specifiche di richiesta e risposta di consegna degli endpoint HTTP

Affinché Amazon Data Firehose fornisca correttamente i dati agli endpoint HTTP personalizzati, questi endpoint devono accettare richieste e inviare risposte utilizzando determinati formati di richiesta e risposta di Amazon Data Firehose. Questa sezione descrive le specifiche di formato delle richieste HTTP che il servizio Amazon Data Firehose invia agli endpoint HTTP personalizzati, nonché le specifiche di formato delle risposte HTTP che il servizio Amazon Data Firehose si aspetta. Gli endpoint HTTP dispongono di 3 minuti per rispondere a una richiesta prima che Amazon Data Firehose effettui il timeout della richiesta. Amazon Data Firehose considera le risposte che non rispettano il formato corretto come errori di consegna.

Formato della richiesta

Parametri relativi al percorso e all'URL

Questi parametri sono configurati direttamente dall'utente come parte di un singolo campo URL. Amazon Data Firehose li invia così come configurati senza modifiche. Sono supportate solo le destinazioni https. Le restrizioni relative agli URL vengono applicate durante la configurazione del flusso di distribuzione.

Note

Attualmente, solo la porta 443 è supportata per la distribuzione dei dati degli endpoint HTTP.

Intestazioni HTTP - -Versione X-Amz-Firehose-Protocol

Questa intestazione viene utilizzata per indicare la versione dei formati di richiesta/risposta. Attualmente, l'unica versione consentita è 1.0.

Intestazioni HTTP - -Id X-Amz-Firehose-Request

Il valore di questa intestazione è un GUID opaco che può essere utilizzato per scopi di debug e deduplicazione. Le implementazioni degli endpoint devono registrare il valore di questa intestazione, se possibile, sia per le richieste riuscite che per quelle non riuscite. L'ID della richiesta viene mantenuto invariato tra più tentativi della stessa richiesta.

Intestazioni HTTP: Content-Type

Il valore dell'intestazione Content-Type è sempre `application/json`.

Intestazioni HTTP: Content-Encoding

Uno stream Firehose può essere configurato per utilizzare GZIP per comprimere il body durante l'invio delle richieste. Quando questa compressione è abilitata, il valore dell'intestazione Content-Encoding è impostato su `gzip`, come da prassi standard. Se la compressione non è abilitata, l'intestazione Content-Encoding è del tutto assente.

Intestazioni HTTP: Content-Length

Viene utilizzato nel modo standard.

Intestazioni HTTP - -Arn: X-Amz-Firehose-Source

L'ARN del flusso Firehose rappresentato in formato stringa ASCII. L'ARN codifica la regione, l'ID AWS dell'account e il nome dello stream. Ad esempio, `arn:aws:firehose:us-east-1:123456789:deliverystream/testStream`.

Intestazioni HTTP - -Key X-Amz-Firehose-Access

Questa intestazione contiene una chiave API o altre credenziali. Hai la possibilità di creare o aggiornare la chiave API (nota anche come token di autorizzazione) durante la creazione o l'aggiornamento del flusso di distribuzione. Amazon Data Firehose limita la dimensione della

chiave di accesso a 4096 byte. Amazon Data Firehose non tenta di interpretare questa chiave in alcun modo. La chiave configurata viene copiata letteralmente nel valore di questa intestazione. Tuttavia, se si utilizza Secrets Manager per configurare la chiave, il segreto deve seguire un formato oggetto JSON specifico: {"api_key": "..."}.

I contenuti possono essere arbitrari e possono potenzialmente rappresentare un token JWT o un ACCESS_KEY. Se un endpoint richiede credenziali multi-campo (ad esempio nome utente e password), i valori di tutti i campi devono essere memorizzati insieme in un'unica chiave di accesso in un formato comprensibile all'endpoint (JSON o CSV). Questo campo può essere codificato in base 64 se i contenuti originali sono binari. Amazon Data Firehose non modifica, and/or codifica il valore configurato e utilizza i contenuti così come sono.

Intestazioni HTTP - -Attributi X-Amz-Firehose-Common

Questa intestazione contiene gli attributi comuni (metadati) relativi all'intera richiesta, a tutti i record and/or all'interno della richiesta. Questi vengono configurati direttamente dall'utente durante la creazione di uno stream Firehose. Il valore di questo attributo è codificato come oggetto JSON con il seguente schema:

```
"$schema": http://json-schema.org/draft-07/schema#

properties:
  commonAttributes:
    type: object
    minProperties: 0
    maxProperties: 50
    patternProperties:
      "^.{1,256}$":
        type: string
        minLength: 0
        maxLength: 1024
```

Ecco un esempio:

```
"commonAttributes": {
  "deployment -context": "pre-prod-gamma",
  "device-types": ""
}
```

Corpo: dimensione massima

La dimensione massima del corpo è configurata dall'utente e può arrivare fino a un massimo di 64 MiB, prima della compressione.

Corpo: schema

Il corpo contiene un singolo documento JSON con il seguente schema JSON (scritto in YAML):

```
"$schema": http://json-schema.org/draft-07/schema#

title: FirehoseCustomHttpsEndpointRequest
description: >
  The request body that the Firehose service sends to
  custom HTTPS endpoints.
type: object
properties:
  requestId:
    description: >
      Same as the value in the X-Amz-Firehose-Request-Id header,
      duplicated here for convenience.
    type: string
  timestamp:
    description: >
      The timestamp (milliseconds since epoch) at which the Firehose
      server generated this request.
    type: integer
  records:
    description: >
      The actual records of the Firehose stream, carrying
      the customer data.
    type: array
    minItems: 1
    maxItems: 10000
    items:
      type: object
      properties:
        data:
          description: >
            The data of this record, in Base64. Note that empty
            records are permitted in Firehose. The maximum allowed
            size of the data, before Base64 encoding, is 1024000
            bytes; the maximum length of this field is therefore
```

```
    1365336 chars.
    type: string
    minLength: 0
    maxLength: 1365336

required:
  - requestId
  - records
```

Ecco un esempio:

```
{
  "requestId": "ed4acda5-034f-9f42-bba1-f29aea6d7d8f",
  "timestamp": 1578090901599
  "records": [
    {
      "data": "aGVsbG8="
    },
    {
      "data": "aGVsbG8gd29ybGQ="
    }
  ]
}
```

Formato della risposta

Comportamento predefinito in caso di errore

Se una risposta non è conforme ai requisiti seguenti, il server Firehose la considera come se avesse un codice di stato 500 senza corpo.

Codice di stato

Il codice di stato HTTP DEVE essere compreso nell'intervallo 2XX, 4XX o 5XX.

Il server Amazon Data Firehose NON segue i reindirizzamenti (codici di stato 3XX). Solo il codice di risposta 200 viene considerato come una distribuzione riuscita dei record a HTTP/EP. Il codice di risposta 413 (dimensione superata) è considerato un errore permanente e il batch di record non viene inviato al bucket di errori se configurato. Tutti gli altri codici di risposta sono considerati

errori recuperabili e sono soggetti all' algoritmo di back-off relativo ai nuovi tentativi illustrato più avanti.

Intestazioni: tipo di contenuto

L'unico tipo di contenuto accettabile è application/json.

Intestazioni HTTP: Content-Encoding

La codifica del contenuto NON DEVE essere utilizzata. Il corpo DEVE essere decompresso.

Intestazioni HTTP: Content-Length

L'intestazione Content-Length DEVE essere presente se la risposta ha un corpo.

Corpo: dimensione massima

Il corpo della risposta deve avere dimensioni pari o inferiori a 1 MiB.

```
"$schema": http://json-schema.org/draft-07/schema#  
  
title: FirehoseCustomHttpsEndpointResponse  
  
description: >  
  The response body that the Firehose service sends to  
  custom HTTPS endpoints.  
type: object  
properties:  
  requestId:  
    description: >  
      Must match the requestId in the request.  
    type: string  
  
  timestamp:  
    description: >  
      The timestamp (milliseconds since epoch) at which the  
      server processed this request.  
    type: integer  
  
  errorMessage:  
    description: >  
      For failed requests, a message explaining the failure.  
      If a request fails after exhausting all retries, the last  
      Instance of the error message is copied to error output  
      S3 bucket if configured.
```

```
type: string
minLength: 0
maxLength: 8192
required:
- requestId
- timestamp
```

Ecco un esempio:

```
Failure Case (HTTP Response Code 4xx or 5xx)
{
  "requestId": "ed4acda5-034f-9f42-bba1-f29aea6d7d8f",
  "timestamp": "1578090903599",
  "errorMessage": "Unable to deliver records due to unknown error."
}
Success case (HTTP Response Code 200)
{
  "requestId": "ed4acda5-034f-9f42-bba1-f29aea6d7d8f",
  "timestamp": 1578090903599
}
```

Gestione delle risposte di errore

In tutti i casi di errore, il server Amazon Data Firehose ritenta la consegna dello stesso batch di record utilizzando un algoritmo di back-off esponenziale. Il backup dei tentativi viene eseguito utilizzando un tempo di back-off iniziale (1 secondo) con un fattore di jitter del (15%) e ogni tentativo successivo viene bloccato utilizzando la formula $(\text{initial-backoff-time} * (\text{multiplier } 2)^{\text{retry_count}})$ con jitter aggiunto. Il tempo di back-off è limitato a un intervallo massimo di 2 minuti. Ad esempio, al 'n'-esimo tentativo, il tempo di annullamento è $= \text{MAX}(120, 2^n) * \text{casuale}(0,85, 1,15)$.

I parametri specificati nell'equazione precedente sono soggetti a modifiche. Fate riferimento alla documentazione di AWS Firehose per il tempo esatto di backoff iniziale, il tempo massimo di backoff, i moltiplicatori e le percentuali di jitter utilizzate nell'algoritmo di backoff esponenziale.

In ogni tentativo successivo, la and/or destinazione della chiave di accesso a cui vengono consegnati i record potrebbe cambiare in base alla configurazione aggiornata del flusso Firehose. Il servizio Amazon Data Firehose utilizza lo stesso ID di richiesta per tutti i tentativi nel miglior

modo possibile. Quest'ultima funzionalità può essere utilizzata per scopi di deduplicazione dal server endpoint HTTP. Se la richiesta non viene ancora consegnata dopo il tempo massimo consentito (in base alla configurazione del flusso Firehose), il batch di record può essere facoltativamente inviato a un bucket di errori basato sulla configurazione del flusso.

Esempi

Esempio di richiesta proveniente dall'origine CWLog .

```
{
  "requestId": "ed4acda5-034f-9f42-bba1-f29aea6d7d8f",
  "timestamp": 1578090901599,
  "records": [
    {
      "data": {
        "messageType": "DATA_MESSAGE",
        "owner": "123456789012",
        "logGroup": "log_group_name",
        "logStream": "log_stream_name",
        "subscriptionFilters": [
          "subscription_filter_name"
        ],
        "logEvents": [
          {
            "id": "01234567890123456789012345678901234567890123456789012345",
            "timestamp": 1510109208016,
            "message": "log message 1"
          },
          {
            "id": "01234567890123456789012345678901234567890123456789012345",
            "timestamp": 1510109208017,
            "message": "log message 2"
          }
        ]
      }
    ]
  ]
}
```

Gestisci gli errori di consegna dei dati

Ogni destinazione Amazon Data Firehose dispone di una propria gestione degli errori di consegna dei dati.

Quando si configura uno stream Firehose, per molte destinazioni come OpenSearch gli endpoint Splunk e HTTP, si configura anche un bucket S3 in cui è possibile eseguire il backup dei dati che non vengono consegnati. Per ulteriori informazioni su come Firehose esegue il backup dei dati in caso di mancate consegne, consultate le sezioni relative alla destinazione in questa pagina. Per ulteriori informazioni su come concedere l'accesso ai bucket S3 in cui è possibile eseguire il backup dei dati che non vengono consegnati, consulta [Concedere l'accesso a Firehose a una destinazione Amazon S3](#). Quando Firehose (a) non riesce a consegnare i dati alla destinazione dello stream e (b) non riesce a scrivere i dati nel bucket S3 di backup in caso di consegne non riuscite, di fatto sospende la consegna dello stream fino a quando i dati non possono essere consegnati alla destinazione o scritti nella posizione di backup S3.

Simple Storage Service (Amazon S3)

La distribuzione dei dati sul bucket S3 potrebbe non riuscire per diversi motivi. Ad esempio, il bucket potrebbe non esistere più, il ruolo IAM che Amazon Data Firehose presuppone potrebbe non avere accesso al bucket, il problema di rete o eventi simili. In queste condizioni, Amazon Data Firehose continua a riprovare per un massimo di 24 ore fino al completamento della consegna. Il tempo massimo di archiviazione dei dati di Amazon Data Firehose è di 24 ore. Se la distribuzione dei dati non va a buon fine per più di 24 ore, i dati vengono persi.

La consegna dei dati al bucket S3 può fallire per vari motivi, ad esempio:

- Il bucket non esiste più.
- Il ruolo IAM assunto da Amazon Data Firehose non ha accesso al bucket.
- Problemi di rete.
- Errori S3, come HTTP 500 o altri errori dell'API.

In questi casi, Amazon Data Firehose riproverà la consegna:

- DirectPut fonti: i tentativi continuano per un massimo di 24 ore.
- Sorgenti Kinesis Data Streams o Amazon MSK: i nuovi tentativi continuano a tempo indeterminato, fino alla politica di conservazione definita nello stream.

Amazon Data Firehose invia i record non riusciti a un bucket di errore S3 solo quando l'elaborazione Lambda o la conversione del parquet falliscono. Altri scenari di errore comporteranno continui tentativi di riprovare S3 fino al raggiungimento del periodo di conservazione. Quando Firehose invia correttamente i record a S3, crea un file oggetto S3 e, in caso di errori parziali dei record, riprova automaticamente il recapito e aggiorna lo stesso file oggetto S3 con i record elaborati correttamente.

Amazon Redshift

Per una destinazione Amazon Redshift, puoi specificare una durata dei tentativi (0—7200 secondi) durante la creazione di uno stream Firehose.

La distribuzione dei dati sul cluster con provisioning Amazon Redshift o sul gruppo di lavoro Amazon Redshift serverless potrebbe non riuscire per diversi motivi. Ad esempio, potresti avere una configurazione cluster errata del tuo flusso Firehose, un cluster o un gruppo di lavoro in manutenzione o un errore di rete. In queste condizioni, Amazon Data Firehose riprova per il periodo di tempo specificato e salta quel particolare batch di oggetti Amazon S3. Le informazioni relative agli oggetti non elaborati vengono inviate al bucket S3 sotto forma di file manifest nella cartella `errors/`, che potrai utilizzare per recuperare le informazioni manualmente. Per ulteriori informazioni su come copiare manualmente i file manifest, consulta [Utilizzo di un manifest per specificare i file di dati](#).

Amazon OpenSearch Service e OpenSearch Serverless

Per la destinazione OpenSearch Service e OpenSearch Serverless, è possibile specificare una durata del nuovo tentativo (0—7200 secondi) durante la creazione del flusso Firehose.

La consegna dei dati al cluster di OpenSearch servizio o alla raccolta OpenSearch Serverless potrebbe non riuscire per diversi motivi. Ad esempio, si potrebbe avere una configurazione errata del cluster di OpenSearch servizio o della raccolta OpenSearch Serverless del flusso Firehose, OpenSearch un cluster di servizio OpenSearch o una raccolta Serverless in manutenzione, un errore di rete o eventi simili. In queste condizioni, Amazon Data Firehose riprova per la durata specificata e quindi salta quella particolare richiesta di indice. I documenti non elaborati vengono distribuiti sul bucket S3 nella cartella `AmazonOpenSearchService_failed/`, che potrai utilizzare per recuperare le informazioni manualmente.

Per OpenSearch Service, ogni documento ha il seguente formato JSON:

```
{
  "attemptsMade": "(number of index requests attempted)",
  "arrivalTimestamp": "(the time when the document was received by Firehose)",
```

```
"errorCode": "(http error code returned by OpenSearch Service)",
"errorMessage": "(error message returned by OpenSearch Service)",
"attemptEndingTimestamp": "(the time when Firehose stopped attempting index
request)",
"esDocumentId": "(intended OpenSearch Service document ID)",
"esIndexName": "(intended OpenSearch Service index name)",
"esTypeName": "(intended OpenSearch Service type name)",
"rawData": "(base64-encoded document data)"
}
```

Per OpenSearch Serverless, ogni documento ha il seguente formato JSON:

```
{
  "attemptsMade": "(number of index requests attempted)",
  "arrivalTimestamp": "(the time when the document was received by Firehose)",
  "errorCode": "(http error code returned by OpenSearch Serverless)",
  "errorMessage": "(error message returned by OpenSearch Serverless)",
  "attemptEndingTimestamp": "(the time when Firehose stopped attempting index
request)",
  "osDocumentId": "(intended OpenSearch Serverless document ID)",
  "osIndexName": "(intended OpenSearch Serverless index name)",
  "rawData": "(base64-encoded document data)"
}
```

Splunk

Quando Amazon Data Firehose invia dati a Splunk, attende una conferma da parte di Splunk. Se si verifica un errore o la conferma non arriva entro il periodo di timeout del riconoscimento, Amazon Data Firehose avvia il contatore della durata dei nuovi tentativi. Continua a riprovare fino alla scadenza della durata del nuovo tentativo. Successivamente, Amazon Data Firehose lo considera un errore di consegna dei dati ed esegue il backup dei dati nel bucket Amazon S3.

Ogni volta che Amazon Data Firehose invia dati a Splunk, che si tratti del tentativo iniziale o di un nuovo tentativo, riavvia il contatore del timeout di conferma. Attende quindi il riconoscimento che deve arrivare da Splunk. Anche se la durata del nuovo tentativo scade, Amazon Data Firehose attende comunque il riconoscimento fino a quando non lo riceve o non viene raggiunto il timeout di conferma. Se la conferma scade, Amazon Data Firehose verifica se è rimasto del tempo nel contatore dei tentativi. Se rimane del tempo, riprova ancora e ripete la logica fino a quando non riceve un riconoscimento o stabilisce che il tempo dei nuovi tentativi è scaduto.

Di seguito è riportato un esempio di record degli errori.

```
{
  "attemptsMade":5,
  "arrivalTimestamp":1594265943615,
  "errorCode":"HttpEndpoint.DestinationException",
  "errorMessage":"Received the following response from the endpoint destination.
  {\"requestId\": \"109777ac-8f9b-4082-8e8d-b4f12b5fc17b\", \"timestamp\": 1594266081268,
  \"errorMessage\": \"Unauthorized\"}\",
  "attemptEndingTimestamp":1594266081318,
  "rawData\":\"c2FtcGx1IHJhdYBkYXRh\",
  "subsequenceNumber":0,
  "dataId\":\"49607357361271740811418664280693044274821622880012337186.0\"
}
```

Snowflake

Per la destinazione Snowflake, quando si crea uno stream Firehose, è possibile specificare una durata del nuovo tentativo opzionale (0-7200 secondi). Il valore predefinito per la durata dei nuovi tentativi è 60 secondi.

La consegna dei dati alla tabella Snowflake potrebbe non riuscire per diversi motivi, ad esempio una configurazione errata della destinazione Snowflake, un'interruzione di Snowflake, un errore di rete, ecc. La politica sui nuovi tentativi non si applica agli errori non recuperabili. Ad esempio, se Snowflake rifiuta il payload JSON perché nella tabella manca una colonna aggiuntiva, Firehose non tenterà di consegnarla nuovamente. Al contrario, crea un backup di tutti gli errori di inserimento dovuti a problemi di payload JSON nel bucket di errori S3.

Allo stesso modo, se la consegna non riesce a causa di un ruolo, una tabella o un database errati, Firehose non riprova e scrive i dati nel bucket S3. La durata del nuovo tentativo si applica solo in caso di errore dovuto a un problema del servizio Snowflake, problemi temporanei di rete, ecc. In queste condizioni, Firehose riprova per il periodo di tempo specificato prima di consegnarli a S3. I record con errori vengono inviati nella cartella snowflake-failed/, che è possibile utilizzare per il riempimento manuale.

Di seguito è riportato un esempio di JSON per ogni record che invii a S3.

```
{
  "attemptsMade": 3,
  "arrivalTimestamp": 1594265943615,
  "errorCode": "Snowflake.InvalidColumns",
```

```
"errorMessage": "Snowpipe Streaming does not support columns of type AUTOINCREMENT,
IDENTITY, GEO, or columns with a default value or collation",
"attemptEndingTimestamp": 1712937865543,
"rawData": "c2FtcGx1IHJhdyBkYXRh"
}
```

Configurazione del formato dei nomi degli oggetti Amazon S3

Quando Firehose fornisce dati ad Amazon S3, il nome della chiave dell'oggetto S3 segue il `<evaluated prefix><suffix>` formato, dove il suffisso ha il formato `----- <Firehose stream name><Firehose stream version><year><month><day><hour><minute><second><uuid><file extension><Firehose stream version>` inizia con 1 e aumenta di 1 per ogni modifica di configurazione del flusso Firehose. È possibile modificare le configurazioni dei flussi Firehose (ad esempio, il nome del bucket S3, i suggerimenti di buffering, la compressione e la crittografia). È possibile farlo utilizzando la console Firehose o l'operazione [UpdateDestinationAPI](#).

Perché `<evaluated prefix>`, Firehose aggiunge un prefisso orario predefinito nel formato. `YYYY/MM/dd/HH` Questo prefisso crea una gerarchia logica nel bucket, in cui ogni barra (/) crea un livello nella gerarchia. È possibile modificare questa struttura specificando un prefisso personalizzato che include espressioni valutate in fase di esecuzione. Per informazioni su come specificare un prefisso personalizzato, consulta [Prefissi personalizzati per Amazon Simple Storage Service Objects](#).

Per impostazione predefinita, il fuso orario utilizzato per il prefisso e il suffisso orario è in UTC, ma puoi modificarlo con il fuso orario che preferisci. Ad esempio, per utilizzare l'ora solare del Giappone anziché l'UTC, puoi configurare il fuso Asia/Tokyo orario in o [nell'impostazione Console di gestione AWS del parametro API CustomTimeZone \(\)](#). L'elenco seguente contiene i fusi orari supportati da Firehose per la configurazione del prefisso S3.

Fusi orari supportati

Di seguito è riportato un elenco di fusi orari supportati da Firehose per la configurazione del prefisso S3.

Africa

```
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmera
```

Africa/Bangui
Africa/Banjul
Africa/Bissau
Africa/Blantyre
Africa/Bujumbura
Africa/Cairo
Africa/Casablanca
Africa/Conakry
Africa/Dakar
Africa/Dar_es_Salaam
Africa/Djibouti
Africa/Douala
Africa/Freetown
Africa/Gaborone
Africa/Harare
Africa/Johannesburg
Africa/Kampala
Africa/Khartoum
Africa/Kigali
Africa/Kinshasa
Africa/Lagos
Africa/Libreville
Africa/Lome
Africa/Luanda
Africa/Lubumbashi
Africa/Lusaka
Africa/Malabo
Africa/Maputo
Africa/Maseru
Africa/Mbabane
Africa/Mogadishu
Africa/Monrovia
Africa/Nairobi
Africa/Ndjamena
Africa/Niamey
Africa/Nouakchott
Africa/Ouagadougou
Africa/Porto-Novo
Africa/Sao_Tome
Africa/Timbuktu
Africa/Tripoli
Africa/Tunis
Africa/Windhoek

America

America/Adak
America/Anchorage
America/Anguilla
America/Antigua
America/Aruba
America/Asuncion
America/Barbados
America/Belize
America/Bogota
America/Buenos_Aires
America/Caracas
America/Cayenne
America/Cayman
America/Chicago
America/Costa_Rica
America/Cuiaba
America/Curacao
America/Dawson_Creek
America/Denver
America/Dominica
America/Edmonton
America/El_Salvador
America/Fortaleza
America/Godthab
America/Grand_Turk
America/Grenada
America/Guadeloupe
America/Guatemala
America/Guayaquil
America/Guyana
America/Halifax
America/Havana
America/Indianapolis
America/Jamaica
America/La_Paz
America/Lima
America/Los_Angeles
America/Managua
America/Manaus
America/Martinique
America/Mazatlan
America/Mexico_City

```
America/Miquelon  
America/Montevideo  
America/Montreal  
America/Montserrat  
America/Nassau  
America/New_York  
America/Noronha  
America/Panama  
America/Paramaribo  
America/Phoenix  
America/Port_of_Spain  
America/Port-au-Prince  
America/Porto_Acre  
America/Puerto_Rico  
America/Regina  
America/Rio_Branco  
America/Santiago  
America/Santo_Domingo  
America/Sao_Paulo  
America/Scoresbysund  
America/St_Johns  
America/St_Kitts  
America/St_Lucia  
America/St_Thomas  
America/St_Vincent  
America/Tegucigalpa  
America/Thule  
America/Tijuana  
America/Tortola  
America/Vancouver  
America/Winnipeg
```

Antarctica

```
Antarctica/Casey  
Antarctica/DumontDUrville  
Antarctica/Mawson  
Antarctica/McMurdo  
Antarctica/Palmer
```

Asia

```
Asia/Aden
```

Asia/Almaty
Asia/Amman
Asia/Anadyr
Asia/Aqtau
Asia/Aqtobe
Asia/Ashgabat
Asia/Ashkhabad
Asia/Baghdad
Asia/Bahrain
Asia/Baku
Asia/Bangkok
Asia/Beirut
Asia/Bishkek
Asia/Brunei
Asia/Calcutta
Asia/Colombo
Asia/Dacca
Asia/Damascus
Asia/Dhaka
Asia/Dubai
Asia/Dushanbe
Asia/Hong_Kong
Asia/Irkutsk
Asia/Jakarta
Asia/Jayapura
Asia/Jerusalem
Asia/Kabul
Asia/Kamchatka
Asia/Karachi
Asia/Katmandu
Asia/Krasnoyarsk
Asia/Kuala_Lumpur
Asia/Kuwait
Asia/Macao
Asia/Magadan
Asia/Manila
Asia/Muscat
Asia/Nicosia
Asia/Novosibirsk
Asia/Phnom_Penh
Asia/Pyongyang
Asia/Qatar
Asia/Rangoon
Asia/Riyadh

Asia/Saigon
Asia/Seoul
Asia/Shanghai
Asia/Singapore
Asia/Taipei
Asia/Tashkent
Asia/Tbilisi
Asia/Tehran
Asia/Thimbu
Asia/Thimphu
Asia/Tokyo
Asia/Ujung_Pandang
Asia/Ulaanbaatar
Asia/Ulan_Bator
Asia/Vientiane
Asia/Vladivostok
Asia/Yakutsk
Asia/Yekaterinburg
Asia/Yerevan

Atlantic

Atlantic/Azores
Atlantic/Bermuda
Atlantic/Canary
Atlantic/Cape_Verde
Atlantic/Faeroe
Atlantic/Jan_Mayen
Atlantic/Reykjavik
Atlantic/South_Georgia
Atlantic/St_Helena
Atlantic/Stanley

Australia

Australia/Adelaide
Australia/Brisbane
Australia/Broken_Hill
Australia/Darwin
Australia/Hobart
Australia/Lord_Howe
Australia/Perth
Australia/Sydney

Europe

Europe/Amsterdam
Europe/Andorra
Europe/Athens
Europe/Belgrade
Europe/Berlin
Europe/Brussels
Europe/Bucharest
Europe/Budapest
Europe/Chisinau
Europe/Copenhagen
Europe/Dublin
Europe/Gibraltar
Europe/Helsinki
Europe/Istanbul
Europe/Kaliningrad
Europe/Kiev
Europe/Lisbon
Europe/London
Europe/Luxembourg
Europe/Madrid
Europe/Malta
Europe/Minsk
Europe/Monaco
Europe/Moscow
Europe/Oslo
Europe/Paris
Europe/Prague
Europe/Riga
Europe/Rome
Europe/Samara
Europe/Simferopol
Europe/Sofia
Europe/Stockholm
Europe/Tallinn
Europe/Tirane
Europe/Vaduz
Europe/Vienna
Europe/Vilnius
Europe/Warsaw
Europe/Zurich

Indian

Indian/Antananarivo
Indian/Chagos
Indian/Christmas
Indian/Cocos
Indian/Comoro
Indian/Kerguelen
Indian/Mahe
Indian/Maldives
Indian/Mauritius
Indian/Mayotte
Indian/Reunion

Pacific

Pacific/Apia
Pacific/Auckland
Pacific/Chatham
Pacific/Easter
Pacific/Efate
Pacific/Enderbury
Pacific/Fakaofu
Pacific/Fiji
Pacific/Funafuti
Pacific/Galapagos
Pacific/Gambier
Pacific/Guadalcanal
Pacific/Guam
Pacific/Honolulu
Pacific/Kiritimati
Pacific/Kosrae
Pacific/Majuro
Pacific/Marquesas
Pacific/Nauru
Pacific/Niue
Pacific/Norfolk
Pacific/Noumea
Pacific/Pago_Pago
Pacific/Palau
Pacific/Pitcairn
Pacific/Ponape
Pacific/Port_Moresby

```
Pacific/Rarotonga
Pacific/Saipan
Pacific/Tahiti
Pacific/Tarawa
Pacific/Tongatapu
Pacific/Truk
Pacific/Wake
Pacific/Wallis
```

<file extension>Non è possibile modificare il campo del suffisso tranne. Quando si abilita la conversione o la compressione del formato dei dati, Firehose aggiungerà un'estensione di file in base alla configurazione. La tabella seguente illustra l'estensione di file predefinita aggiunta da Firehose:

Configurazione	Estensione di file
Conversione del formato dei dati: Parquet	.parquet
Conversione del formato dei dati: ORC	.orc
Compressione: Gzip	.gz
Compressione: Zip	.zip
Compressione: Snappy	.snappy
Compressione: Hadoop-Snappy	.hsnappy

È inoltre possibile specificare l'estensione di file che si preferisce nella console o nell'API Firehose. L'estensione del file deve iniziare con un punto (.) e può contenere caratteri consentiti: 0-9a-z! -_.*' (). L'estensione del file non può superare i 128 caratteri.

Note

Quando si specifica un'estensione di file, questa sostituirà l'estensione di file predefinita aggiunta da Firehose [quando è abilitata la conversione o la compressione del formato dei dati](#).

Comprendi i prefissi personalizzati per gli oggetti Amazon S3

<evaluated prefix><suffix>Gli oggetti consegnati ad Amazon S3 seguono il [formato del nome](#) di. Puoi specificare il tuo prefisso personalizzato che include espressioni che vengono valutate in fase di esecuzione. Il prefisso personalizzato specificato sostituirà il prefisso predefinito di. yyyy/MM/dd/HH

Puoi utilizzare le seguenti forme di espressione nel prefisso personalizzato: `!{namespace: value}`, dove namespace può essere uno dei seguenti, come descritto nelle sezioni successive.

- `firehose`
- `timestamp`
- `partitionKeyFromQuery`
- `partitionKeyFromLambda`

Se un prefisso termina con una barra, viene visualizzato come cartella nel bucket Amazon S3. Per ulteriori informazioni, consulta [Amazon S3 Object Name Format](#) nella Amazon Data Firehose Developer Guide.

Spazio dei nomi **timestamp**

[I valori validi per questo spazio dei nomi sono stringhe che sono stringhe Java valide.](#)

[DateTimeFormatter](#) Ad esempio, nell'anno 2018, l'espressione `!{timestamp:yyyy}` restituisce 2018.

Durante la valutazione dei timestamp, Firehose utilizza il timestamp di arrivo approssimativo del record più vecchio contenuto nell'oggetto Amazon S3 in fase di scrittura.

Per impostazione predefinita, il timestamp è in UTC. Tuttavia, puoi specificare il fuso orario che preferisci. Ad esempio, puoi configurare il fuso orario in Console di gestione AWS o Asia/Tokyo nell'impostazione del parametro API ([CustomTimeZone](#)) se desideri utilizzare l'ora solare del

Giappone anziché l'UTC. Per visualizzare l'elenco dei fusi orari supportati, consulta [Amazon S3 Object Name](#) Format.

Se utilizzi lo spazio dei nomi `timestamp` più di una volta nella stessa espressione del prefisso, ogni istanza restituisce lo stesso istante temporale.

Spazio dei nomi **firehose**

Con questo spazio dei nomi puoi utilizzare due valori: `error-output-type` e `random-string`. La tabella seguente spiega come utilizzarli.

Valori dello spazio dei nomi **firehose**

Conversione	Description	Input di esempio	Output di esempio	Note
<code>error-output-type</code>	Restituisce una delle seguenti stringhe, a seconda della configurazione del flusso Firehose e del motivo dell'errore: <code>{processing-failed, AmazonOpenSearchService-failed, splunk-failed,,}</code> . <code>format-conversion-failed</code> <code>http-endpoint-failed</code>	<code>myPrefix/result={!{firehose:error-output-type}/!{timestamp:yyyy/MM/dd}}</code>	<code>myPrefix/result=processing-failed/2018/08/03</code>	Il valore può essere utilizzato solo nel campo <code>error-output-type</code> <code>ErrorOutputPrefix</code>
	Se lo utilizzi più di una volta nella stessa espressione, ogni istanza restituisce la			

Conversione	Description	Input di esempio	Output di esempio	Note
	stessa stringa di errore.			
random-string	Restituisce una stringa casuale di 11 caratteri. Se lo utilizzi più di una volta nella stessa espressione, ogni istanza restituisce una nuova stringa casuale.	myPrefix/! firehose:random-string}/	myPrefix/ 046b6c7f- 0b/	<p>Puoi utilizzarlo con entrambi i tipi di prefisso.</p> <p>Puoi posizionarlo all'inizio della stringa di formato per ottenere un prefisso randomizzato, che talvolta è necessario per ottenere una velocità di trasmissione effettiva estremamente elevata con Amazon S3.</p>

Spazi dei nomi `partitionKeyFromLambda` e `partitionKeyFromQuery`

Per il [partizionamento dinamico](#), è necessario utilizzare il seguente formato di espressione nel prefisso del bucket S3: `!{namespace:value}`, dove lo spazio dei nomi può essere `partitionKeyFromQuery` o `partitionKeyFromLambda` o entrambi. Se si utilizza l'analisi in linea per creare le chiavi di partizionamento per i dati di origine, è necessario specificare un valore del prefisso del bucket S3 costituito da espressioni specificate nel seguente formato: `"partitionKeyFromQuery:keyID"`. Se si utilizza una funzione AWS Lambda per creare chiavi di partizionamento per i dati di origine, è necessario specificare un valore di prefisso del bucket S3 costituito da espressioni specificate nel seguente formato: `"partitionKeyFromLambda:keyID"`.

Per ulteriori informazioni, consulta «Scegli Amazon S3 per la tua destinazione» in [Creazione di uno stream Amazon Firehose](#).

Regole semantiche

Le seguenti regole si applicano alle espressioni `Prefix` e `ErrorOutputPrefix`.

- Per lo spazio dei nomi `timestamp`, vengono restituiti tutti i caratteri che non sono tra virgolette singole. In altre parole, tutte le stringhe precedute da virgolette singole nel campo dei valori vengono prese alla lettera.
- Se si specifica un prefisso che non contiene un'espressione dello spazio dei nomi con `timestamp`, Firehose aggiunge l'espressione al valore nel `!{timestamp:yyyy/MM/dd/HH/}` campo. `Prefix`
- La sequenza `!{` può comparire solo nelle espressioni `!{namespace: value}`.
- `ErrorOutputPrefix` può essere null solo se `Prefix` non contiene espressioni. In questo caso, `Prefix` valuta `<specified-prefix>yyyy/MM/DDD/HH/` e `ErrorOutputPrefix` valuta `<specified-prefix><error-output-type>yyyy/MM/DDD/HH/`. DDD rappresenta il giorno dell'anno.
- Se specifichi un'espressione per `ErrorOutputPrefix`, devi includere almeno un'istanza di `!{firehose:error-output-type}`.
- `Prefix` non può contenere `!{firehose:error-output-type}`.
- Né `Prefix` né `ErrorOutputPrefix` possono contenere più di 512 dopo la restituzione.
- Se la destinazione è Amazon Redshift, `Prefix` non deve contenere espressioni e `ErrorOutputPrefix` deve essere null.
- Quando la destinazione è Amazon OpenSearch Service o Splunk e non `ErrorOutputPrefix` viene specificato alcun valore, Firehose utilizza `Prefix` il campo per i record non riusciti.
- Quando la destinazione è Amazon S3, `Prefix` e `ErrorOutputPrefix` nella configurazione di destinazione di Amazon S3 vengono utilizzati rispettivamente per record riusciti e record non riusciti. Con l'AWS CLI o l'API, puoi utilizzare `ExtendedS3DestinationConfiguration` per specificare una configurazione di backup di Amazon S3 con `Prefix` e `ErrorOutputPrefix`.
- Quando si utilizza Console di gestione AWS e si imposta la destinazione su Amazon S3, Firehose utilizza la `Prefix` e `ErrorOutputPrefix` nella configurazione di destinazione rispettivamente per i record riusciti e per i record con esito negativo. Se si specifica un prefisso utilizzando espressioni, è necessario specificare il prefisso di errore comprensivo di `!{firehose:error-output-type}`

- Quando si utilizza `ExtendedS3DestinationConfiguration` con AWS CLI, l'API o CloudFormation, se si specifica un `S3BackupConfiguration`, Firehose non fornisce un valore predefinito. `ErrorOutputPrefix`
- Non è possibile utilizzare gli `partitionKeyFromQuery` spazi `partitionKeyFromLambda` dei nomi and durante la creazione di espressioni. `ErrorOutputPrefix`

Esempi di prefisso

Esempi di **Prefix** e **ErrorOutputPrefix**

Input	Prefisso restituito (alle 10:30 UTC in data 27 ago 2018)
Prefix: non specificato ErrorOutputPrefix : myFirehoseFailures/!{firehose:error-output-type}/	Prefix: 2018/08/27/10 ErrorOutputPrefix : myFirehoseFailures/processing-failed/
Prefix: !{timestamp:yyyy/MM/dd} ErrorOutputPrefix : non specificato	Input non valido: ErrorOutputPrefix non può essere null se Prefix contiene espressioni
Prefix: myFirehose/DeliveredYear=!{timestamp:yyyy}/anyMonth/rand=!{firehose:random-string} ErrorOutputPrefix : myFirehoseFailures/!{firehose:error-output-type}/!{timestamp:yyyy}/anyMonth/!{timestamp:dd}	Prefix: myFirehose/DeliveredYear=2018/anyMonth/rand=5abf82daaa5 ErrorOutputPrefix : myFirehoseFailures/processing-failed/2018/anyMonth/10
Prefix: myPrefix/year=!{timestamp:yyyy}/month=!{timestamp:MM}/day=!{timestamp:dd}/hour=!{timestamp:HH}/ ErrorOutputPrefix : myErrorPrefix/year=!{timestamp:yyyy}/month=!	Prefix: myPrefix/year=2018/month=07/day=06/hour=23/ ErrorOutputPrefix : myErrorPrefix/year=2018/month=07/day=06/hour=23/processing-failed


Input	Prefisso restituito (alle 10:30 UTC in data 27 ago 2018)
<code>{timestamp:MM}/day=!{timestamp:dd}/hour=!{timestamp:HH}/!{firehose:error-output-type}</code>	
Prefix: myFirehosePrefix/ ErrorOutputPrefix : non specificato	Prefix: myFirehosePrefix/2018/08/27/ ErrorOutputPrefix : myFirehosePrefix/processing-failed/2018/08/27/

Configura la rotazione dell'indice per Service OpenSearch

Per la destinazione del OpenSearch servizio, è possibile specificare un'opzione di rotazione dell'indice basata sul tempo tra una delle cinque opzioni seguenti: NoRotation,, OneHour, OneDay o. OneWeek OneMonth

A seconda dell'opzione di rotazione scelta, Amazon Data Firehose aggiunge una parte del timestamp UTC di arrivo al nome di indice specificato. Ruota il timestamp aggiunto di conseguenza. L'esempio seguente mostra il nome dell'indice risultante in OpenSearch Service per ogni opzione di rotazione dell'indice, dove si trova il nome dell'indice specificato myindex e il timestamp di arrivo è. 2016-02-25T13:00:00Z

RotationPeriod	IndexName
NoRotation	myindex
OneHour	myindex-2016-02-25-13
OneDay	myindex-2016-02-25
OneWeek	myindex-2016-w08
OneMonth	myindex-2016-02


 Note

Con l'opzione OneWeek, Data Firehose crea automaticamente gli indici utilizzando il formato <YEAR>-w<WEEK NUMBER> (ad esempio, 2020-w33), in cui il numero della settimana viene calcolato utilizzando il tempo UTC e secondo le seguenti convenzioni statunitensi:

- Una settimana inizia di domenica
- La prima settimana dell'anno è la prima settimana che contiene un sabato dell'anno in corso

Sospendere e riprendere la consegna dei dati

Dopo aver configurato uno stream Firehose, i dati disponibili nella sorgente del flusso vengono continuamente consegnati alla destinazione. In situazioni in cui la destinazione del flusso è temporaneamente non disponibile (ad esempio, durante operazioni di manutenzione programmate), potresti voler sospendere temporaneamente la distribuzione dei dati e riprenderla quando la destinazione sarà nuovamente disponibile.

 Important

Quando utilizzi l'approccio descritto di seguito per mettere in pausa e riprendere uno stream, dopo averlo ripreso, vedrai che pochi record vengono consegnati al bucket di errori in Amazon S3 mentre il resto dello stream continua a essere recapitato alla destinazione. Questa è una limitazione nota dell'approccio e si verifica perché un numero limitato di record, che non era possibile consegnare in precedenza alla destinazione dopo più tentativi, vengono considerati falliti.

Mettere in pausa uno stream Firehose

Per sospendere la distribuzione dello stream in Firehose, rimuovete innanzitutto le autorizzazioni che consentono a Firehose di scrivere nella posizione di backup S3 per le consegne non riuscite. Ad esempio, se desideri mettere in pausa lo stream Firehose con OpenSearch una destinazione, puoi farlo aggiornando le autorizzazioni. Per ulteriori informazioni, vedere [Concedere a Firehose l'accesso a una destinazione di OpenSearch servizio pubblico](#).

Rimuovi l'autorizzazione "Effect": "Allow" per l'azione s3:PutObject e aggiungi esplicitamente un'istruzione che applichi l'autorizzazione Effect": "Deny" all'azione s3:PutObject per il bucket S3 utilizzato per il backup delle distribuzioni non riuscite. Quindi, disattiva la destinazione dello stream (ad esempio, disattivando il OpenSearch dominio di destinazione) o rimuovi le autorizzazioni per Firehose di scrivere nella destinazione. Per aggiornare le autorizzazioni per altre destinazioni, consulta la sezione relativa alla tua destinazione in [Controlling Access with Amazon Data Firehose](#). Dopo aver completato queste due azioni, Firehose interromperà la distribuzione degli stream e potrai monitorarla utilizzando le [CloudWatch metriche](#) per Firehose.

Important

Quando si sospende la distribuzione dello stream in Firehose, è necessario assicurarsi che l'origine dello stream (ad esempio, in Kinesis Data Streams o in Managed Service for Kafka) sia configurata per conservare i dati fino alla ripresa della distribuzione dello stream e alla consegna dei dati alla destinazione. Se la fonte è DirectPut, Firehose conserverà i dati per 24 ore. Se la distribuzione del flusso non riprende e i dati non vengono distribuiti prima della scadenza del periodo di conservazione dei dati, potrebbe verificarsi una perdita di dati.

Riprendere uno stream Firehose

Per riprendere la consegna, ripristina innanzitutto la modifica apportata in precedenza alla destinazione dello stream attivando la destinazione e assicurandoti che Firehose disponga delle autorizzazioni per consegnare lo stream alla destinazione. Successivamente, ripristina le modifiche apportate in precedenza alle autorizzazioni applicate al bucket S3 per il backup delle distribuzioni non riuscite. Vale a dire, applica l'autorizzazione "Effect": "Allow" per l'azione s3:PutObject e rimuovi l'autorizzazione "Effect": "Deny" sull'azione s3:PutObject per il bucket S3 utilizzato per il backup delle distribuzioni non riuscite. Infine, monitorate utilizzando le [CloudWatch metriche di Firehose per](#) confermare che lo stream venga recapitato alla destinazione. Per visualizzare e risolvere gli errori, usa il monitoraggio di [Amazon CloudWatch Logs per](#) Firehose.

Distribuisci dati ad Apache Iceberg Tables con Amazon Data Firehose

Apache Iceberg è un formato di tabella open source ad alte prestazioni per eseguire analisi di big data. Apache Iceberg porta l'affidabilità e la semplicità delle tabelle SQL nei data lake Amazon S3 e consente a motori di analisi open source come Spark, Flink, Trino, Hive e Impala di lavorare con gli stessi dati contemporaneamente. Per [ulteriori](#) informazioni, consulta Apache Iceberg e.

[Considerazioni e limitazioni](#)

Puoi usare Firehose per distribuire dati in streaming a Apache Iceberg Tables in Amazon S3. Le tabelle Apache Iceberg possono essere gestite autonomamente in Amazon S3 o ospitate in Amazon S3 Tables. Nelle tabelle Iceberg autogestite, gestisci tutte le ottimizzazioni delle tabelle, come la compattazione e la scadenza degli snapshot. Le tabelle Amazon S3 forniscono uno storage ottimizzato per carichi di lavoro di analisi su larga scala, con funzionalità che migliorano continuamente le prestazioni delle query e riducono i costi di storage per i dati tabulari. Per ulteriori informazioni su Amazon S3 Tables, consulta [Amazon S3 Tables](#).

Questa funzionalità consente di indirizzare i record da un singolo flusso a diverse tabelle Apache Iceberg. È possibile applicare automaticamente le operazioni di inserimento, aggiornamento ed eliminazione ai record in tali tabelle. Supporta inoltre un controllo granulare dell'accesso ai dati sulle tabelle Apache Iceberg in Amazon S3 con AWS Lake Formation. È possibile specificare i controlli di accesso centralmente AWS Lake Formation e fornire autorizzazioni più granulari a livello di tabella e colonna per Firehose.

Considerazioni e limitazioni

Note

Firehose supporta Apache Iceberg Tables come destinazione in tutte le regioni tranne [Regioni AWS](#) Cina AWS GovCloud (US) Regions, Asia Pacifico (Taipei), Asia Pacifico (Malesia), Asia Pacifico (Nuova Zelanda) e Messico (Centrale).

Il supporto di Firehose per le tabelle Apache Iceberg presenta le seguenti considerazioni e limitazioni.

- Throughput: se utilizzi Direct PUT come fonte per fornire dati alle tabelle Apache Iceberg, la velocità effettiva massima per flusso è 5 MiB/second nelle regioni Stati Uniti orientali (Virginia

settentrionale), Stati Uniti occidentali (Oregon) ed Europa (Irlanda) e 1 in tutte le altre. MiB/second Regioni AWS Se desideri inserire dati nelle tabelle Iceberg senza aggiornamenti ed eliminazioni e desideri un throughput più elevato per il tuo stream, puoi utilizzare il [modulo Firehose Limits per richiedere un aumento del limite](#) di throughput.

Puoi anche impostare il `AppendOnly` flag su `True` se desideri solo inserire dati e non eseguire aggiornamenti ed eliminazioni. Impostando il `AppendOnly` flag su `True`, Firehose si ridimensiona automaticamente in base alla velocità effettiva. Attualmente, è possibile impostare questo flag solo con l'[CreateDeliveryStream](#) operazione API.

Se uno stream Direct PUT subisce una limitazione a causa di volumi di acquisizione dati più elevati che superano la capacità di throughput di uno stream Firehose, Firehose aumenta automaticamente il limite di throughput dello stream fino a contenere la limitazione. A seconda dell'aumento del throughput e del throttling, Firehose potrebbe impiegare più tempo per aumentare la velocità di trasmissione di uno stream ai livelli desiderati. Per questo motivo, continua a riprovare i record di acquisizione dei dati non riusciti. Se prevedi che il volume di dati aumenti in caso di picchi improvvisi di grandi dimensioni o se il tuo nuovo stream richiede una velocità di trasmissione superiore al limite di throughput predefinito, richiedi di aumentare il limite di throughput.

- **S3 Transaction Per Second (TPS):** per ottimizzare le prestazioni di S3, se utilizzi Kinesis Data Streams o Amazon MSK come origine, ti consigliamo di partizionare il record di origine utilizzando una chiave di partizione appropriata. In questo modo, i record di dati che vengono indirizzati alla stessa tabella Iceberg vengono mappati su una o più partizioni di origine note come shard. Se possibile, distribuisce i record di dati appartenenti a diverse tabelle Iceberg di destinazione in diverse. `partitions/shards`, so that you can use all the aggregate throughput available across all the `partitions/shards` of the source topic/stream
- **Colonne:** per i nomi e i valori delle colonne, Firehose utilizza solo il primo livello di nodi in un JSON annidato a più livelli. Ad esempio, Firehose seleziona i nodi disponibili nel primo livello, incluso il campo di posizione. Affinché Firehose fornisca correttamente i nomi delle colonne e i tipi di dati di origine devono corrispondere esattamente a quelli delle tabelle di destinazione. In questo caso, Firehose prevede che nelle tabelle Iceberg sia presente una colonna del tipo di dati `struct` o `map` che corrisponda al campo di posizione. Firehose supporta 16 livelli di nidificazione. Di seguito è riportato un esempio di JSON annidato.

```
{
  "version": "2016-04-01",
  "deviceId": "<solution_unique_device_id>",
  "sensorId": "<device_sensor_id>",
  "timestamp": "2024-01-11T20:42:45.000Z",
```

```
"value": "<actual_value>",
"position": {
  "x": 143.595901,
  "y": 476.399628,
  "z": 0.24234876
}
```

Se i nomi delle colonne o i tipi di dati non corrispondono, Firehose genera un errore e invia i dati al bucket di errore S3. Se tutti i nomi delle colonne e i tipi di dati corrispondono nelle tabelle di Apache Iceberg, ma nel record di origine è presente un campo aggiuntivo, Firehose salta il nuovo campo.

- Un oggetto JSON per record: è possibile inviare solo un oggetto JSON in un record Firehose. Se aggregate e inviate più oggetti JSON all'interno di un record, Firehose genera un errore e invia i dati al bucket di errore S3. Se si aggregano record con [KPL](#) e si inseriscono dati in Firehose con Amazon Kinesis Data Streams come origine, Firehose si disaggrega automaticamente e utilizza un oggetto JSON per record.
- Ottimizzazione della compattazione e dello storage: ogni volta che scrivi su Iceberg Tables utilizzando Firehose, esegue il commit e genera istantanee, file di dati e file eliminati. La presenza di molti file di dati aumenta il sovraccarico dei metadati e influisce sulle prestazioni di lettura. Per ottenere prestazioni di query efficienti, potresti prendere in considerazione una soluzione che acquisisca periodicamente file di dati di piccole dimensioni e li riscriva in file di dati di dimensioni inferiori. Questo processo si chiama compattazione. AWS Glue Data Catalog supporta la compattazione automatica delle tabelle Apache Iceberg. Per ulteriori informazioni, consulta la sezione [Gestione della compattazione](#) nella AWS Glue User Guide. Per ulteriori informazioni, consulta [Compattazione automatica delle tabelle Apache Iceberg](#). In alternativa, è possibile eseguire il comando Athena Optimize per eseguire la compattazione manualmente. Per ulteriori informazioni sul comando Optimize, vedere [Athena Optimize](#).

Oltre alla compattazione dei file di dati, è possibile ottimizzare il consumo di storage anche con l'istruzione [VACUUM](#) che esegue la manutenzione delle tabelle sulle tabelle Apache Iceberg, ad esempio la scadenza delle istantanee e la rimozione dei file orfani. In alternativa, è possibile utilizzarlo per supportare anche l'ottimizzazione gestita delle tabelle di AWS Glue Data Catalog Apache Iceberg rimuovendo automaticamente i file di dati, i file orfani e le istantanee con scadenza che non sono più necessarie. Per ulteriori informazioni, consulta questo post di blog sull'[ottimizzazione dello storage](#) delle tabelle Apache Iceberg.

- Non supportiamo il codice sorgente Amazon MSK Serverless per Apache Iceberg Tables come destinazione.

- Per un'operazione di aggiornamento, Firehose inserisce un file di eliminazione seguito da un'operazione di inserimento. L'inserimento di file eliminati comporta i costi di invio di Amazon S3.
- Firehose non consiglia di utilizzare più flussi Firehose per scrivere dati sulla stessa tabella Apache Iceberg. [Questo perché Apache Iceberg si affida all'Optimistic Concurrency Control \(OCC\)](#). Se più stream Firehose tentano di scrivere contemporaneamente su una singola tabella Iceberg, solo uno stream riesce a salvare i dati alla volta. Gli altri stream che non riescono a eseguire il commit si disattivano e riprovano a eseguire l'operazione di commit fino alla scadenza della durata del tentativo configurata. Una volta esaurita la durata del nuovo tentativo, i dati e le chiavi di eliminazione dei file (percorsi Amazon S3) vengono inviati al prefisso di errore Amazon S3 configurato.
- L'attuale versione di Iceberg Library supportata da Firehose è la versione 1.5.2.
- Per distribuire dati crittografati a Amazon S3 Tables, è necessario configurare AWS Key Management Service i parametri in Amazon S3 Tables e non nella configurazione Firehose. Se si configurano AWS Key Management Service i parametri in Firehose per la distribuzione di dati crittografati alle tabelle Amazon S3, Firehose non può utilizzare tali parametri per crittografare. Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con chiavi](#). AWS KMS
- Gli stream Firehose supportano solo la distribuzione a database e tabelle creati tramite l'API di Iceberg. GlueCatalog La consegna a database e tabelle creati tramite Glue SDK non è supportata. Nota che il trattino (-) non è un carattere supportato per il database e il nome della tabella nella libreria Iceberg. Per maggiori dettagli, vedi [Glue Database Regex](#) e [Glue Table Regex](#) supportati dalla libreria Iceberg.
- Tutti i file scritti da Firehose vengono calcolati utilizzando la partizione presente nel record. Questo vale anche per i file eliminati. Le eliminazioni globali, come la scrittura di file di eliminazione non partizionati per una tabella partizionata, non sono supportate.

Prerequisiti per utilizzare Apache Iceberg Tables come destinazione

Scegliete tra le seguenti opzioni per completare i prerequisiti richiesti.

Argomenti

- [Prerequisiti per la consegna a Iceberg Tables in Amazon S3](#)
- [Prerequisiti per la distribuzione su Amazon S3 Tables](#)

Prerequisiti per la consegna a Iceberg Tables in Amazon S3

Prima di iniziare, completa i seguenti prerequisiti.

- Crea un bucket Amazon S3: devi creare un bucket Amazon S3 per aggiungere il percorso del file di metadati durante la creazione delle tabelle. [Per ulteriori informazioni, consulta Creare un bucket S3.](#)
- Crea un ruolo IAM con le autorizzazioni richieste: Firehose necessita di un ruolo IAM con autorizzazioni specifiche per AWS Glue accedere alle tabelle e scrivere dati su Amazon S3. Lo stesso ruolo viene utilizzato per concedere AWS Glue l'accesso ai bucket Amazon S3. È necessario questo ruolo IAM quando si crea una tabella Iceberg e uno stream Firehose. Per ulteriori informazioni, consulta [Concedi a Firehose l'accesso alle tabelle Amazon S3.](#)
- Creazione di tabelle Apache Iceberg: se si configurano chiavi univoche nel flusso Firehose per aggiornamenti ed eliminazioni, Firehose verifica se la tabella e le chiavi uniche esistono come parte della creazione dello stream. In questo scenario, è necessario creare tabelle prima di creare il flusso Firehose. È possibile utilizzare AWS Glue per creare tabelle Apache Iceberg. Per ulteriori informazioni, consulta [Creazione di tabelle Apache Iceberg.](#) Se non si configurano chiavi univoche nello stream Firehose, non è necessario creare tabelle Iceberg prima di creare uno stream Firehose.

Note

Firehose supporta la versione e il formato di tabella seguenti per le tabelle Apache Iceberg.

- Versione in formato tabella: Firehose supporta solo il formato tabella [V2](#). Non create tabelle in formato V1, altrimenti si verifica un errore e i dati vengono invece inviati al bucket di errore S3.
- Formato di archiviazione dati: Firehose scrive i dati su Apache Iceberg Tables in formato Parquet.
- Funzionamento a livello di riga: Firehose supporta la modalità Merge-on-Read (MOR) di scrittura dei dati su Apache Iceberg Tables.

Prerequisiti per la distribuzione su Amazon S3 Tables

Per fornire dati ai bucket da tabella Amazon S3, completa i seguenti prerequisiti.

- Crea un bucket S3 Table, un namespace, tabelle nel table bucket e altri passaggi di integrazione descritti in Guida introduttiva [ad Amazon S3 Tables](#). [I nomi delle colonne devono essere in minuscolo a causa delle limitazioni imposte dall'integrazione del catalogo S3 Tables, come specificato nelle limitazioni di integrazione del catalogo di tabelle S3](#).
- Crea un ruolo IAM con le autorizzazioni richieste: Firehose necessita di un ruolo IAM con autorizzazioni specifiche per AWS AWS Glue accedere alle tabelle e scrivere dati nelle tabelle in un bucket di tabelle Amazon S3. Per scrivere su tabelle in un bucket di tabelle Amazon S3, devi anche fornire al ruolo IAM le autorizzazioni richieste. Le autorizzazioni richieste per il catalogo Amazon S3 Tables dipendono dalla modalità di controllo degli accessi utilizzata:
 - Controllo degli accessi IAM: il ruolo di consegna Firehose richiede le autorizzazioni IAM direttamente sulle risorse di Amazon S3 Tables.
 - Controllo degli accessi a Lake Formation: il ruolo di consegna Firehose richiede le AWS Lake Formation autorizzazioni per gestire l'accesso alle risorse della tabella. AWS Lake Formation utilizza il proprio modello di autorizzazioni che consente un controllo granulare degli accessi per le risorse del Data Catalog.

Questo ruolo IAM viene configurato quando si crea uno stream Firehose. Per ulteriori informazioni, consulta [Concedere a Firehose l'accesso alle tabelle Amazon S3](#).

Per step-by-step l'integrazione, consulta il blog [Crea un data lake per lo streaming di dati con Amazon S3 Tables e Amazon Data Firehose](#). Per ulteriori informazioni, consulta anche [Using Amazon S3 Tables with AWS analytics services](#).

Configurare lo stream Firehose

Per creare uno stream Firehose con Apache Iceberg Tables come destinazione, è necessario configurare quanto segue.

Note

La configurazione di uno stream Firehose per la distribuzione alle tabelle nei bucket di tabelle S3 è la stessa di Apache Iceberg Tables in Amazon S3.

Configurazione dell'origine e della destinazione

Per inviare dati ad Apache Iceberg Tables, scegli la fonte per il tuo stream.

Per configurare la fonte per lo streaming, consulta [Configurare le impostazioni della sorgente](#).

Quindi, scegli Apache Iceberg Tables come destinazione e fornisci un nome di stream Firehose.

Configura la trasformazione dei dati

Per eseguire trasformazioni personalizzate sui dati, come aggiungere o modificare record nel flusso in entrata, è possibile aggiungere una funzione Lambda allo stream Firehose. Per ulteriori informazioni sulla trasformazione dei dati utilizzando Lambda in uno stream Firehose, vedere.

[Trasforma i dati di origine in Amazon Data Firehose](#)

Per Apache Iceberg Tables, è necessario specificare come si desidera indirizzare i record in entrata verso diverse tabelle di destinazione e le operazioni che si desidera eseguire. Uno dei modi per fornire le informazioni di routing richieste a Firehose consiste nell'utilizzare una funzione Lambda.

Per ulteriori informazioni, consulta [Instradare i record verso diverse](#) tabelle Iceberg.

Connect data catalog

Apache Iceberg richiede un catalogo di dati per scrivere su Apache Iceberg Tables. Firehose si integra con Apache Iceberg AWS Glue Data Catalog Tables.

È possibile AWS Glue Data Catalog utilizzarlo nello stesso account dello stream Firehose o in un account multiplo e nella stessa regione dello stream Firehose (impostazione predefinita) o in una regione diversa.

Se effettui la consegna su un tavolo Amazon S3 e utilizzi la console per configurare lo stream Firehose, seleziona il catalogo che corrisponde al tuo catalogo di tabelle Amazon S3. Se si utilizza la CLI per configurare lo stream Firehose, nell'`CatalogConfigurationInput`, utilizzare `CatalogARN` con il formato: `arn:aws:glue:<region>:<account-id>:catalog/s3tablescatalog/<s3 table bucket name>` Per ulteriori informazioni, consulta [Configurazione di un flusso Firehose sulle tabelle Amazon S3](#).

Note

Firehose supporta tre operazioni per le tabelle Iceberg: inserimento, aggiornamento ed eliminazione. Senza un'operazione specificata, Firehose utilizza come impostazione predefinita l'inserimento, l'aggiunta di ogni record in entrata come nuova riga e la conservazione dei duplicati. Per modificare invece i record esistenti, specifica l'operazione «update», che utilizza le chiavi primarie per individuare e modificare le righe esistenti.

Esempio:

- Predefinito (inserimento): più record di clienti identici creano righe duplicate.
- Aggiornamento specificato: il nuovo indirizzo del cliente aggiorna il record esistente.

Configura le espressioni JQ

Per le tabelle Apache Iceberg, è necessario specificare come si desidera indirizzare i record in entrata a diverse tabelle di destinazione e le operazioni come inserimento, aggiornamento ed eliminazione che si desidera eseguire. È possibile farlo configurando le espressioni JQ in modo che Firehose analizzi e ottenga le informazioni richieste. Per ulteriori informazioni, consulta [???](#).

Configura chiavi univoche

Aggiornamenti ed eliminazioni con più di una tabella: le chiavi univoche sono uno o più campi nel record di origine che identificano in modo univoco una riga nelle tabelle Apache Iceberg. Se è stato impostato lo scenario Insert Only con più di una tabella, non è necessario configurare chiavi univoche. Se desideri eseguire aggiornamenti ed eliminazioni su determinate tabelle, devi configurare chiavi univoche per quelle tabelle richieste. Tieni presente che l'aggiornamento inserirà automaticamente la riga se manca la riga nelle tabelle. Se hai una sola tabella, puoi configurare chiavi univoche. Per un'operazione di aggiornamento, Firehose inserisce un file di eliminazione seguito da un inserto.

[È possibile configurare chiavi univoche per tabella come parte della creazione del flusso Firehose oppure impostarle identifier-field-ids nativamente in Iceberg durante l'operazione di creazione della tabella o di modifica della tabella.](#) La configurazione di chiavi univoche per tabella durante la creazione dello stream è facoltativa. Se non configuri chiavi univoche per tabella durante la creazione dello stream, Firehose verifica le tabelle `identifier-field-ids` richieste e le utilizzerà come chiavi univoche. Se entrambe non sono configurate, la consegna dei dati con le operazioni di aggiornamento ed eliminazione fallisce.

Per configurare questa sezione, fornisci il nome del database, il nome della tabella e le chiavi univoche per le tabelle in cui desideri aggiornare o eliminare i dati. È possibile avere solo voci per ogni tabella nella configurazione. Non è necessario configurare questa sezione per gli scenari di sola aggiunta. Facoltativamente, puoi anche scegliere di fornire un prefisso Error Bucket se i dati della tabella non vengono forniti, come illustrato nell'esempio seguente.

```
[
```

```

{
  "DestinationDatabaseName": "MySampleDatabase",
  "DestinationTableName": "MySampleTable",
  "UniqueKeys": [
    "COLUMN_PLACEHOLDER"
  ],
  "S3ErrorOutputPrefix": "OPTIONAL_PREFIX_PLACEHOLDER"
}
]

```

Firehose supporta la configurazione di chiavi univoche se il nome di colonna fornito è univoco nell'intera tabella. Tuttavia, non supporta nomi di colonna completi come chiavi univoche. Ad esempio, una chiave denominata `top._id` è considerata una chiave univoca se il nome della colonna `_id` è presente anche al livello superiore. Se `_id` è univoca nell'intera tabella, viene utilizzata indipendentemente dalla sua posizione all'interno della struttura della tabella. A prescindere dal fatto che si tratti di una colonna di primo livello o di una colonna annidata. Nell'esempio seguente, `_id` è una chiave univoca valida per lo schema perché il nome della colonna è univoco in tutto lo schema.

```

[
  "schema": {
    "type": "struct",
    "fields": [
      {
        "name": "top",
        "type": {
          "type": "struct",
          "fields": [
            { "name": "_id", "type": "string" },
            { "name": "name", "type": "string" }
          ]
        }
      },
      { "name": "user", "type": "string" }
    ]
  }
]

```

Nell'esempio seguente, `non_id` è una chiave univoca valida per lo schema perché viene utilizzata sia nella colonna di primo livello che nella struttura annidata.

```
[
  "schema": {
    "type": "struct",
    "fields": [
      {
        "name": "top",
        "type": {
          "type": "struct",
          "fields": [
            { "name": "_id", "type": "string" },
            { "name": "name", "type": "string" }
          ]
        }
      },
      { "name": "_id", "type": "string" }
    ]
  }
]
```

Specificare la durata del nuovo tentativo

È possibile utilizzare questa configurazione per specificare la durata in secondi per cui Firehose deve tentare di riprovare, se riscontra errori nella scrittura su Apache Iceberg Tables in Amazon S3. È possibile impostare qualsiasi valore compreso tra 0 e 7200 secondi per eseguire nuovi tentativi. Per impostazione predefinita, Firehose riprova per 300 secondi.

Gestire la consegna o l'elaborazione non riuscite

È necessario configurare Firehose per inviare i record a un bucket di backup S3 nel caso in cui si verifichino errori nell'elaborazione o nella consegna di uno stream dopo la scadenza della durata dei nuovi tentativi. Per questo, configura il prefisso di output dell'errore del bucket di backup S3 e del bucket di backup S3 dalle impostazioni di backup nella console.

Handle errors

Firehose invia tutti gli errori di consegna ai CloudWatch log e ai bucket di errore Amazon S3.

Elenco degli errori:

Messaggio di errore	Descrizione
<code>Iceberg.NoSuchTable</code>	Firehose sta scrivendo su una tabella che non esiste oppure la tabella non è in formato V2. Firehose non supporta le tabelle in formato V1.
<code>Iceberg.InvalidTableName</code>	Viene passato un nome di tabella vuoto o nullo oppure la tabella non è in formato V2. Firehose non supporta le tabelle in formato V1.
<code>S3.AccessDenied</code>	Assicurati che il ruolo IAM creato nella fase dei prerequisiti disponga delle autorizzazioni e della policy di fiducia richieste.
<code>Glue.AccessDenied</code>	Assicurati che il ruolo IAM creato nella fase dei prerequisiti disponga delle autorizzazioni e della policy di fiducia richieste.

Configura i buffer hint

Firehose memorizza i dati di streaming in entrata in memoria fino a una certa dimensione (dimensione del buffering) e per un determinato periodo di tempo (intervallo di buffering) prima di consegnarli ad Apache Iceberg Tables. È possibile scegliere una dimensione del buffer compresa tra 1 e 128 e un intervallo di buffer compreso tra 0 e 900 secondi. MiBs Un buffer hint più elevato si traduce in un numero inferiore di scritture S3, in un minor costo di compattazione grazie a file di dati più grandi e in un tempo di esecuzione delle query più rapido, ma con una latenza più elevata. Valori di buffer hint inferiori forniscono i dati con una latenza inferiore.

Configurare le impostazioni avanzate

Puoi configurare la crittografia lato server, la registrazione degli errori, le autorizzazioni e i tag per le tue tabelle Apache Iceberg. Per ulteriori informazioni, consulta [Configurare le impostazioni avanzate](#). Devi aggiungere il ruolo IAM che hai creato come parte di [???](#) Firehose assumerà il ruolo di accedere alle AWS Glue tabelle e scrivere nei bucket Amazon S3.

Il completamento della creazione di stream Firehose può richiedere diversi minuti. Dopo aver creato con successo lo stream Firehose, è possibile iniziare a importare dati al suo interno e visualizzare i dati nelle tabelle di Apache Iceberg.

Indirizza i record in entrata a una singola tabella Iceberg

Se desideri che Firehose inserisca dati in una singola tabella Iceberg, configura semplicemente un singolo database e una singola tabella nella configurazione dello stream, come mostrato nell'esempio JSON seguente. Per una singola tabella, non sono necessarie l'espressione JQ e la funzione Lambda per fornire le informazioni di routing a Firehose. Se fornisci questi campi insieme a JQ o Lambda, Firehose riceverà input da JQ o Lambda.

```
[
  {
    "DestinationDatabaseName": "UserEvents",
    "DestinationTableName": "customer_id",
    "UniqueKeys": [
      "COLUMN_PLACEHOLDER"
    ],
    "S3ErrorOutputPrefix": "OPTIONAL_PREFIX_PLACEHOLDER"
  }
]
```

In questo esempio, Firehose indirizza tutti i record di input alla `customer_id` tabella del database. `UserEvents` Se si desidera eseguire operazioni di aggiornamento o eliminazione su una singola tabella, è necessario fornire l'operazione per ogni record in entrata a Firehose utilizzando il metodo [JSONQuery](#) il metodo [Lambda](#).

Indirizza i record in entrata a diverse tabelle Iceberg

Amazon Data Firehose può indirizzare i record in entrata in un flusso verso diverse tabelle Iceberg in base al contenuto del record. I registri non vengono mantenuti in ordine quando vengono consegnati da Amazon Data Firehose. Considera il seguente record di input di esempio.

```
{
  "deviceId": "Device1234",
  "timestamp": "2024-11-28T11:30:00Z",
  "data": {
    "temperature": 21.5,
    "location": {
      "latitude": 37.3324,
      "longitude": -122.0311
    }
  }
}
```

```
},
"powerlevel": 84,
"status": "online"
}
```

```
{
  "deviceId": "Device4567",
  "timestamp": "2023-11-28T10:40:00Z",
  "data": {
    "pressure": 1012.4,
    "location": {
      "zipcode": 24567
    }
  },
  "powerlevel": 82,
  "status": "online"
}
```

In questo esempio, il **deviceId** campo ha due valori possibili: Device1234 e Device4567. Quando un record in entrata ha il **deviceId** campo asDevice1234, vogliamo scrivere il record in una tabella Iceberg denominata Device1234, e quando un record in entrata ha il **deviceId** campo asDevice4567, vogliamo scrivere il record in una tabella denominata. Device4567

Nota che i record con Device1234 e Device4567 potrebbero avere un set diverso di campi mappati a colonne diverse nella tabella Iceberg corrispondente. I record in entrata potrebbero avere una struttura JSON annidata in cui **deviceId** possono essere annidati all'interno del record JSON. Nelle prossime sezioni, discuteremo di come indirizzare i record a tabelle diverse fornendo le informazioni di routing appropriate a Firehose in tali scenari.

Fornire informazioni di routing a JSONQuery Firehose con espressione

Il modo più semplice ed economico per fornire informazioni sul routing dei record a Firehose è fornire JSONQuery un'espressione. Con questo approccio, si forniscono JSONQuery espressioni per tre parametri: Database NameTable Name, e (facoltativamente). Operation Firehose utilizza l'espressione fornita dall'utente per estrarre informazioni dai record dei flussi in entrata per instradare i record.

Il Database Name parametro specifica il nome del database di destinazione. Il Table Name parametro specifica il nome della tabella di destinazione. Operation è un parametro opzionale che indica se inserire il record dello stream in entrata come nuovo record nella tabella di destinazione o

modificare o eliminare un record esistente nella tabella di destinazione. Il campo `Operazione` deve avere uno dei seguenti valori: `insert`, `update`, o `delete`.

Per ognuno di questi tre parametri, è possibile fornire un valore statico o un'espressione dinamica in cui il valore viene recuperato dal record in entrata. Ad esempio, se si desidera inviare tutti i record di flusso in entrata a un unico database denominato `IoTeEvents`, il nome del database avrà un valore statico di `"IoTeEvents"`. Se il nome della tabella di destinazione deve essere ottenuto da un campo del record in entrata, il nome della tabella è un'espressione dinamica che specifica il campo nel record in entrata da cui deve essere recuperato il nome della tabella di destinazione.

Nell'esempio seguente, utilizziamo un valore statico per `Database Name`, un valore dinamico per `Table Name` e un valore statico per l'operazione. Si noti che la specificazione dell'operazione è facoltativa. Se non viene specificata alcuna operazione, Firehose inserisce i record in entrata nella tabella di destinazione come nuovi record per impostazione predefinita.

```
Database Name : "IoTeEvents"  
Table Name : .deviceId  
Operation : "insert"
```

Se il `deviceId` campo è nidificato all'interno del record JSON, specifichiamo `Table Name` con le informazioni sul campo nidificato come `.event.deviceId`

Note

- Quando si specifica l'operazione come `update` o `delete`, è necessario specificare chiavi univoche per la tabella di destinazione quando si imposta il flusso Firehose o impostarle [identifier-field-ids](#) in Iceberg quando si eseguono le operazioni di [creazione tabella o modifica tabella](#) in Iceberg. Se non lo specifichi, Firehose genera un errore e invia i dati a un bucket di errore S3.
- I `Table Name`, `Database Name` and devono corrispondere esattamente ai nomi delle tabelle e del database di destinazione. Se non corrispondono, Firehose genera un errore e invia i dati a un bucket di errore S3.

Fornisci informazioni di routing utilizzando una funzione AWS Lambda

Potrebbero esserci scenari in cui sono presenti regole complesse che determinano come indirizzare i record in entrata a una tabella di destinazione. Ad esempio, potresti avere una regola che definisce

se un campo contiene il valore A, B o F, che deve essere indirizzato a una tabella di destinazione denominata `TableX` oppure potresti voler aumentare il record dello stream in entrata aggiungendo attributi aggiuntivi. Ad esempio, se un record contiene un campo `device_id` come 1, potresti voler aggiungere un altro campo `device_type` come «modem» e scrivere il campo aggiuntivo nella colonna della tabella di destinazione. In questi casi, è possibile trasformare il flusso di origine utilizzando una AWS Lambda funzione in Firehose e fornire informazioni di routing come parte dell'output della funzione di trasformazione Lambda. Per capire come trasformare il flusso di origine utilizzando una AWS Lambda funzione in Firehose, consulta [Trasformare i dati di origine in Amazon Data Firehose](#).

Quando si utilizza Lambda per la trasformazione di un flusso di origine in Firehose, l'output deve contenere e o `recordId` `parametriresult`. `data` `KafkaRecordValue` Il parametro `recordId` contiene il record del flusso di input, `result` indica se la trasformazione ha avuto successo e `data` contiene l'output trasformato con codifica Base64 della funzione Lambda. Per ulteriori informazioni, consulta [???](#).

```
{
  "recordId": "49655962066601463032522589543535113056108699331451682818000000",
  "result": "Ok",
  "data": "1IiwiI6ICJmYWxsIiwgImdgU21IiwiI6ICJmYWxsIiwg==tcHV0ZXIgdU2NpZW5jZSIzZW11"
}
```

Per specificare a Firehose informazioni di routing su come indirizzare il record dello stream a una tabella di destinazione come parte della funzione Lambda, l'output della funzione Lambda deve contenere una sezione aggiuntiva per `metadata`. L'esempio seguente mostra come la sezione dei metadati viene aggiunta all'output Lambda per un flusso Firehose che utilizza Kinesis Data Streams come origine dati per indicare a Firehose che deve inserire il record come nuovo record nella tabella denominata `Device1234` `IoTevents`

```
{
  "recordId": "49655962066601463032522589543535113056108699331451682818000000",
  "result": "Ok",
  "data":
    "1IiwiI6ICJmYWxsIiwgImdgU21IiwiI6ICJmYWxsIiwg==tcHV0ZXIgdU2NpZW5jZSIzZW11",

  "metadata":{
    "otfMetadata":{
      "destinationTableName":"Device1234",
      "destinationDatabaseName":"IoTevents",
      "operation":"insert"
    }
  }
}
```

```

    }
  }
}

```

Analogamente, l'esempio seguente mostra come aggiungere la sezione dei metadati all'output Lambda per un Firehose che utilizza Amazon Managed Streaming for Apache Kafka come origine dati per indicare a Firehose che deve inserire il record come nuovo record in una tabella denominata nel database. Device1234 IoTevents

```

{
  "recordId": "49655962066601463032522589543535113056108699331451682818000000",
  "result": "Ok",
  "kafkaRecordValue":
  "1IiwiI6ICJmYwxsIiwgImdgU21IiwiI6ICJmYwxsIiwg==tcHV0ZXIgaU2NpZW5jZSIzICJzZW1",

  "metadata":{
  "otfMetadata":{
    "destinationTableName":"Device1234",
    "destinationDatabaseName":"IoTevents",
    "operation":"insert"
  }
}
}
}

```

Per questo esempio,

- `destinationDatabaseName` si riferisce al nome del database di destinazione ed è un campo obbligatorio.
- `destinationTableName` si riferisce al nome della tabella di destinazione ed è un campo obbligatorio.
- `operation` è un campo opzionale con valori possibili come `insert`, `update`, ed `delete`. Se non si specifica alcun valore, l'operazione predefinita è `insert`.

Note

- Quando si specifica l'operazione come `update` o `delete`, è necessario specificare chiavi univoche per la tabella di destinazione quando si imposta il flusso Firehose o impostarle [identifier-field-ids](#) in Iceberg quando si eseguono le operazioni di [creazione tabella o](#)

[modifica tabella](#) in Iceberg. Se non lo specifichi, Firehose genera un errore e invia i dati a un bucket di errore S3.

- I `Table Name` valori `Database Name` and devono corrispondere esattamente ai nomi delle tabelle e del database di destinazione. Se non corrispondono, Firehose genera un errore e invia i dati a un bucket di errore S3.
- Quando il flusso Firehose ha sia una funzione di trasformazione Lambda che un'espressione `JSONQuery`, Firehose verifica innanzitutto il campo dei metadati nell'output Lambda per determinare come indirizzare il record alla tabella di destinazione appropriata, quindi esamina l'output dell'espressione per individuare i campi mancanti. `JSONQuery`

Se la Lambda o `JSONQuery` l'espressione non forniscono le informazioni di routing richieste, Firehose lo presuppone come uno scenario a tabella singola e cerca le informazioni su una singola tabella nella configurazione delle chiavi uniche.

Per ulteriori informazioni, consulta la tabella [Instradare i record in entrata verso una singola tabella Iceberg](#). Se Firehose non riesce a determinare le informazioni di routing e ad abbinare il record a una tabella di destinazione specificata, invia i dati al bucket di errore S3 specificato.

Funzione Lambda di esempio

Questa funzione Lambda è un esempio di codice Python che analizza i record dei flussi in entrata e aggiunge i campi obbligatori per specificare come i dati devono essere scritti in tabelle specifiche. È possibile utilizzare questo codice di esempio per aggiungere la sezione dei metadati per le informazioni di routing.

```
import json
import base64

def lambda_handler(firehose_records_input, context):
    print("Received records for processing from DeliveryStream: " +
          firehose_records_input['deliveryStreamArn'])

    firehose_records_output = {}
    firehose_records_output['records'] = []
```

```
for firehose_record_input in firehose_records_input['records']:

    # Get payload from Lambda input, it could be different with different sources
    if 'kafkaRecordValue' in firehose_record_input:
        payload_bytes =
base64.b64decode(firehose_record_input['kafkaRecordValue']).decode('utf-8')
    else
        payload_bytes =
base64.b64decode(firehose_record_input['data']).decode('utf-8')

    # perform data processing on customer payload bytes here

    # Create output with proper record ID, output data (may be different with
different sources), result, and metadata
    firehose_record_output = {}

    if 'kafkaRecordValue' in firehose_record_input:
        firehose_record_output['kafkaRecordValue'] =
base64.b64encode(payload_bytes.encode('utf-8'))
    else
        firehose_record_output['data'] =
base64.b64encode(payload_bytes.encode('utf-8'))

    firehose_record_output['recordId'] = firehose_record_input['recordId']
    firehose_record_output['result'] = 'Ok'
    firehose_record_output['metadata'] = {
        'otfMetadata': {
            'destinationDatabaseName': 'your_destination_database',
            'destinationTableName': 'your_destination_table',
            'operation': 'insert'
        }
    }

    firehose_records_output['records'].append(firehose_record_output)
return firehose_records_output
```

Monitoraggio di parametri

Per la distribuzione dei dati ad Apache Iceberg Tables, Firehose emette le seguenti CloudWatch metriche a livello di flusso.

Metrica	Description
<code>DeliveryToIceberg.Bytes</code>	Il numero di byte consegnati alle tabelle Apache Iceberg nel periodo di tempo specificato. Unità: byte
<code>DeliveryToIceberg.IncomingRowCount</code>	Numero di record che Firehose tenta di inviare ad Apache Iceberg Tables. Unità: numero
<code>DeliveryToIceberg.SuccessfulRowCount</code>	Numero di righe riuscite consegnate ad Apache Iceberg Tables. Unità: numero
<code>DeliveryToIceberg.FailedRowCount</code>	Numero di righe non riuscite consegnate al bucket di backup S3. Unità: numero
<code>DeliveryToIceberg.DataFreshness</code>	L'epoca (dall'ingresso nei Firehose ad oggi) del primo disco in Firehose. Qualsiasi disco precedente a questa età è stato consegnato ad Apache Iceberg Tables. Unità: secondi
<code>DeliveryToIceberg.Success</code>	Somma dei commit eseguiti con successo su Apache Iceberg Tables.
<code>JQProcessing.Duration</code>	Il tempo impiegato per eseguire l'espressione JQ. Unità: millisecondi

Comprendi i tipi di dati supportati

Firehose supporta tutti i tipi di dati primitivi e complessi supportati da Apache Iceberg. Per ulteriori informazioni, consulta [Schemi](#) e tipi di dati. Quando si inviano dati binari come stringa, è necessario

utilizzare i tipi di codifica supportati da Firehose: Basic Base64, MIME Base64, URL and filename safe Base64 e Hex. Per i tipi di dati Timestamp, è necessario inviare sempre in microsecondi.

Esempi di tipi di dati

La sezione seguente mostra esempi di diversi tipi di dati.

MapType

```
{
  "destination_column_0":
  {"WP5o0J0kuIQcDPcsvpJJygF1xza0Sq0wUlGTwuIeCEzgVneGxA":"P03ReF3auyDqbfonx9Cd8NTmcQnqnw7JuZ0CWwI
  "destination_column_1": "{\"destination_nested_column_0\": \\
  \\\"18:56:14.974\\\", \\\"destination_nested_column_1\\\": 241.86246}\"":
  \\\"M07kAvYdHvBh61F7RzfxEd39YQI33LnM2NbGS67D0FFsRUyUUujKT5VnK7Wtfz1mHNeIix6FAY9cYpwTdedgr9XnFwG0
  \",\"{destination_nested_column_0\": \\\"18:56:14.974\\
  \\\", \\\"destination_nested_column_1\\\": 562.56384}\"":
  \\\"9G1xhDcT95LxBo51HybBZihq0qf6EU8jrDu7NMpxtGB2dY6q6kXpvxIrFuMdqHCJKIZIcDikwggLniUm8kgE4d
  \",\"{destination_nested_column_0\": \\\"18:56:14.974\\
  \\\", \\\"destination_nested_column_1\\\": 496.03268}\"":
  \\\"keTJZYLNvLRB50DMKzEI6M0AM4mueyNnA1m2YVnYdDwyxUpPqkb72Q6LiX0B9s8gCjZ6trW6C1PFk9KNBIpxYsj5Tc5Xs
  \",\"{destination_nested_column_0\": \\\"18:56:14.974\\\", \\
  \\\"destination_nested_column_1\\\": 559.0878}\"":
  \\\"mG0ZET84BUF28E312UCIWgmyPyQFSU0DH9NAMAnF3LJEutbooZWcBt97PP5AhaopNvC8pQZ4mGXB9hmVmJUNmuj5Qanyx
  \",\"{destination_nested_column_0\": \\\"18:56:14.974\\
  \\\", \\\"destination_nested_column_1\\\": 106.845245}\"":
  \\\"aidovYrzu8gcLRkVVUyTKCN9gqTUFYi8uJQsrXEFY11f9ool7JhAtg9QKG5BBu67Ngb95ENSNKQyCHNImsu5x4hMnmHU
  \\\"}"}
}
```

DecimalType

```
{
  "destination_column_0": 9455262425851.1342772,
  "destination_column_1": "9455262425851.1342772",
  "destination_column_2": 9455262425852
}
```

BinaryType (base64-default, base64-mime, base64-url-safe, hex)

```
{
  "destination_column_0": "AsYhnHD\\Ra54hITl1daNV9gl0jtWPEfopH
  +PjgUKHYB6K7UcYi4K19b80wD4J\\93x5tyh+0y"
```

```

+k5cMljVRlmfIkIuLx19ERBiPPLhf4+yoJ2k70VavPnYWmNLs1hLDHlfeEMIfvHrq0GzJMoA
+CBAXfIuiG420JSQP5iAx5xFG\
m0fkM5zYothje80GX1tdthcCL6WYBiP0S1wXcE0uMerfwc1Ac9fT0Bz6RzdJ1HhUDjoAXg
+4cvly27F82XpuGMNwpUj98A0rgbh2MoU9yvvsM9ZrjD0eGVg0ZP8Ky7Za4oE\ok8j
+qABF6XV712iA6pVtTNJFvX6Ey3ssNYvno+LYF5ZsySs2rB5AbVM73RfOPqdS\c\
r3MEqoEqt+nPx6eGam4WSA+0swztt7aLdr1X6yK7xJeIJ0rTlIDBo0ZUaw011ykY
\8Bvy+4byoPlmr4Z5yhN1z3ZT0kx7eDR6xMv+vDVSDbtItVazDwHgDy41r
\hQNeNedPKrozc8TY9k7wZre\6V2lCa3BmT8Uu9b9yjdjR9z+fCSdG
+VRv35nz5kdqdKy8YIrynYs4e0cjh8jH3UwVYrYQcnWkBAFF7Xk9CoPVnL3ciHZtyiZ0aTGIj9r00xX\
W5dGe9\4YChs6LbD584kxLTxvHgS14vadaTGNKci3SvNmZNsz8ducxtNXF\Tv2DUub465hzgpaLPur3+MB
+kfdN2YXUfqb
+xJAgxThWfUe151nrH0EPow9lgS1p21rUBGznJAvPRl1ExGIAuc7JYAoUrJUkx5Hf16PekPDhqt7+yJwCB8qhxTTryxo
+bjtai4ndRCGcuCaxT8Kk0cXsS37urd3YGSdMinZdMNVc646s25415qK6nBRlqqAY8+EYmcUIVB9XcNdke4zoUfhVQoruwidzDU\
\kFafoulo5DEoM0yaH1N2HCSxG5tZXNQocSZPaY8efZYMCpmDXsPAzkmGskYRDSu\3wUqR0a2tGK5\
pQY24v+Jq0U\jQ99GShlU283nZ85ot2ocbtMAGD\WsrSEh61Nt9RaI3HfA7\HcH\
fgr9jsTtxDgZhabTBwwDwX0zjWgX1bCuTLKBN7byxg9ZvAVgqwPS4HERLer5T5UkKf74zn9Eq3HYH1Q5JpyDUx
+im7mte1sprf1+A24kksVU\MD9aP9N8\QDsQ13gkh0n5KwFMz3BC2Vw5gL
+gGNHFKDRL6wGIIfhuYcx9LucolZ1yNy9Gbb3ioWSSufyFpyXqtndDLPI5QS1SjPm2KDyqch1SmRLIhd9MNRUC73EAEm
+N05wxPzBRSjhCHZpf8SrYITWJl7K3XzG0fPFh2NgES3jMP9cvSX06yyICcep2HBYGbfFlni89+Rw==",
    "destination_column_1": "AsYhnHD\Ra54hITl1daNV9g10jtwPEfopH
+PjgUKHYB6K7UcYi4K19b80wD4J\93x5tyh+0y+k5c\r
\nMljVRlmfIkIuLx19ERBiPPLhf4+yoJ2k70VavPnYWmNLs1hLDHlfeEMIfvHrq0GzJMoA+CBAXfI\r
\nuiG420JSQP5iAx5xFG\m0fkM5zYothje80GX1tdthcCL6WYBiP0S1wXcE0uMerfwc1Ac9fT0Bz6R\r
\nzdJ1HhUDjoAXg+4cvly27F82XpuGMNwpUj98A0rgbh2MoU9yvvsM9ZrjD0eGVg0ZP8Ky7Za4oE\ok\r
\n8j+qABF6XV712iA6pVtTNJFvX6Ey3ssNYvno+LYF5ZsySs2rB5AbVM73RfOPqdS\c\r3MEqoEqt+
\r\nnPx6eGam4WSA+0swztt7aLdr1X6yK7xJeIJ0rTlIDBo0ZUaw011ykY\8Bvy+4byoPlmr4Z5yhN1z
\r\n3ZT0kx7eDR6xMv+vDVSDbtItVazDwHgDy41r\hQNeNedPKrozc8TY9k7wZre\6V2lCa3BmT8Uu9b
\r\n9yjdjR9z+fCSdG+VRv35nz5kdqdKy8YIrynYs4e0cjh8jH3UwVYrYQcnWkBAFF7Xk9CoPVnL3ciHZ
\r\nntyiz0aTGIj9r00xX\W5dGe9\4YChs6LbD584kxLTxvHgS14vadaTGNKci3SvNmZNsz8ducxtNXF
\r\nTv2DUub465hzgpaLPur3+MB+kfdN2YXUfqb+xJAgxThWfUe151nrH0EPow9lgS1p21rUBGznJAvP
\r\nRl1ExGIAuc7JYAoUrJUkx5Hf16PekPDhqt7+yJwCB8qhxTTryxo+bjtai4ndRCGcuCaxT8Kk0cXs\r
\nS37urd3YGSdMinZdMNVc646s25415qK6nBRlqqAY8+EYmcUIVB9XcNdke4zoUfhVQoruwidzDU\k\r
\nFafoulo5DEoM0yaH1N2HCSxG5tZXNQocSZPaY8efZYMCpmDXsPAzkmGskYRDSu\3wUqR0a2tGK5\r
\n\pQY24v+Jq0U\jQ99GShlU283nZ85ot2ocbtMAGD\WsrSEh61Nt9RaI3HfA7\HcH\fgfr9jsTtxDg
\r\nZhabTBwwDwX0zjWgX1bCuTLKBN7byxg9ZvAVgqwPS4HERLer5T5UkKf74zn9Eq3HYH1Q5JpyDUx\r
\nim7mte1sprf1+A24kksVU\MD9aP9N8\QDsQ13gkh0n5KwFMz3BC2Vw5gL+gGNHFKDRL6wGIIfhuYc
\r\nx9LucolZ1yNy9Gbb3ioWSSufyFpyXqtndDLPI5QS1SjPm2KDyqch1SmRLIhd9MNRUC73EAEm+N0\r
\n5wxPzBRSjhCHZpf8SrYITWJl7K3XzG0fPFh2NgES3jMP9cvSX06yyICcep2HBYGbfFlni89+Rw==",
    "destination_column_2": "AsYhnHD_Ra54hITl1daNV9g10jtwPEfopH-
PjgUKHYB6K7UcYi4K19b80wD4J_93x5tyh-0y-k5cMljVRlmfIkIuLx19ERBiPPLhf4-
yoJ2k70VavPnYWmNLs1hLDHlfeEMIfvHrq0GzJMoA-
CBAXfIuiG420JSQP5iAx5xFG_m0fkM5zYothje80GX1tdthcCL6WYBiP0S1wXcE0uMerfwc1Ac9fT0Bz6RzdJ1HhUDjoAXg-
qABF6XV712iA6pVtTNJFvX6Ey3ssNYvno-LYF5ZsySs2rB5AbVM73RfOPqdS_c_r3MEqoEqt-
nPx6eGam4WSA-0swztt7aLdr1X6yK7xJeIJ0rTlIDBo0ZUaw011ykY_8Bvy-4byoPlmr4Z5yhN1z3ZT0kx7eDR6xMv-

```

```
vDVSDbTItVazDwHgDy41r_hQNeNedPKrozc8TY9k7wZre_6V2lCa3BmT8Uu9b9yjdjR9z-fCSdG-
VRv35nz5kdqdKy8YIrynYs4e0cjh8jH3UwVYrYQcnWkBAFF7Xk9CoPVnL3ciHZtyiZ0aTGIj9r00xX_W5dGe9_4YChs6LbD
MB-kfdN2YXUfqb-
xJAgxThWfUe151nrH0EPow9lgSlp21rUBGznJAvPRl1ExGIAuc7JYAoUrJUkx5Hf16PekPDhqt7-
yJwCB8qxhTTryxo-bjtai4ndRCGcuCaxT8Kk0cXsS37urd3YGSDMinZdMNVc646s25415qK6nBRlqqAY8-
EYmcUIVB9XcNdke4zoUfhVQoruwidzDU_kFafoulo5DEoM0yaH1N2HCSxG5tZXNQocSZPaY8efZYMCpmDXsPAzkmGskYRDS
Jq0U_jQ99GShlU283nZ85ot2ocbtMAgD_WsrSEh6lNt9RaI3HfA7_HcH_fgr9jsTtxDgZhabTBwwDwX0zjWGx1bCuTLKBN7
im7mte1sprf1-A24kksVU_MD9aP9N8_QDsQ13gkh0n5KwFMz3BC2Vw5gL-
gGNHFKDRL6wGI fhuYcx9LucolZ1yNy9Gbb3ioWSSufyFpyXqtndDLPI5QS1S5JpJm2KDYqcH1SmRLIhd9MNRUC73EAEm-
N05wxPzBRSjhCHZpf8SrYITWJl7K3XzG0fPFh2NgES3jMP9cvSX06yyICcep2HBYGbFflni89-Rw==" ,
  "destination_column_3":
    "02c6219c70ff45ae788484e5d5d68d57d8253a3b563c47e8a47f8f8e050a1d807a2bb51c622e0ad7d6fcd300f827f
}
```

TimeType (Epoca in microsecondi, oggetto LocalTime Java)

```
{
  "destination_column_0": 68175096000,
  "destination_column_1": "18:56:15.096"
}
```

TimestampType.withZone (Epoch in microsecondi, oggetto Java, OffsetDateTime oggetto Java)
LocalDateTime

```
{
  "destination_column_0": 1725476175099000,
  "destination_column_1": "2024-09-04T18:56:15.099Z",
  "destination_column_2": "2024-09-04T18:56:15.099"
}
```

DoubleType

```
{
  "destination_column_0": 9.18477568715142,
  "destination_column_1": "9.18477568715142"
}
```

BooleanType

```
{
  "destination_column_0": true,
}
```

```
"destination_column_1": "false",  
"destination_column_2": 1,  
"destination_column_3": 0  
}
```

FloatType

```
{  
  "destination_column_0": 0.6242226,  
  "destination_column_1": "0.6242226"  
}
```

IntegerType

```
{  
  "destination_column_0": 7,  
  "destination_column_1": "7"  
}
```

TimestampType.withoutZone (Epoch in microsecondi, oggetto Java, oggetto Java, oggetto Java
LocalDateTime) OffsetDateTime ZonedDateTime

```
{  
  "destination_column_0": 1725476175114000,  
  "destination_column_1": "2024-09-04T18:56:15.114",  
  "destination_column_2": "2024-09-04T18:56:15.114Z",  
  "destination_column_3": "2024-09-04T18:56:15.114-07:00"  
}
```

DateType

```
{  
  "destination_column_0": 19970,  
  "destination_column_1": "2024-09-04"  
}
```

LongType

```
{  
  "destination_column_0": 8,  
}
```

```
"destination_column_1": "8"
}
```

UUIDType (Oggetto Java UUID)

```
{
  "destination_column_0": "21c5521c-a6d4-48d4-b2c8-7f6d842f72c3"
}
```

ListType

```
{
  "destination_column_0":
  ["s1FSrgb0lGDxfn2iYT0Et1P47aHSjwmLZgrdr1JqRs0dmbeCcQoaLr4Xhi2KIVvmus9ppFdpWIc0HnJ0omhAPhXH0yns
  "destination_column_1": "[{"destination_nested_column_0": "\bb00f8e6-
db82-4241-a5c5-0d9c0d2f71a4", "destination_nested_column_1": 907.35345},
{"destination_nested_column_0": "\2c77b702-d405-4fe1-beee-fb541d7ab833",
"destination_nested_column_1": 544.0026}, {"destination_nested_column_0":
\68389200-d6b1-413d-bcd9-fdb931708395", "destination_nested_column_1": 153.683},
{"destination_nested_column_0": "\bc31cbaa-39cd-4e2f-b357-9ea9ce75532b",
"destination_nested_column_1": 977.5165}, {"destination_nested_column_0":
\b7d627f9-0d5b-41b7-903a-525488259fba", "destination_nested_column_1": 434.17215},
{"destination_nested_column_0": "\06b6ec1e-1952-4582-b285-46aaf40064b8",
"destination_nested_column_1": 580.33124}, {"destination_nested_column_0":
\f04b3bbf-61ad-4c5c-8740-6f666f57c431", "destination_nested_column_1": 550.75793}]"
}
```

Resources

Utilizza le seguenti risorse per saperne di più:

- [Trasmetti dati in tempo reale nelle tabelle Apache Iceberg in Amazon S3 utilizzando Amazon Data Firehose](#)
- [Semplifica l'analisi dei AWS WAF log con Apache Iceberg e Amazon Data Firehose](#)
- [Crea un data lake per lo streaming di dati con Amazon S3 Tables e Amazon Data Firehose](#)

Etichetta uno stream Firehose

Puoi assegnare i tuoi metadati ai flussi Firehose che crei in Amazon Data Firehose sotto forma di tag. Un tag è un valore-chiave che definisci per un flusso. L'uso dei tag è un modo semplice ma efficace per gestire AWS le risorse e organizzare i dati, compresi i dati di fatturazione.

È possibile specificare i tag quando si richiama [CreateDeliveryStream](#) per creare un nuovo stream Firehose. Per gli stream Firehose esistenti, è possibile aggiungere, elencare e rimuovere tag utilizzando le tre operazioni seguenti:

- [TagDeliveryStream](#)
- [ListTagsForDeliveryStream](#)
- [UntagDeliveryStream](#)

Comprendi le nozioni di base sui tag

Puoi utilizzare le operazioni dell'API Amazon Data Firehose per completare le seguenti attività:

- Aggiungere tag a uno stream Firehose.
- Elenca i tag per i tuoi stream Firehose.
- Rimuove i tag da uno stream Firehose.

Puoi usare i tag per classificare i tuoi stream Firehose. Ad esempio, è possibile classificare i flussi Firehose per scopo, proprietario o ambiente. Poiché definisci una chiave e un valore per ogni tag, puoi creare un set di categorie personalizzate per soddisfare esigenze specifiche. Ad esempio, è possibile definire un set di tag che consenta di tracciare i flussi Firehose per proprietario e applicazione associata.

Di seguito sono illustrati alcuni esempi di tag:

- Project: *Project name*
- Owner: *Name*
- Purpose: Load testing
- Application: *Application name*
- Environment: Production

Se specifichi tag nell'`CreateDeliveryStream` operazione, Amazon Data Firehose esegue un'autorizzazione aggiuntiva sull'`firehose:TagDeliveryStream` operazione per verificare se gli utenti dispongono delle autorizzazioni per creare tag. Se non si fornisce questa autorizzazione, le richieste di creazione di nuovi flussi Firehose con tag di risorse IAM falliranno con uno degli `AccessDeniedException` esempi seguenti.

```
AccessDeniedException
```

```
User: arn:aws:sts::x:assumed-role/x/x is not authorized to perform:
  firehose:TagDeliveryStream on resource: arn:aws:firehose:us-east-1:x:deliverystream/x
  with an explicit deny in an identity-based policy.
```

L'esempio seguente illustra una politica che consente agli utenti di creare uno stream Firehose e applicare i tag.

Tieni traccia dei costi con l'etichettatura

Puoi utilizzare i tag per classificare e tenere traccia AWS dei costi. Quando applichi tag alle tue AWS risorse, inclusi i flussi Firehose, il report sull'allocazione AWS dei costi include l'utilizzo e i costi aggregati per tag. Puoi organizzare i costi tra più servizi applicando tag che rappresentano categorie di business (come centri di costo, nomi di applicazioni o proprietari). Per ulteriori informazioni, consulta [Utilizzo dei tag per l'allocazione dei costi ai fini dei report di fatturazione personalizzati](#) nella AWS Billing User Guide (Guida per l'utente di Amazon API Gateway).

Conosci le restrizioni relative ai tag

Le seguenti restrizioni si applicano ai tag in Amazon Data Firehose.

Limitazioni di base

- Il numero massimo di tag per risorsa (flusso) è 50.
- Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole.
- Non è possibile cambiare o modificare i tag di un flusso eliminato.

Limitazioni applicate alle chiavi di tag

- Ogni chiave di tag deve essere univoca. Se aggiungi un tag con una chiave già in uso, il nuovo tag sovrascrive la coppia chiave-valore esistente.

- Una chiave di tag non può iniziare con `aws :` perché questo prefisso è riservato per l'utilizzo da parte di AWS. AWS crea tag con questo prefisso per tuo conto, ma non puoi modificarli o eliminarli.
- Le chiavi di tag devono avere una lunghezza compresa tra 1 e 128 caratteri Unicode.
- Le chiavi di tag devono contenere i seguenti caratteri: lettere Unicode, cifre, spazio e i seguenti caratteri speciali: `_ . / = + - @`.

Limitazioni applicate ai valori dei tag

- I valori dei tag devono avere una lunghezza compresa tra 0 e 255 caratteri Unicode.
- I valori dei tag possono essere vuoti. In caso contrario, devono contenere i seguenti caratteri: lettere Unicode, cifre, spazio e i seguenti caratteri speciali: `_ . / = + - @`.

Sicurezza in Amazon Data Firehose

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, trarrai vantaggio da un data center e da un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti come parte dei [programmi di conformità AWS](#). Per ulteriori informazioni sui programmi di conformità che si applicano a Data Firehose, vedere [AWS Services in Scope by Compliance Program](#).
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e leggi e normative applicabili.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Data Firehose. I seguenti argomenti mostrano come configurare Data Firehose per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che possono aiutarti a monitorare e proteggere le tue risorse Data Firehose.

Argomenti

- [Protezione dei dati in Amazon Data Firehose](#)
- [Controllo dell'accesso con Amazon Data Firehose](#)
- [Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose](#)
- [Gestisci i ruoli IAM tramite la console Amazon Data Firehose](#)
- [Comprendi la conformità per Amazon Data Firehose](#)
- [Resilienza in Amazon Data Firehose](#)
- [Comprendi la sicurezza dell'infrastruttura in Amazon Data Firehose](#)
- [Implementa le best practice di sicurezza per Amazon Data Firehose](#)

Protezione dei dati in Amazon Data Firehose

Amazon Data Firehose crittografa tutti i dati in transito utilizzando il protocollo TLS. Inoltre, per i dati archiviati in uno storage provvisorio durante l'elaborazione, Amazon Data Firehose crittografa i dati [AWS Key Management Service](#) utilizzando e verifica l'integrità dei dati mediante la verifica tramite checksum.

Se disponi di dati sensibili, puoi abilitare la crittografia dei dati lato server quando usi Amazon Data Firehose. Il modo in cui esegui questa operazione dipende dall'origine dei dati.

Note

Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-2](#).

Crittografia lato server con Kinesis Data Streams

Quando invii dati dai tuoi produttori di dati al tuo flusso di dati, Kinesis Data Streams crittografa i dati AWS Key Management Service utilizzando AWS KMS una chiave () prima di archivarli a riposo. Quando il flusso Firehose legge i dati dal flusso di dati, Kinesis Data Streams prima decrittografa i dati e poi li invia ad Amazon Data Firehose. Amazon Data Firehose memorizza nel buffer i dati in memoria in base ai suggerimenti di buffering specificati. Li distribuisce quindi alle destinazioni senza archiviare i dati inattivi non crittografati.

Per informazioni su come abilitare la crittografia lato server per Kinesis Data Streams, consulta [Utilizzo della crittografia lato server](#) nella Guida per gli sviluppatori del flusso di dati Amazon Kinesis.

Crittografia lato server con Direct PUT o altre fonti di dati

Se invii dati al tuo stream Firehose utilizzando [PutRecord](#) o [PutRecordBatch](#), o se invii i dati utilizzando AWS IoT Amazon CloudWatch Logs o CloudWatch Events, puoi attivare la crittografia lato server utilizzando l'operazione. [StartDeliveryStreamEncryption](#)

Per interrompere server-side-encryption, usa l'operazione. [StopDeliveryStreamEncryption](#)

È inoltre possibile abilitare SSE quando si crea lo stream Firehose. A tale scopo, specificate [DeliveryStreamEncryptionConfigurationInput](#) quando richiamate. [CreateDeliveryStream](#)

Per un utilizzo corretto `CUSTOMER_MANAGED_CMK`, sia la policy IAM del chiamante che la policy KMS key devono consentire `kms:GenerateDataKey` operazioni. `kms:Decrypt` Firehose convalida queste autorizzazioni durante la chiamata `PutRecord` o con la crittografia. `PutRecordBatch` `CUSTOMER_MANAGED_CMK` Inoltre, è richiesta `kms:CreateGrant` l'autorizzazione durante la chiamata `CreateDeliveryStream` o `StartDeliveryStreamEncryption` con la crittografia. `CUSTOMER_MANAGED_CMK`

Quando la CMK è di tipo `CUSTOMER_MANAGED_CMK`, se il servizio Amazon Data Firehose non è in grado di decrittografare i record a causa di `KMSNotFoundException`, `KMSInvalidStateException` o `KMSDisabledException` `KMSAccessDeniedException`, il servizio attende fino a 24 ore (periodo di conservazione) prima che tu risolva il problema. Se il problema persiste oltre il periodo di conservazione, il servizio ignora i record che hanno superato il periodo di conservazione e non sono stati decrittografati, quindi elimina i dati. Amazon Data Firehose fornisce le seguenti quattro CloudWatch metriche che puoi utilizzare per tenere traccia delle quattro eccezioni: AWS KMS

- `KMSKeyAccessDenied`
- `KMSKeyDisabled`
- `KMSKeyInvalidState`
- `KMSKeyNotFound`

Per ulteriori informazioni su questi parametri, consulta [the section called “Monitoraggio con metriche CloudWatch”](#).

Important

Per crittografare il tuo stream Firehose, usa `symmetric`. CMKs Amazon Data Firehose non supporta l'asimmetria. CMKs [Per informazioni su simmetrico e asimmetrico, consulta About Symmetric and Asymmetric nella CMKs guida per sviluppatori. CMKs](#) AWS Key Management Service

Note

Quando si utilizza una [chiave gestita dal cliente](#) (`CUSTOMER_MANAGED_CMK`) per abilitare la crittografia lato server (SSE) per lo stream Firehose, il servizio Firehose imposta un contesto di crittografia ogni volta che utilizza la chiave. Poiché questo contesto di crittografia

rappresenta un evento in cui è stata utilizzata una chiave di proprietà dell'account, viene registrato come parte dei registri degli eventi AWS dell'account. AWS CloudTrail AWS Questo contesto di crittografia è un sistema generato dal servizio Firehose. L'applicazione non deve fare ipotesi sul formato o sul contenuto del contesto di crittografia impostato dal servizio Firehose.

Controllo dell'accesso con Amazon Data Firehose

Le seguenti sezioni spiegano come controllare l'accesso da e verso le risorse Amazon Data Firehose. Le informazioni trattate includono come concedere l'accesso all'applicazione in modo che possa inviare dati allo stream Firehose. Descrivono inoltre come concedere ad Amazon Data Firehose l'accesso al tuo bucket Amazon Simple Storage Service (Amazon S3), al cluster Amazon Redshift OpenSearch o al cluster Amazon Service, nonché le autorizzazioni di accesso necessarie se utilizzi Datadog, LogicMonitor Dynatrace, MongoDB, New Relic, Splunk o Sumo Logic come destinazione. Infine, in questo argomento troverai indicazioni su come configurare Amazon Data Firehose in modo che possa fornire dati a una destinazione che appartiene a un account diverso AWS . La tecnologia per gestire tutte queste forme di accesso è AWS Identity and Access Management (IAM). Per ulteriori informazioni su IAM, consulta [Che cos'è IAM?](#).

Indice

- [Concedi l'accesso alle tue risorse Firehose](#)
- [Concedi a Firehose l'accesso al tuo cluster Amazon MSK privato](#)
- [Consenti a Firehose di assumere un ruolo IAM](#)
- [Concedi a Firehose l'accesso a AWS Glue per la conversione del formato dei dati](#)
- [Concedi a Firehose l'accesso a una destinazione Amazon S3](#)
- [Concedi a Firehose l'accesso alle tabelle Amazon S3](#)
- [Concedi a Firehose l'accesso a una destinazione Apache Iceberg Tables](#)
- [Concedi a Firehose l'accesso a una destinazione Amazon Redshift](#)
- [Concedi a Firehose l'accesso a una destinazione di servizio pubblico OpenSearch](#)
- [Concedere a Firehose l'accesso a una destinazione OpenSearch di servizio in un VPC](#)
- [Concedere a Firehose l'accesso a una destinazione Serverless pubblica OpenSearch](#)
- [Concedi a Firehose l'accesso a una destinazione OpenSearch Serverless in un VPC](#)
- [Concedi a Firehose l'accesso a una destinazione Splunk](#)

- [Accesso a Splunk in VPC](#)
- [Inserisci i log di flusso VPC in Splunk utilizzando Amazon Data Firehose](#)
- [Accesso a Snowflake o all'endpoint HTTP](#)
- [Concedi a Firehose l'accesso a una destinazione Snowflake](#)
- [Accesso a Snowflake in VPC](#)
- [Concedere a Firehose l'accesso a una destinazione endpoint HTTP](#)
- [Consegna su più account da Amazon MSK](#)
- [Consegna su più account a una destinazione Amazon S3](#)
- [Consegna tra più account a una OpenSearch destinazione del servizio](#)
- [Utilizzo dei tag per controllare l'accesso](#)

Concedi l'accesso alle tue risorse Firehose

Per consentire all'applicazione di accedere allo stream Firehose, utilizzate un criterio simile a questo esempio. Puoi regolare le singole operazioni API alle quali concedi l'accesso modificando la sezione Action; oppure puoi concedere l'accesso a tutte le operazioni con "firehose:*".

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "firehose:DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
      ],
      "Resource": [
        "arn:aws:firehose:us-east-1:123456789012:deliverystream/delivery-stream-name"
      ]
    }
  ]
}
```

Concedi a Firehose l'accesso al tuo cluster Amazon MSK privato

Se l'origine del tuo stream Firehose è un cluster Amazon MSK privato, utilizza una policy simile a questo esempio.

È necessario aggiungere una politica come questa alla politica basata sulle risorse del cluster per concedere al responsabile del servizio Firehose l'autorizzazione a richiamare l'operazione dell'API Amazon MSK. `CreateVpcConnection`

Consenti a Firehose di assumere un ruolo IAM

Questa sezione descrive le autorizzazioni e le politiche che concedono ad Amazon Data Firehose l'accesso per l'acquisizione, l'elaborazione e la distribuzione dei dati dalla sorgente alla destinazione.

Note

Se si utilizza la console per creare uno stream Firehose e si sceglie l'opzione per creare un nuovo ruolo, al ruolo AWS viene associata la policy di fiducia richiesta. Se desideri che Amazon Data Firehose utilizzi un ruolo IAM esistente o se ne crei uno personalizzato, collega le seguenti policy di trust a quel ruolo in modo che Amazon Data Firehose possa assumerlo. Modifica le politiche per sostituirle *account-id* con l'ID del tuo AWS account. Per informazioni su come modificare la relazione di trust di un ruolo, consulta [Modifica di un ruolo](#).

Amazon Data Firehose utilizza un ruolo IAM per tutte le autorizzazioni necessarie allo stream Firehose per elaborare e fornire dati. Assicurati che a quel ruolo siano associate le seguenti policy di fiducia in modo che Amazon Data Firehose possa assumerlo.

Se scegli Amazon MSK come origine per il tuo stream Firehose, devi specificare un altro ruolo IAM che conceda ad Amazon Data Firehose le autorizzazioni per importare dati di origine dal cluster Amazon MSK specificato. Assicurati che a quel ruolo siano associate le seguenti policy di fiducia in modo che Amazon Data Firehose possa assumerlo.

JSON

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

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

Assicurati che questo ruolo che concede ad Amazon Data Firehose le autorizzazioni per importare dati di origine dal cluster Amazon MSK specificato conceda le seguenti autorizzazioni:

Concedi a Firehose l'accesso a AWS Glue per la conversione del formato dei dati

Se lo stream Firehose esegue una conversione in formato dati, Amazon Data Firehose fa riferimento alle definizioni delle tabelle memorizzate in AWS Glue. Per fornire ad Amazon Data Firehose l'accesso necessario a AWS Glue, aggiungi la seguente dichiarazione alla tua politica. Per informazioni su come trovare l'ARN della tabella, vedere [Specifying AWS Glue Resource ARNs](#).

```
{  
  "Sid": "",  
  "Effect": "Allow",  
  "Action": [  
    "glue:GetTable",  
    "glue:GetTableVersion",  
    "glue:GetTableVersions"  
  ],  
  "Resource": [  
    "arn:aws:glue:us-east-1:123456789012:catalog",  
    "arn:aws:glue:us-east-1:123456789012:database/b",  
    "arn:aws:glue:us-east-1:123456789012:table/b/easd"  
  ]  
},  
{  
  actions: ['glue:GetSchemaVersion'],
```

```
    grantee: options.role,  
    resourceArns: ['*'],  
  }  
}
```

La politica consigliata per recuperare gli schemi dal registro degli schemi non ha restrizioni sulle risorse. Per ulteriori informazioni, consulta [gli esempi IAM per i deserializzatori](#) nella Developer Guide. AWS Glue

Concedi a Firehose l'accesso a una destinazione Amazon S3

Quando utilizzi una destinazione Amazon S3, Amazon Data Firehose invia i dati al tuo bucket S3 e può opzionalmente utilizzare una AWS KMS chiave di tua proprietà per la crittografia dei dati. Se la registrazione degli errori è abilitata, Amazon Data Firehose invia anche gli errori di consegna dei dati al gruppo di log e CloudWatch ai flussi. È necessario disporre di un ruolo IAM durante la creazione di uno stream Firehose. Amazon Data Firehose assume il ruolo IAM e ottiene l'accesso al bucket, alla chiave, al gruppo di log e CloudWatch ai flussi specificati.

Utilizza la seguente politica di accesso per consentire ad Amazon Data Firehose di accedere al tuo bucket e alla tua chiave S3. AWS KMS Se non sei proprietario del bucket S3, aggiungi `s3:PutObjectACL` all'elenco delle operazioni Amazon S3. Ciò garantisce al proprietario del bucket l'accesso completo agli oggetti forniti da Amazon Data Firehose.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3:AbortMultipartUpload",  
        "s3:GetBucketLocation",  
        "s3:GetObject",  
        "s3:ListBucket",  
        "s3:ListBucketMultipartUploads",  
        "s3:PutObject"  
      ],  
      "Resource": [  
        "arn:aws:s3:::amzn-s3-demo-bucket",  
        "arn:aws:s3:::amzn-s3-demo-bucket/*"  
      ]  
    }  
  ]  
}
```

```

    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kinesis:DescribeStream",
      "kinesis:GetShardIterator",
      "kinesis:GetRecords",
      "kinesis:ListShards"
    ],
    "Resource": "arn:aws:kinesis:us-east-1:123456789012:stream/stream-
name"
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": [
      "arn:aws:kms:us-east-1:123456789012:key/key-id"
    ],
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "s3.us-east-1.amazonaws.com"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-
demo-bucket/prefix*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:us-east-1:123456789012:log-group:log-group-name:log-
stream:log-stream-name"
    ]
  },
  {
    "Effect": "Allow",

```

```

    "Action": [
      "lambda:InvokeFunction",
      "lambda:GetFunctionConfiguration"
    ],
    "Resource": [
      "arn:aws:lambda:us-east-1:123456789012:function:function-
      name:function-version"
    ]
  }
]
}

```

La policy in alto ha anche un'istruzione che permette l'accesso a flusso di dati Amazon Kinesis. Se non utilizzi Kinesis Data Firehose come origine dati, puoi rimuovere questa istruzione. Se utilizzi Amazon MSK come fonte, puoi sostituire tale dichiarazione con la seguente:

```

{
  "Sid": "",
  "Effect": "Allow",
  "Action": [
    "kafka:GetBootstrapBrokers",
    "kafka:DescribeCluster",
    "kafka:DescribeClusterV2",
    "kafka-cluster:Connect"
  ],
  "Resource": "arn:aws:kafka:{{mskClusterRegion}}:{{mskClusterAccount}}:cluster/
  {{mskClusterName}}/{{clusterUUID}}"
},
{
  "Sid": "",
  "Effect": "Allow",
  "Action": [
    "kafka-cluster:DescribeTopic",
    "kafka-cluster:DescribeTopicDynamicConfiguration",
    "kafka-cluster:ReadData"
  ],
  "Resource": "arn:aws:kafka:{{mskClusterRegion}}:{{mskClusterAccount}}:topic/
  {{mskClusterName}}/{{clusterUUID}}/{{mskTopicName}}"
},
{
  "Sid": "",
  "Effect": "Allow",

```

```
"Action": [
  "kafka-cluster:DescribeGroup"
],
"Resource": "arn:aws:kafka:{{mskClusterRegion}}:{{mskClusterAccount}}:group/
{{mskClusterName}}/{{clusterUUID}}/*"
}
```

Per ulteriori informazioni su come consentire ad altri AWS servizi di accedere alle tue AWS risorse, consulta [Creating a Role to Delegate Permissions to an AWS Service](#) nella IAM User Guide.

Per informazioni su come concedere ad Amazon Data Firehose l'accesso a una destinazione Amazon S3 in un altro account, consulta [the section called "Consegna su più account a una destinazione Amazon S3"](#)

Concedi a Firehose l'accesso alle tabelle Amazon S3

Firehose necessita di un ruolo IAM con autorizzazioni specifiche per accedere alle AWS AWS Glue tabelle e scrivere dati nelle tabelle in un bucket di tabelle Amazon S3. Per scrivere su tabelle in un bucket di tabelle Amazon S3, devi anche fornire al ruolo IAM le autorizzazioni richieste. Le autorizzazioni richieste per il catalogo Amazon S3 Tables dipendono dalla modalità di controllo degli accessi utilizzata:

- Controllo degli accessi IAM: il ruolo di consegna Firehose richiede le autorizzazioni IAM direttamente sulle risorse di Amazon S3 Tables.
- Controllo degli accessi a Lake Formation: il ruolo di consegna Firehose richiede le AWS AWS Lake Formation autorizzazioni per gestire l'accesso alle risorse della tabella. AWS Lake Formation utilizza il proprio modello di autorizzazioni che consente un controllo granulare degli accessi per le risorse del Data Catalog.

Questo ruolo IAM viene configurato quando si crea uno stream Firehose. Scegli la scheda che corrisponde alla tua modalità di controllo degli accessi.

Controllo degli accessi IAM

Se utilizzi la modalità di controllo degli accessi IAM (senza AWS Lake Formation), il ruolo di consegna Firehose richiede le autorizzazioni IAM direttamente sulle risorse di Amazon S3 Tables e sugli oggetti Data Catalog. AWS Glue

Accedi Console di gestione AWS e apri la console IAM all'indirizzo. <https://console.aws.amazon.com/iam/>

Crea una policy e scegli JSON nell'editor delle policy. Aggiungi la seguente politica in linea che concede le autorizzazioni richieste.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3TablesAccessPermission",
      "Effect": "Allow",
      "Action": [
        "s3tables:GetTable",
        "s3tables:GetTableData",
        "s3tables:GetTableMetadataLocation",
        "s3tables:UpdateTableMetadataLocation"
      ],
      "Resource": [
        "arn:aws:s3tables:region:account-id:bucket/*",
        "arn:aws:s3tables:region:account-id:bucket/*/table/*"
      ]
    },
    {
      "Sid": "S3TableBucketAccessPermission",
      "Effect": "Allow",
      "Action": [
        "s3tables:GetTableBucket"
      ],
      "Resource": "arn:aws:s3tables:region:account-id:bucket/*"
    },
    {
      "Sid": "GlueCatalogAccessPermission",
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:UpdateTable"
      ],
      "Resource": [
        "arn:aws:glue:region:account-id:catalog",
        "arn:aws:glue:region:account-id:catalog/s3tablescatalog",
        "arn:aws:glue:region:account-id:catalog/s3tablescatalog/*",
        "arn:aws:glue:region:account-id:database/*",

```

```

        "arn:aws:glue:region:account-id:table/*/*"
    ]
},
{
    "Sid": "S3DeliveryErrorBucketPermission",
    "Effect": "Allow",
    "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3::error-delivery-bucket",
        "arn:aws:s3::error-delivery-bucket/*"
    ]
},
{
    "Sid": "RequiredWhenUsingKinesisDataStreamsAsSource",
    "Effect": "Allow",
    "Action": [
        "kinesis:DescribeStream",
        "kinesis:GetShardIterator",
        "kinesis:GetRecords",
        "kinesis:ListShards"
    ],
    "Resource": "arn:aws:kinesis:region:account-id:stream/stream-name"
},
{
    "Sid": "KMSPermissionForS3TablesEncryption",
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": [
        "arn:aws:kms:region:account-id:key/key-id"
    ],
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "s3.amazonaws.com"
        }
    },

```

```

        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn":
"arn:aws:s3tables:region:account-id:bucket/*/table/*"
        }
    },
    {
        "Sid": "RequiredWhenUsingLambdaForDataTransformation",
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction",
            "lambda:GetFunctionConfiguration"
        ],
        "Resource": "arn:aws:lambda:region:account-id:function:function-
name:function-version"
    },
    {
        "Sid": "CloudWatchLogsPermission",
        "Effect": "Allow",
        "Action": [
            "logs:PutLogEvents"
        ],
        "Resource": "arn:aws:logs:region:account-id:log-group:log-group-name:log-
stream:log-stream-name"
    }
]
}

```

La policy contiene istruzioni che consentono l'accesso ad Amazon Kinesis Data Streams, l'invocazione di funzioni Lambda e l'accesso alle chiavi. AWS KMS Se non si utilizza nessuna di queste risorse, è possibile rimuovere le rispettive istruzioni. Se la registrazione degli errori è abilitata, Amazon Data Firehose invia anche gli errori di consegna dei dati al gruppo di log e CloudWatch ai flussi. È necessario configurare i nomi dei gruppi di log e dei flussi di log per utilizzare questa opzione. Per i nomi dei gruppi di log e dei flussi di log, vedere [Monitora Amazon Data Firehose utilizzando i log CloudWatch](#).

Nella politica in linea, sostituisci i valori segnaposto con i nomi, il Account AWS numero e la regione delle risorse effettivi.

Dopo aver creato la policy, apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>e crea un ruolo IAM con il tipo Servizio AWS di entità affidabile.

Per Servizio o caso d'uso scegli Kinesis. Per il caso d'uso, scegli Kinesis Firehose.

Nella pagina successiva, scegli la policy creata nel passaggio precedente da associare a questo ruolo. Nella pagina di revisione, troverai una politica di fiducia già allegata a questo ruolo che autorizza il servizio Firehose ad assumere questo ruolo. Quando crei il ruolo, Amazon Data Firehose può assumerlo per eseguire le operazioni richieste su AWS Glue e sulle tabelle Amazon S3. Aggiungere il responsabile del servizio Firehose alla politica di attendibilità del ruolo creato. Per ulteriori informazioni, consulta [Consenti a Firehose di assumere un ruolo IAM](#).

Controllo degli accessi a Lake Formation

Se si utilizza la modalità di controllo degli AWS Lake Formation accessi, il ruolo di consegna Firehose necessita AWS Lake Formation delle autorizzazioni per la vendita di credenziali oltre alla policy IAM.

Accedi Console di gestione AWS e apri la console IAM all'indirizzo. <https://console.aws.amazon.com/iam/>

Crea una policy e scegli JSON nell'editor delle policy. Aggiungi la seguente politica in linea che concede autorizzazioni Amazon S3, ad esempio read/write autorizzazioni, autorizzazioni per aggiornare la tabella nel catalogo dati e altre.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3TableAccessViaGlueFederation",
      "Effect": "Allow",
      "Action": [
        "glue:GetTable",
        "glue:GetDatabase",
        "glue:UpdateTable"
      ],
      "Resource": [
        "arn:aws:glue:us-east-1:123456789012:catalog/s3tablescatalog/*",
        "arn:aws:glue:us-east-1:123456789012:catalog/s3tablescatalog",
        "arn:aws:glue:us-east-1:123456789012:catalog",
        "arn:aws:glue:us-east-1:123456789012:database/*",
        "arn:aws:glue:us-east-1:123456789012:table/*/*"
      ]
    }
  ],
}
```

```

{
  "Sid": "S3DeliveryErrorBucketPermission",
  "Effect": "Allow",
  "Action": [
    "s3:AbortMultipartUpload",
    "s3:GetBucketLocation",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:ListBucketMultipartUploads",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::<error delivery bucket>",
    "arn:aws:s3:::<error delivery bucket>/*"
  ]
},
{
  "Sid": "RequiredWhenUsingKinesisDataStreamsAsSource",
  "Effect": "Allow",
  "Action": [
    "kinesis:DescribeStream",
    "kinesis:GetShardIterator",
    "kinesis:GetRecords",
    "kinesis:ListShards"
  ],
  "Resource": "arn:aws:kinesis:us-east-1:123456789012:stream/<stream-name>"
},
{
  "Sid":
  "RequiredWhenDoingMetadataReadsANDDataAndMetadataWriteViaLakeformation",
  "Effect": "Allow",
  "Action": [
    "lakeformation:GetDataAccess"
  ],
  "Resource": "*"
},
{
  "Sid": "RequiredWhenUsingKMSEncryptionForS3ErrorBucketDelivery",
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": [

```

```

    "arn:aws:kms:us-east-1:123456789012:key/<KMS-key-id>"
  ],
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "s3.us-east-1.amazonaws.com"
    },
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::<error delivery
bucket>/prefix*"
    }
  }
},
{
  "Sid": "LoggingInCloudWatch",
  "Effect": "Allow",
  "Action": [
    "logs:PutLogEvents"
  ],
  "Resource": [
    "arn:aws:logs:us-east-1:123456789012:log-group:log-group-name>:log-
stream:<log-stream-name>"
  ]
},
{
  "Sid": "RequiredWhenAttachingLambdaToFirehose",
  "Effect": "Allow",
  "Action": [
    "lambda:InvokeFunction",
    "lambda:GetFunctionConfiguration"
  ],
  "Resource": [
    "arn:aws:lambda:us-east-1:123456789012:function:<function-
name>:<function-version>"
  ]
}
]
}

```

La policy contiene istruzioni che consentono l'accesso ad Amazon Kinesis Data Streams, l'invocazione di funzioni Lambda e l'accesso alle chiavi AWS KMS. Se non si utilizza nessuna di queste risorse, è possibile rimuovere le rispettive istruzioni. Se la registrazione degli errori è abilitata, Amazon Data Firehose invia anche gli errori di consegna dei dati al gruppo di log e CloudWatch.

ai flussi. È necessario configurare i nomi dei gruppi di log e dei flussi di log per utilizzare questa opzione. Per i nomi dei gruppi di log e dei flussi di log, vedere [Monitora Amazon Data Firehose utilizzando i log CloudWatch](#).

Nelle politiche in linea, sostituiscilo `<error_delivery_bucket>` con il nome `aws-account-id` del bucket Amazon S3 e la regione con un numero e una regione Account AWS validi della risorsa.

Oltre alla policy IAM, devi anche concedere al ruolo di consegna Firehose le autorizzazioni richieste in AWS Lake Formation. Per ulteriori informazioni, consulta [Concedere le autorizzazioni sulle tabelle](#).

Dopo aver creato la policy, apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/> e crea un ruolo IAM con Servizio AWS come tipo di entità affidabile.

Per Servizio o caso d'uso scegli Kinesis. Per il caso d'uso, scegli Kinesis Firehose.

Nella pagina successiva, scegli la policy creata nel passaggio precedente da associare a questo ruolo. Nella pagina di revisione, troverai una politica di fiducia già allegata a questo ruolo che autorizza il servizio Firehose ad assumere questo ruolo. Quando crei il ruolo, Amazon Data Firehose può assumerlo per eseguire le operazioni richieste su bucket AWS Glue S3. Aggiungere il responsabile del servizio Firehose alla politica di attendibilità del ruolo creato. Per ulteriori informazioni, consulta [Consenti a Firehose di assumere un ruolo IAM](#).

Concedi a Firehose l'accesso a una destinazione Apache Iceberg Tables

È necessario disporre di un ruolo IAM prima di creare uno stream Firehose e utilizzare Apache Iceberg Tables. AWS Glue Utilizza i seguenti passaggi per creare una policy e un ruolo IAM. Firehose assume questo ruolo IAM ed esegue le azioni richieste.

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo. <https://console.aws.amazon.com/iam/>
2. Crea una policy e scegli JSON nell'editor delle policy.
3. Aggiungi la seguente politica in linea che concede autorizzazioni Amazon S3 come le autorizzazioni, read/write le autorizzazioni per aggiornare la tabella nel catalogo dati, ecc.

Questa policy contiene una dichiarazione che consente l'accesso ad Amazon Kinesis Data Streams, l'utilizzo di funzioni Lambda e l'accesso alle chiavi KMS. Se non si utilizza nessuna di queste risorse, è possibile rimuovere le rispettive istruzioni.

Se la registrazione degli errori è abilitata, Firehose invia anche gli errori di consegna dei dati al gruppo di log e CloudWatch ai flussi. A tale scopo è necessario configurare i nomi dei gruppi di

log e dei flussi di log. Per i nomi dei gruppi di log e dei flussi di log, vedere [Monitora Amazon Data Firehose utilizzando i log CloudWatch](#).

4. Nelle politiche in linea, sostituiscilo *amzn-s3-demo-bucket* con il nome aws-account-id del bucket Amazon S3 e la regione con un numero e una regione Account AWS validi delle risorse.

Note

Questo ruolo concede l'autorizzazione a tutti i database e le tabelle del tuo catalogo dati. Se lo si desidera, è possibile concedere le autorizzazioni solo a tabelle e database specifici.

5. Dopo aver creato la policy, apri la [console IAM](#) e crea un ruolo IAM con Servizio AWS come tipo di entità affidabile.
6. Per Servizio o caso d'uso scegli Kinesis. Per Caso d'uso scegli Kinesis Firehose.
7. Nella pagina successiva, scegli la policy creata nel passaggio precedente da associare a questo ruolo. Nella pagina di revisione, troverai una politica di fiducia già allegata a questo ruolo che autorizza il servizio Firehose ad assumere questo ruolo. Quando crei il ruolo, Amazon Data Firehose può assumerlo per eseguire le operazioni richieste su bucket AWS Glue S3.

Concedi a Firehose l'accesso a una destinazione Amazon Redshift

Fai riferimento a quanto segue quando concedi l'accesso ad Amazon Data Firehose quando utilizzi una destinazione Amazon Redshift.

Argomenti

- [Ruolo e politica di accesso di IAM](#)
- [Accesso VPC a un cluster con provisioning di Amazon Redshift o a un gruppo di lavoro Serverless Amazon Redshift](#)

Ruolo e politica di accesso di IAM

Quando utilizzi una destinazione Amazon Redshift, Amazon Data Firehose invia i dati al tuo bucket S3 come posizione intermedia. Facoltativamente, può utilizzare qualsiasi AWS KMS chiave di tua proprietà per la crittografia dei dati. Amazon Data Firehose carica quindi i dati dal bucket S3 al cluster con provisioning di Amazon Redshift o al gruppo di lavoro Serverless Amazon Redshift. Se la registrazione degli errori è abilitata, Amazon Data Firehose invia anche gli errori di consegna dei dati

al gruppo di log e CloudWatch ai flussi. Amazon Data Firehose utilizza il nome utente e la password Amazon Redshift specificati per accedere al cluster o al gruppo di lavoro Amazon Redshift Serverless forniti e utilizza un ruolo IAM per accedere al bucket, alla chiave, al gruppo di log e ai flussi specificati. CloudWatch È necessario disporre di un ruolo IAM durante la creazione di uno stream Firehose.

Utilizza la seguente politica di accesso per consentire ad Amazon Data Firehose di accedere al tuo bucket e alla tua chiave S3. AWS KMS Se non possiedi il bucket S3, aggiungilo `s3:PutObject` all'elenco delle azioni Amazon S3, che garantiscono al proprietario del bucket l'accesso completo agli oggetti forniti da Amazon Data Firehose. Questa policy ha anche un'istruzione che permette l'accesso a flusso di dati Amazon Kinesis. Se non utilizzi Kinesis Data Firehose come origine dati, puoi rimuovere questa istruzione.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:123456789012:key/key-id"
      ]
    }
  ]
}
```

```

    ],
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "s3.us-east-1.amazonaws.com"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-
demo-bucket/prefix*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kinesis:DescribeStream",
      "kinesis:GetShardIterator",
      "kinesis:GetRecords",
      "kinesis:ListShards"
    ],
    "Resource": "arn:aws:kinesis:us-east-1:123456789012:stream/stream-
name"
  },
  {
    "Effect": "Allow",
    "Action": [
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:us-east-1:123456789012:log-group:log-group-name:log-
stream:log-stream-name"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "lambda:InvokeFunction",
      "lambda:GetFunctionConfiguration"
    ],
    "Resource": [
      "arn:aws:lambda:us-east-1:123456789012:function:func-
tion-name:function-version"
    ]
  }
]

```

}

Per ulteriori informazioni su come consentire ad altri AWS servizi di accedere alle tue AWS risorse, consulta [Creating a Role to Delegate Permissions to an Service nella IAM User Guide](#). AWS

Accesso VPC a un cluster con provisioning di Amazon Redshift o a un gruppo di lavoro Serverless Amazon Redshift

Se il cluster con provisioning Amazon Redshift o il gruppo di lavoro Amazon Redshift serverless si trova in un cloud virtuale privato (VPC), deve essere accessibile pubblicamente con un indirizzo IP pubblico. Inoltre, concedi ad Amazon Data Firehose l'accesso al tuo cluster fornito di Amazon Redshift o al gruppo di lavoro Amazon Redshift Serverless sbloccando gli indirizzi IP di Amazon Data Firehose. Amazon Data Firehose attualmente utilizza un blocco CIDR per ogni regione disponibile.

Region	Blocchi CIDR
Stati Uniti orientali (Ohio)	13.58.135.96/27
Stati Uniti orientali (Virginia settentrionale)	52.70.63.192/27
Stati Uniti occidentali (California settentrionale)	13.57.135.192/27
Stati Uniti occidentali (Oregon)	52.89.255.224/27
AWS GovCloud (Stati Uniti orientali)	18.253.138.96/27
AWS GovCloud (Stati Uniti occidentali)	52.61.204.160/27
Canada (Centrale)	35.183.92.128/27
Canada occidentale (Calgary)	40.176.98.192/27

Region	Blocchi CIDR
Asia Pacifico (Hong Kong)	18.162.221.32/27
Asia Pacifico (Mumbai)	13.232.67.32/27
Asia Pacific (Hyderabad)	18.60.192.128/27
Asia Pacifico (Seul)	13.209.1.64/27
Asia Pacifico (Singapore)	13.228.64.192/27
Asia Pacifico (Sydney)	13.210.67.224/27
Asia Pacifico (Giacarta)	108.136.221.64/27
Asia Pacifico (Tokyo)	13.113.196.224/27
Asia Pacifico (Osaka)	13.208.177.192/27
Asia Pacifico (Thailandia)	43.208.112.96/27
Asia Pacifico (Taipei)	43.212.53.160/27
Cina (Pechino)	52.81.151.32/27
Cina (Ningxia)	161.189.23.64/27
Europa (Zurigo)	16.62.183.32/27
Europa (Francoforte)	35.158.127.160/27
Europa (Irlanda)	52.19.239.192/27
Europa (Londra)	18.130.1.96/27
Europe (Paris)	35.180.1.96/27
Europa (Stoccolma)	13.53.63.224/27
Europa (Spagna)	18.100.71.96/27

Region	Blocchi CIDR
Medio Oriente (Bahrein)	15.185.91.0/27
Messico (centrale)	78.12.207.32/27
Sud America (San Paolo)	18.228.1.128/27
Europa (Milano)	15.161.135.128/27
Africa (Città del Capo)	13.244.121.224/27
Medio Oriente (Emirati Arabi Uniti)	3.28.159.32/27
Israele (Tel Aviv)	51.16.102.0/27
Asia Pacifico (Melbourne)	16.50.161.128/27
Asia Pacifico (Malesia)	43.216.58.0/27

Per ulteriori informazioni su come sbloccare gli indirizzi IP, consulta la fase [Autorizzare l'accesso al cluster](#) nella guida Guida alle operazioni di base di Amazon Redshift.

Concedi a Firehose l'accesso a una destinazione di servizio pubblico OpenSearch

Quando utilizzi una destinazione di OpenSearch servizio, Amazon Data Firehose invia i dati al tuo cluster di OpenSearch servizi e contemporaneamente esegue il backup di tutti i documenti non riusciti o di tutti i documenti nel tuo bucket S3. Se la registrazione degli errori è abilitata, Amazon Data Firehose invia anche gli errori di consegna dei dati al gruppo di log e CloudWatch ai flussi. Amazon Data Firehose utilizza un ruolo IAM per accedere al dominio di OpenSearch servizio, al bucket S3, alla AWS KMS chiave, al gruppo di CloudWatch log e ai flussi specificati. È necessario disporre di un ruolo IAM durante la creazione di uno stream Firehose.

Utilizza la seguente politica di accesso per consentire ad Amazon Data Firehose di accedere al tuo bucket S3, al dominio di OpenSearch servizio e alla chiave AWS KMS. Se non possiedi il bucket S3, aggiungilo `s3:PutObjectACL` all'elenco delle azioni Amazon S3, che garantiscono al proprietario del bucket l'accesso completo agli oggetti forniti da Amazon Data Firehose. Questa policy ha anche

un'istruzione che permette l'accesso a flusso di dati Amazon Kinesis. Se non utilizzi Kinesis Data Firehose come origine dati, puoi rimuovere questa istruzione.

Per ulteriori informazioni su come consentire ad altri AWS servizi di accedere alle tue AWS risorse, consulta [Creating a Role to Delegate Permissions to an Service nella IAM User Guide](#). AWS

Per informazioni su come concedere ad Amazon Data Firehose l'accesso a un cluster di OpenSearch servizi in un altro account, consulta. [the section called “Consegna tra più account a una OpenSearch destinazione del servizio”](#)

Concedere a Firehose l'accesso a una destinazione OpenSearch di servizio in un VPC

Se il tuo dominio di OpenSearch servizio si trova in un VPC, assicurati di concedere ad Amazon Data Firehose le autorizzazioni descritte nella sezione precedente. Inoltre, devi concedere ad Amazon Data Firehose le seguenti autorizzazioni per consentirgli di accedere al VPC del tuo dominio di OpenSearch servizio.

- `ec2:DescribeVpcs`
- `ec2:DescribeVpcAttribute`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2>DeleteNetworkInterface`

Important

Non revoke queste autorizzazioni dopo aver creato lo stream Firehose. Se revochi queste autorizzazioni, il tuo stream Firehose subirà una degradazione o smetterà di fornire dati al tuo dominio di servizio ogni volta che il OpenSearch servizio tenta di eseguire una query o un aggiornamento. ENIs

⚠ Important

Quando specifichi delle sottoreti per la consegna dei dati alla destinazione in un VPC privato, assicurati di avere un numero sufficiente di indirizzi IP liberi nelle sottoreti scelte. Se non è disponibile un indirizzo IP gratuito in una sottorete specificata, Firehose non può creare o ENIs aggiungere dati per la consegna dei dati nel VPC privato e la consegna verrà compromessa o avrà esito negativo.

Quando crei o aggiorni il tuo stream Firehose, specifichi un gruppo di sicurezza che Firehose deve utilizzare per inviare dati al tuo dominio di servizio. OpenSearch È possibile utilizzare lo stesso gruppo di sicurezza utilizzato dal dominio del OpenSearch servizio o uno diverso. Se specifichi un gruppo di sicurezza diverso, assicurati che consenta il traffico HTTPS in uscita al gruppo di sicurezza del dominio del OpenSearch servizio. Assicuratevi inoltre che il gruppo di sicurezza del dominio di OpenSearch servizio consenta il traffico HTTPS proveniente dal gruppo di sicurezza specificato al momento della configurazione dello stream Firehose. Se utilizzi lo stesso gruppo di sicurezza sia per lo stream Firehose che per il dominio di OpenSearch servizio, assicurati che la regola in entrata del gruppo di sicurezza consenta il traffico HTTPS. Per ulteriori informazioni sulle regole dei gruppi di sicurezza, consulta [Regole del gruppo di sicurezza](#) nella documentazione di Amazon VPC.

Concedere a Firehose l'accesso a una destinazione Serverless pubblica OpenSearch

Quando utilizzi una destinazione OpenSearch Serverless, Amazon Data Firehose invia i dati alla OpenSearch tua raccolta Serverless ed esegue contemporaneamente il backup di tutti i documenti non riusciti o di tutti i documenti nel tuo bucket S3. Se la registrazione degli errori è abilitata, Amazon Data Firehose invia anche gli errori di consegna dei dati al gruppo di log e CloudWatch ai flussi. Amazon Data Firehose utilizza un ruolo IAM per accedere alla raccolta OpenSearch Serverless, al bucket S3, alla AWS KMS chiave, al gruppo di log e CloudWatch ai flussi specificati. È necessario disporre di un ruolo IAM durante la creazione di uno stream Firehose.

Utilizza la seguente politica di accesso per consentire ad Amazon Data Firehose di accedere al tuo bucket S3, al dominio OpenSearch Serverless e alla chiave AWS KMS. Se non possiedi il bucket S3, aggiungilo `s3:PutObjectACL` all'elenco delle azioni Amazon S3, che garantiscono al proprietario del bucket l'accesso completo agli oggetti forniti da Amazon Data Firehose. Questa policy ha anche un'istruzione che permette l'accesso a flusso di dati Amazon Kinesis. Se non utilizzi Kinesis Data Firehose come origine dati, puoi rimuovere questa istruzione.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:123456789012:key/key-id"
      ],
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "s3.us-east-1.amazonaws.com"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-
demo-bucket/prefix*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kinesis:DescribeStream",

```

```

        "kinesis:GetShardIterator",
        "kinesis:GetRecords",
        "kinesis:ListShards"
    ],
    "Resource": "arn:aws:kinesis:us-east-1:123456789012:stream/stream-name"
},
{
    "Effect": "Allow",
    "Action": [
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:us-east-1:123456789012:log-group:log-group-name:log-
stream:log-stream-name"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "lambda:InvokeFunction",
        "lambda:GetFunctionConfiguration"
    ],
    "Resource": [
        "arn:aws:lambda:us-east-1:123456789012:function:func-
name:func-version"
    ]
},
{
    "Effect": "Allow",
    "Action": "aoss:APIAccessAll",
    "Resource": "arn:aws:aoss:us-east-1:123456789012:collection/collection-
id"
}
]
}

```

Oltre alla politica di cui sopra, devi anche configurare Amazon Data Firehose per avere le seguenti autorizzazioni minime assegnate in una policy di accesso ai dati:

```
[
{
```

```
"Rules":[
  {
    "ResourceType":"index",
    "Resource":[
      "index/target-collection/target-index"
    ],
    "Permission":[
      "aoss:WriteDocument",
      "aoss:UpdateIndex",
      "aoss>CreateIndex"
    ]
  }
],
"Principal":[
  "arn:aws:sts::123456789012:assumed-role/firehose-delivery-role-name/*"
]
}
```

Per ulteriori informazioni su come consentire ad altri AWS servizi di accedere alle tue AWS risorse, consulta [Creating a Role to Delegate Permissions to an AWS Service](#) nella IAM User Guide.

Concedi a Firehose l'accesso a una destinazione OpenSearch Serverless in un VPC

Se la tua raccolta OpenSearch Serverless è in un VPC, assicurati di concedere ad Amazon Data Firehose le autorizzazioni descritte nella sezione precedente. Inoltre, devi concedere ad Amazon Data Firehose le seguenti autorizzazioni per consentirgli di accedere al VPC della tua OpenSearch collezione Serverless.

- ec2:DescribeVpcs
- ec2:DescribeVpcAttribute
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkInterfaces
- ec2:CreateNetworkInterface
- ec2:CreateNetworkInterfacePermission
- ec2>DeleteNetworkInterface

⚠ Important

Non revocate queste autorizzazioni dopo aver creato lo stream Firehose. Se revochi queste autorizzazioni, il tuo stream Firehose subirà una degradazione o smetterà di fornire dati al tuo dominio di servizio ogni volta che il OpenSearch servizio tenta di eseguire una query o un aggiornamento. ENIs

⚠ Important

Quando specifichi delle sottoreti per la consegna dei dati alla destinazione in un VPC privato, assicurati di avere un numero sufficiente di indirizzi IP liberi nelle sottoreti scelte. Se non è disponibile un indirizzo IP gratuito in una sottorete specificata, Firehose non può creare o ENIs aggiungere dati per la consegna dei dati nel VPC privato e la consegna verrà compromessa o avrà esito negativo.

Quando crei o aggiorni il tuo stream Firehose, specifichi un gruppo di sicurezza da utilizzare per l'invio di dati alla tua raccolta Serverless. OpenSearch È possibile utilizzare lo stesso gruppo di sicurezza utilizzato dalla raccolta OpenSearch Serverless o uno diverso. Se specificate un gruppo di sicurezza diverso, assicuratevi che consenta il traffico HTTPS in uscita al gruppo di sicurezza della raccolta OpenSearch Serverless. Assicuratevi inoltre che il gruppo di sicurezza della collezione OpenSearch Serverless consenta il traffico HTTPS proveniente dal gruppo di sicurezza specificato al momento della configurazione dello stream Firehose. Se utilizzi lo stesso gruppo di sicurezza sia per lo stream Firehose che per la raccolta OpenSearch Serverless, assicurati che la regola in entrata del gruppo di sicurezza consenta il traffico HTTPS. Per ulteriori informazioni sulle regole dei gruppi di sicurezza, consulta [Regole del gruppo di sicurezza](#) nella documentazione di Amazon VPC.

Concedi a Firehose l'accesso a una destinazione Splunk

Quando utilizzi una destinazione Splunk, Amazon Data Firehose fornisce dati all'endpoint Splunk HTTP Event Collector (HEC). Inoltre, esegue il backup di tali dati nel bucket Amazon S3 da te specificato e, facoltativamente, puoi utilizzare una AWS KMS chiave di tua proprietà per la crittografia lato server di Amazon S3. Se la registrazione degli errori è abilitata, Firehose invia gli errori di consegna dei CloudWatch dati ai flussi di log. È possibile utilizzarlo anche AWS Lambda per la trasformazione dei dati.

Se utilizzi un AWS load balancer, assicurati che sia un Classic Load Balancer o un Application Load Balancer. Inoltre, abilita sessioni permanenti basate sulla durata con la scadenza dei cookie disabilitata per Classic Load Balancer e la scadenza è impostata al massimo (7 giorni) per Application Load Balancer. [Per informazioni su come eseguire questa operazione, consulta *Duration-Based Session Stickiness for Classic Load Balancer* o un *Application Load Balancer*.](#)

È necessario disporre di un ruolo IAM quando si crea uno stream Firehose. Firehose assume quel ruolo IAM e ottiene l'accesso al bucket, alla chiave, al gruppo di log e CloudWatch ai flussi specificati.

Utilizza la seguente politica di accesso per consentire ad Amazon Data Firehose di accedere al tuo bucket S3. Se non possiedi il bucket S3, aggiungilo `s3:PutObjectAc1` all'elenco delle azioni Amazon S3, che garantiscono al proprietario del bucket l'accesso completo agli oggetti forniti da Amazon Data Firehose. Questa policy concede inoltre ad Amazon Data Firehose l'accesso CloudWatch alla registrazione degli errori e AWS Lambda alla trasformazione dei dati. La policy ha anche un'istruzione che permette l'accesso a flusso di dati Amazon Kinesis. Se non utilizzi Kinesis Data Firehose come origine dati, puoi rimuovere questa istruzione. Amazon Data Firehose non utilizza IAM per accedere a Splunk. Per accedere a Splunk, utilizza il token HEC.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
```

```

    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": [
      "arn:aws:kms:us-east-1:123456789012:key/key-id"
    ],
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "s3.us-east-1.amazonaws.com"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-
demo-bucket/prefix*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kinesis:DescribeStream",
      "kinesis:GetShardIterator",
      "kinesis:GetRecords",
      "kinesis:ListShards"
    ],
    "Resource": "arn:aws:kinesis:us-east-1:123456789012:stream/stream-
name"
  },
  {
    "Effect": "Allow",
    "Action": [
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:us-east-1:123456789012:log-group:log-group-name:log-
stream:*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "lambda:InvokeFunction",
      "lambda:GetFunctionConfiguration"
    ]
  },

```

```

    "Resource": [
      "arn:aws:lambda:us-east-1:123456789012:function:func-
name:func-version"
    ]
  }
]
}

```

Per ulteriori informazioni su come consentire ad altri AWS servizi di accedere alle tue AWS risorse, consulta [Creating a Role to Delegate Permissions to an AWS Service](#) nella IAM User Guide.

Accesso a Splunk in VPC

Se la piattaforma Splunk si trova in un VPC, deve essere accessibile pubblicamente con un indirizzo IP pubblico. Inoltre, concedi ad Amazon Data Firehose l'accesso alla tua piattaforma Splunk sbloccando gli indirizzi IP di Amazon Data Firehose. Amazon Data Firehose attualmente utilizza i seguenti blocchi CIDR.

Region	Blocchi CIDR
Stati Uniti orientali (Ohio)	18.216.68.160/27, 18.216.170.64/27, 18.216.170.96/27 \
Stati Uniti orientali (Virginia settentrionale)	34.238.188.128/26, 34.238.188.192/26, 34.238.195.0/26
Stati Uniti occidentali (California settentrionale)	13.57.180.0/26
Stati Uniti occidentali (Oregon)	34.216.24.32/27, 34.216.24.192/27, 34.216.24.224/27
AWS GovCloud (Stati Uniti orientali)	18.253.138.192/26
AWS GovCloud (Stati Uniti occidentali)	52.61.204.192/26

Region	Blocchi CIDR
Asia Pacifico (Hong Kong)	18.162.221.64/26
Asia Pacifico (Mumbai)	13.232.67.64/26
Asia Pacifico (Seoul)	13.209.71.0/26
Asia Pacifico (Singapore)	13.229.187.128/26
Asia Pacifico (Sydney)	13.211.12.0/26
Asia Pacifico (Thailandia)	43.208.112.128/26
Asia Pacifico (Tokyo)	13.230.21.0/27, 13.230.21.32/27
Canada (Centrale)	35.183.92.64/26
Canada occidentale (Calgary)	40.176.98.128/26
Europa (Francoforte)	18.194.95.192/27, 18.194.95.224/27, 18.195.48.0/27
Europa (Irlanda)	34.241.197.32/27, 34.241.197.64/27, 34.241.197.96/27
Europa (Londra)	18.130.91.0/26
Europa (Parigi)	35.180.112.0/26
Europa (Spagna)	18.100.194.0/26
Europa (Stoccolma)	13.53.191.0/26
Medio Oriente (Bahrein)	15.185.91.64/26
Messico (centrale)	78.12.207.64/26
Sud America (San Paolo)	18.228.1.192/26

Region	Blocchi CIDR
Europa (Milano)	15.161.135.192/26
Africa (Città del Capo)	13.244.165.128/26
Asia Pacifico (Osaka)	13.208.217.0/26
Cina (Pechino)	52.81.151.64/26
Cina (Ningxia)	161.189.23.128/26
Asia Pacifico (Giacarta)	108.136.221.128/26
Medio Oriente (Emirati Arabi Uniti)	3.28.159.64/26
Israele (Tel Aviv)	51.16.102.64/26
Europa (Zurigo)	16.62.183.64/26
Asia Pacifico (Hyderabad)	18.60.192.192/26
Asia Pacifico (Melbourne)	16.50.161.192/26
Asia Pacifico (Malesia)	43.216.44.192/26

Inserisci i log di flusso VPC in Splunk utilizzando Amazon Data Firehose

[Per ulteriori informazioni su come creare un abbonamento ai log di flusso VPC, pubblicare su Firehose e inviare i log di flusso VPC a una destinazione supportata, consulta la sezione Inserimento dei log di flusso VPC in Splunk utilizzando Amazon Data Firehose.](#)

Accesso a Snowflake o all'endpoint HTTP

Non esiste un sottoinsieme di [intervalli di indirizzi AWS IP](#) specifici per Amazon Data Firehose quando la destinazione è un endpoint HTTP o un cluster pubblico Snowflake.

Per aggiungere Firehose a un elenco di indirizzi consentiti per i cluster Snowflake pubblici o agli endpoint HTTP o HTTPS pubblici, aggiungi tutti gli intervalli di [indirizzi AWS IP](#) correnti alle tue regole di ingresso.

Note

Le notifiche non provengono sempre da indirizzi IP nella stessa regione dell'argomento associato. AWS È necessario includere l'intervallo di indirizzi AWS IP per tutte le regioni.

Concedi a Firehose l'accesso a una destinazione Snowflake

Quando utilizzi Snowflake come destinazione, Firehose invia i dati a un account Snowflake utilizzando l'URL del tuo account Snowflake. Inoltre, esegue il backup dei dati di errore nel bucket Amazon Simple Storage Service da te specificato e, facoltativamente, puoi utilizzare una AWS Key Management Service chiave di tua proprietà per la crittografia lato server di Amazon S3. Se la registrazione degli errori è abilitata, Firehose invia gli errori di consegna dei CloudWatch dati ai flussi di log.

È necessario disporre di un ruolo IAM prima di creare uno stream Firehose. Firehose assume quel ruolo IAM e ottiene l'accesso al bucket, alla chiave, al gruppo e CloudWatch agli stream Logs specificati. Utilizza la seguente politica di accesso per consentire a Firehose di accedere al tuo bucket S3. Se non possiedi il bucket S3, aggiungilo `s3:PutObjectACL` all'elenco delle azioni di Amazon Simple Storage Service, che garantiscono al proprietario del bucket l'accesso completo agli oggetti forniti da Firehose. Questa politica concede inoltre a Firehose l'accesso CloudWatch per la registrazione degli errori. La policy ha anche un'istruzione che permette l'accesso a flusso di dati Amazon Kinesis. Se non utilizzi Kinesis Data Firehose come origine dati, puoi rimuovere questa istruzione. Firehose non utilizza IAM per accedere a Snowflake. Per accedere a Snowflake, utilizza l'URL dell'account Snowflake e l>ID PrivateLink Vpce nel caso di un cluster privato.

JSON

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

```

        "Action": [
            "s3:AbortMultipartUpload",
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:ListBucketMultipartUploads",
            "s3:PutObject"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": [
            "arn:aws:kms:us-east-1:123456789012:key/key-id"
        ],
        "Condition": {
            "StringEquals": {
                "kms:ViaService": "s3.us-east-1.amazonaws.com"
            },
            "StringLike": {
                "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket/prefix*"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "kinesis:DescribeStream",
            "kinesis:GetShardIterator",
            "kinesis:GetRecords",
            "kinesis:ListShards"
        ],
        "Resource": "arn:aws:kinesis:us-east-1:123456789012:stream/stream-
name"
    },
    {
        "Effect": "Allow",

```

```

    "Action": [
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:us-east-1:123456789012:log-group:log-group-name:log-
stream:*"
    ]
  }
]
}

```

Per ulteriori informazioni su come consentire ad altri AWS servizi di accedere alle tue AWS risorse, consulta [Creating a Role to Delegate Permissions to an Service nella IAM User Guide](#). AWS

Accesso a Snowflake in VPC

Se il cluster Snowflake è abilitato al collegamento privato, Firehose utilizzerà uno dei seguenti endpoint VPC al momento della creazione del collegamento privato per fornire dati al cluster privato senza passare attraverso la rete Internet pubblica. A tal fine, crea regole di rete Snowflake per consentire l'accesso da quanto segue al cluster in cui si trova il cluster. AwsVpceIds Regione AWS

Per ulteriori informazioni, consulta [Creazione di regole di rete](#) nella Guida per l'utente di Snowflake.

ID degli endpoint VPC da utilizzare in base alle regioni in cui si trova il cluster

Regione AWS	VPCE IDs
Stati Uniti orientali (Ohio)	vpce-0d96cafcd96a50aeb
	vpce-0cec34343d48f537b
Stati Uniti orientali (Virginia settentrionale)	vpce-0b4d7e8478e141ba8
	vpce-0b75cd681fb507352
	vpce-01c03e63820ec00d8
	vpce-0c2cfc51dc2882422
	vpce-06ca862f019e4e056
	vpce-020cda0cfa63f8d1c

Regione AWS	VPCE IDs
	vpce-0b80504a1a783cd70
	vpce-0289b9ff0b5259a96
	vpce-0d7add8628bd69a12
	vpce-02bfb5966cc59b2af
	vpce-09e707674af878bf2
	vpce-049b52e96cc1a2165
	vpce-0bb6c7b7a8a86cdbb
	vpce-03b22d599f51e80f3
	vpce-01d60dc60fc106fe1
	vpce-0186d20a4b24ecbef
	vpce-0533906401a36e416
	vpce-05111fb13d396710e
	vpce-0694613f4fbd6f514
	vpce-09b21cb25fe4cc4f4
	vpce-06029c3550e4d2399
	vpce-00961862a21b033da
	vpce-01620b9ae33273587
	vpce-078cf4ec226880ac9
	vpce-0d711bf076ce56381
	vpce-066b7e13cbfca6f6e
	vpce-0674541252d9ccc26

Regione AWS	VPCE IDs
	vpce-03540b88dedb4b000 vpce-0b1828e79ad394b95 vpce-0dc0e6f001fb1a60d vpce-0d8f82e71a244098a vpce-00e374d9e3f1af5ce vpce-0c1e3d6631ddb442f
Stati Uniti occidentali (Oregon)	vpce-0f60f72da4cd1e4e7 vpce-0c60d21eb8b1669fd vpce-01c4e3e29afdafbef vpce-0cc6bf2a88da139de vpce-0797e08e169e50662 vpce-033cbe480381b5c0e vpce-00debbdd8f9eb10a5 vpce-08ec2f386c809e889 vpce-0856d14310857b545
Europa (Francoforte)	vpce-068dbb7d71c9460fb vpce-0a7a7f095942d4ec9
Europa (Irlanda)	vpce-06857e59c005a6276 vpce-04390f4f8778b75f2 VPCE-011fd2b1f0aa172fd

Regione AWS	VPCE IDs
Asia Pacifico (Tokyo)	vpce-06369e5258144e68a vpce-0f2363cdb8926fbe8
Asia Pacifico (Singapore)	vpce-049cd46cce7a12d52 vpce-0e8965a1a4bdb8941
Asia Pacifico (Seul)	vpce-0aa444d9001e1faa1 vpce-04a49d4dcfd02b884
Asia Pacifico (Sydney)	vpce-048a60a182c52be63 vpce-03c19949787fd1859
Asia Pacifico (Mumbai)	vpce-0d68cb822f6f0db68 vpce-0517d32692ffcbde2
Europa (Londra)	vpce-0fd1874a0ba3b9374 vpce-08091b1a85e206029
Sud America (San Paolo)	vpce-065169b8144e4f12e vpce-0493699f0e5762d63
Canada (Centrale)	vpce-07e6ed81689d5271f vpce-0f53239730541394c
Europa (Parigi)	vpce-09419680077e6488a vpce-0ea81ba2c08140c14
Asia Pacifico (Osaka)	vpce-0a9f003e6a7e38c05 vpce-02886510b897b1c5a

Regione AWS	VPCE IDs
Europa (Stoccolma)	vpce-0d96410833219025a vpce-060a32f9a75ba969f
Asia Pacifico (Giacarta)	vpce-00add4b9a25e5c649 vpce-004ae2de34338a856

Concedere a Firehose l'accesso a una destinazione endpoint HTTP

Puoi utilizzare Amazon Data Firehose per fornire dati a qualsiasi destinazione di endpoint HTTP. Amazon Data Firehose esegue inoltre il backup di tali dati nel bucket Amazon S3 da te specificato e, facoltativamente, puoi utilizzare AWS KMS una chiave di tua proprietà per la crittografia lato server di Amazon S3. Se la registrazione degli errori è abilitata, Amazon Data Firehose invia gli errori di consegna dei dati ai CloudWatch tuoi flussi di log. Puoi utilizzarlo anche AWS Lambda per la trasformazione dei dati.

È necessario disporre di un ruolo IAM durante la creazione di uno stream Firehose. Amazon Data Firehose assume il ruolo IAM e ottiene l'accesso al bucket, alla chiave, al gruppo di log e CloudWatch ai flussi specificati.

Utilizza la seguente politica di accesso per consentire ad Amazon Data Firehose di accedere al bucket S3 che hai specificato per il backup dei dati. Se non possiedi il bucket S3, aggiungilo `s3:PutObjectACL` all'elenco delle azioni Amazon S3, che garantiscono al proprietario del bucket l'accesso completo agli oggetti forniti da Amazon Data Firehose. Questa policy concede inoltre ad Amazon Data Firehose l'accesso CloudWatch alla registrazione degli errori e AWS Lambda alla trasformazione dei dati. La policy ha anche un'istruzione che permette l'accesso a flusso di dati Amazon Kinesis. Se non utilizzi Kinesis Data Firehose come origine dati, puoi rimuovere questa istruzione.

Important

Amazon Data Firehose non utilizza IAM per accedere alle destinazioni degli endpoint HTTP di proprietà di fornitori di servizi terzi supportati, tra cui Datadog, Dynatrace, LogicMonitor MongoDB, New Relic, Splunk o Sumo Logic. Per accedere a una destinazione endpoint HTTP specificata di proprietà di un fornitore di servizi terzo supportato, contatta tale fornitore

di servizi per ottenere la chiave API o la chiave di accesso necessaria per abilitare la consegna dei dati a quel servizio da Amazon Data Firehose.

Per ulteriori informazioni su come consentire ad altri AWS servizi di accedere alle tue AWS risorse, consulta [Creating a Role to Delegate Permissions to an AWS Service](#) nella IAM User Guide.

⚠ Important

Attualmente Amazon Data Firehose NON supporta la consegna di dati agli endpoint HTTP in un VPC.

Consegna su più account da Amazon MSK

Quando crei uno stream Firehose dal tuo account Firehose (ad esempio, Account B) e la tua origine è un cluster MSK in un altro AWS account (Account A), devi avere le seguenti configurazioni.

Account A:

1. Nella console Amazon MSK scegli il cluster con provisioning, quindi scegli Proprietà.
2. In Impostazioni di rete, scegli Modifica e attiva Connettività multi-VPC.
3. In Impostazioni di sicurezza scegli Modifica policy del cluster.
 - a. Se il cluster non ha già configurato una policy, seleziona Includi il principale del servizio Firehose e Abilita la distribuzione S3 multi-account Firehose. Console di gestione AWS Genererà automaticamente una policy con le autorizzazioni appropriate.
 - b. Se il cluster ha già una policy configurata, aggiungi le seguenti autorizzazioni alla policy esistente:

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::us-east-1:role/mskaasTestDeliveryRole"
  },
  "Action": [
    "kafka:GetBootstrapBrokers",
    "kafka:DescribeCluster",
    "kafka:DescribeClusterV2",
```

```

    "kafka-cluster:Connect"
  ],
  "Resource": "arn:aws:kafka:us-east-1:123456789012:cluster/D0-NOT-TOUCH-
mkaas-provisioned-privateLink/xxxxxxxx-2f3a-462a-ba09-xxxxxxxx-20" // ARN
of the cluster
},
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws::iam::us-east-1:role/mskaasTestDeliveryRole"
  },
  "Action": [
    "kafka-cluster:DescribeTopic",
    "kafka-cluster:DescribeTopicDynamicConfiguration",
    "kafka-cluster:ReadData"
  ],
  "Resource": "arn:aws:kafka:us-east-1:arn:topic/D0-NOT-TOUCH-mkaas-
provisioned-privateLink/xxxxxxxx-2f3a-462a-ba09-xxxxxxxx-20/*" //topic of the
cluster
},
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::us-east-1:role/mskaasTestDeliveryRole"
  },
  "Action": "kafka-cluster:DescribeGroup",
  "Resource": "arn:aws:kafka:us-east-1:arn:group/D0-NOT-TOUCH-mkaas-
provisioned-privateLink/xxxxxxxx-2f3a-462a-ba09-xxxxxxxx-20/*" //topic of
the cluster
},
}

```

4. In Principale AWS , inserisci l'ID principale dell'Account B.
5. In Argomento, specificate l'argomento di Apache Kafka da cui desiderate che lo stream Firehose acquisisca i dati. Una volta creato lo stream Firehose, non è possibile aggiornare questo argomento.
6. Scegliere Salva modifiche.

Account B:

1. Nella console Firehose, scegliete Crea stream Firehose utilizzando l'account B.

2. In Origine, scegli Amazon Managed Streaming for Apache Kafka.
3. In Impostazioni di origine, per il cluster Amazon Managed Streaming for Apache Kafka, inserisci l'ARN del cluster Amazon MSK nell'Account A.
4. In Argomento, specificate l'argomento di Apache Kafka da cui desiderate che lo stream Firehose acquisisca i dati. Una volta creato lo stream Firehose, non è possibile aggiornare questo argomento.
5. In Delivery stream name, specificate il nome del vostro stream Firehose.

Nell'Account B, quando crei lo stream Firehose, devi disporre di un ruolo IAM (creato di default quando usi il Console di gestione AWS) che conceda allo stream Firehose l'accesso in «lettura» al cluster Amazon MSK multiaccount per l'argomento configurato.

Di seguito è riportato ciò che viene configurato dalla Console di gestione AWS:

```
{
  "Sid": "",
  "Effect": "Allow",
  "Action": [
    "kafka:GetBootstrapBrokers",
    "kafka:DescribeCluster",
    "kafka:DescribeClusterV2",
    "kafka-cluster:Connect"
  ],
  "Resource": "arn:aws:kafka:us-east-1:arn:aws::cluster/D0-N0T-TOUCH-mskaas-
provisioned-privateLink/xxxxxxxx-2f3a-462a-ba09-xxxxxxxx-20/*" //topic of the
cluster
},
{
  "Sid": "",
  "Effect": "Allow",
  "Action": [
    "kafka-cluster:DescribeTopic",
    "kafka-cluster:DescribeTopicDynamicConfiguration",
    "kafka-cluster:ReadData"
  ],
  "Resource": "arn:aws:kafka:us-east-1:arn:aws::topic/D0-N0T-TOUCH-mskaas-
provisioned-privateLink/xxxxxxxx-2f3a-462a-ba09-xxxxxxxx-20/mskaas_test_topic" //
topic of the cluster
},
{
  "Sid": "",
```

```
"Effect": "Allow",
"Action": [
    "kafka-cluster:DescribeGroup"
],
"Resource": "arn:aws:kafka:us-east-1:arn:aws::group/D0-N0T-T0UCH-mskaas-
provisioned-privateLink/xxxxxxxx-2f3a-462a-ba09-xxxxxxxx-20/*" //topic of the
cluster
},
}
```

Successivamente, puoi completare la fase facoltativa di configurazione della trasformazione del record e della conversione del formato del record. Per ulteriori informazioni, consulta [\(Facoltativo\) Configurare la trasformazione dei record e la conversione del formato.](#)

Consegna su più account a una destinazione Amazon S3

Puoi utilizzare AWS CLI o Amazon Data Firehose APIs per creare uno stream Firehose in un AWS account con una destinazione Amazon S3 in un account diverso. La procedura seguente mostra un esempio di configurazione di uno stream Firehose di proprietà dell'account A per fornire dati a un bucket Amazon S3 di proprietà dell'account B.

1. Crea un ruolo IAM nell'account A utilizzando i passaggi descritti in [Concedere l'accesso a Firehose a una destinazione Amazon S3.](#)

Note

In questo caso il bucket Amazon S3 specificato nella policy di accesso è di proprietà dell'account B. Assicurati di aggiungere `s3:PutObjectAc1` all'elenco delle azioni di Amazon S3 nella policy di accesso, che garantisce all'account B l'accesso completo agli oggetti forniti da Amazon Data Firehose. Questa autorizzazione è necessaria per la distribuzione multi-account. Amazon Data Firehose imposta l'intestazione `x-amz-acl ""` della richiesta su `"». bucket-owner-full-control`

2. Per consentire l'accesso dal ruolo IAM creato in precedenza, crea una policy del bucket S3 nell'account B. Il codice seguente è un esempio di policy del bucket. Per ulteriori informazioni, consulta [Utilizzo delle policy di bucket e delle policy utente.](#)

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PolicyID",
  "Statement": [
    {
      "Sid": "StmtID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/iam-role-name"
      },
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}
```

3. Crea uno stream Firehose nell'account A utilizzando il ruolo IAM creato nel passaggio 1.

Consegna tra più account a una OpenSearch destinazione del servizio

Puoi utilizzare AWS CLI o Amazon Data Firehose APIs per creare uno stream Firehose in un AWS account con una destinazione di OpenSearch servizio in un account diverso. La procedura seguente mostra un esempio di come è possibile creare uno stream Firehose con l'account A e configurarlo per fornire dati a una destinazione del OpenSearch servizio di proprietà dell'account B.

1. Crea un ruolo IAM nell'account A utilizzando le fasi descritte in [the section called “Concedi a Firehose l'accesso a una destinazione di servizio pubblico OpenSearch”](#).
2. Per consentire l'accesso dal ruolo IAM creato nel passaggio precedente, crea una policy di OpenSearch servizio nell'account B. Il seguente JSON è un esempio.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/firehose_delivery_role "
      },
      "Action": "es:ESHttpGet",
      "Resource": [
        "arn:aws:es:us-east-1:123456789012:domain/cross-account-cluster/_all/_settings",
        "arn:aws:es:us-east-1:123456789012:domain/cross-account-cluster/_cluster/stats",
        "arn:aws:es:us-east-1:123456789012:domain/cross-account-cluster/roletest*/_mapping/roletest",
        "arn:aws:es:us-east-1:123456789012:domain/cross-account-cluster/_nodes",
        "arn:aws:es:us-east-1:123456789012:domain/cross-account-cluster/_nodes/stats",
        "arn:aws:es:us-east-1:123456789012:domain/cross-account-cluster/_nodes/*/stats",
        "arn:aws:es:us-east-1:123456789012:domain/cross-account-cluster/_stats",
        "arn:aws:es:us-east-1:123456789012:domain/cross-account-cluster/roletest*/_stats",
        "arn:aws:es:us-east-1:123456789012:domain/cross-account-cluster/"
      ]
    }
  ]
}
```

3. Crea uno stream Firehose nell'account A utilizzando il ruolo IAM creato nel passaggio 1. Quando crei lo stream Firehose, usa AWS CLI o Amazon Data Firehose APIs e specifica il `ClusterEndpoint` campo anziché `Service`. `DomainARN` OpenSearch

Note

Per creare uno stream Firehose in un AWS account con una destinazione di OpenSearch servizio in un account diverso, devi utilizzare AWS CLI o Amazon Data Firehose. APIs Non è possibile utilizzare il Console di gestione AWS per creare questo tipo di configurazione tra account.

Utilizzo dei tag per controllare l'accesso

Puoi utilizzare l'Conditionamento (o Condition blocco) opzionale in una policy IAM per ottimizzare l'accesso alle operazioni di Amazon Data Firehose in base a chiavi e valori dei tag. Le seguenti sottosezioni descrivono come eseguire questa operazione per le diverse operazioni di Amazon Data Firehose. Per ulteriori informazioni sull'utilizzo dell'elemento `Condition` e degli operatori che puoi utilizzare al suo interno, consulta [Elementi della policy JSON di IAM: condizione](#).

CreateDeliveryStream

Per l'operazione `CreateDeliveryStream`, utilizza la chiave di condizione `aws:RequestTag`. Nel seguente esempio, `MyKey` e `MyValue` rappresentano la chiave e il valore corrispondente del tag. Per ulteriori informazioni, consulta [Comprendi le nozioni di base sui tag](#)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "firehose:CreateDeliveryStream",
      "firehose:TagDeliveryStream"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
```

```
        "aws:RequestTag/MyKey": "MyValue"
    }
  }
}]
}
```

TagDeliveryStream

Per l'operazione `TagDeliveryStream`, utilizza la chiave di condizione `aws:TagKeys`. Nel seguente esempio, `MyKey` è un esempio di chiave di tag.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "firehose:TagDeliveryStream",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": "MyKey"
        }
      }
    }
  ]
}
```

UntagDeliveryStream

Per l'operazione `UntagDeliveryStream`, utilizza la chiave di condizione `aws:TagKeys`. Nel seguente esempio, `MyKey` è un esempio di chiave di tag.

JSON

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

```
{
  "Effect": "Allow",
  "Action": "firehose:UntagDeliveryStream",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:TagKeys": "MyKey"
    }
  }
}
```

ListDeliveryStreams

Non puoi utilizzare il controllo degli accessi basato su tag con `ListDeliveryStreams`.

Altre operazioni

Per tutte le operazioni di Firehose diverse da `CreateDeliveryStream`, `TagDeliveryStream`, e `UntagDeliveryStream`, utilizzare il tasto `aws:RequestTag` condition. Nel seguente esempio, `MyKey` e `MyValue` rappresentano la chiave e il valore corrispondente del tag.

`ListDeliveryStreams`, utilizzate il tasto `firehose:ResourceTag` condition per controllare l'accesso in base ai tag di quel flusso Firehose.

Nel seguente esempio, `MyKey` e `MyValue` rappresentano la chiave e il valore corrispondente del tag. La policy si applicherebbe solo ai flussi Data Firehose con un tag denominato `MyKey` con un valore di `MyValue`. Per ulteriori informazioni sul controllo dell'accesso in base ai tag delle risorse, consulta [Controlling access to AWS resources using tags](#) nella IAM User Guide.

Effettua l'autenticazione con Gestione dei segreti AWS Amazon Data Firehose

Amazon Data Firehose si integra con Gestione dei segreti AWS per fornire un accesso sicuro ai tuoi segreti e automatizzare la rotazione delle credenziali. Questa integrazione consente a Firehose di recuperare un segreto da Secrets Manager in fase di esecuzione per connettersi alle destinazioni di streaming menzionate in precedenza e distribuire i flussi di dati. In questo modo, i tuoi segreti non sono visibili in testo semplice durante il flusso di lavoro di creazione di stream Console di gestione

AWS né nei parametri dell'API. Fornisce una pratica sicura per gestire i tuoi segreti e ti solleva da complesse attività di gestione delle credenziali, come la configurazione di funzioni Lambda personalizzate per gestire le rotazioni delle password.

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

Argomenti

- [Comprendi i segreti](#)
- [Creazione di un segreto](#)
- [Usa il segreto](#)
- [Ruota il segreto](#)

Comprendi i segreti

Un segreto può essere una password, un set di credenziali come nome utente e password, un OAuth token o altre informazioni segrete archiviate in forma crittografata in Secrets Manager.

Per ogni destinazione, è necessario specificare la coppia chiave-valore segreta nel formato JSON corretto, come illustrato nella sezione seguente. Amazon Data Firehose non riuscirà a connettersi alla tua destinazione se il tuo segreto non ha il formato JSON corretto per la destinazione.

Formato segreto per database come MySQL e PostgreSQL

```
{
  "username": "<username>",
  "password": "<password>"
}
```

Formato segreto per il cluster Amazon Redshift Provisioned e il gruppo di lavoro Amazon Redshift Serverless

```
{
  "username": "<username>",
  "password": "<password>"
}
```

Formato segreto per Splunk

```
{
```

```
"hec_token": "<hec token>"
}
```

Formato segreto per Snowflake

```
{
  "user": "<snowflake-username>",
  "private_key": "<snowflake-private-key>", // without the beginning and ending
private key, remove all spaces and newlines
  "key_passphrase": "<snowflake-private-key-passphrase>" // optional
}
```

Formato segreto per endpoint HTTP, Coralogix, Datadog, Dynatrace, Elastic, Honeycomb, Logz.io, MongoDB Cloud e New Relic LogicMonitor

```
{
  "api_key": "<apikey>"
}
```

Creazione di un segreto

Per creare un segreto, segui i passaggi in [Creare un Gestione dei segreti AWS segreto nella Guida](#) per l'Gestione dei segreti AWS utente.

Usa il segreto

Ti consigliamo di Gestione dei segreti AWS utilizzarlo per archiviare le credenziali o le chiavi per connetterti a destinazioni di streaming come Amazon Redshift, HTTP endpoint, Snowflake, Splunk, Coralogix, Datadog, Dynatrace, Elastic, Honeycomb, Logz.io, MongoDB Cloud e New Relic LogicMonitor

È possibile configurare l'autenticazione con Secrets Manager per queste destinazioni tramite la console di AWS gestione al momento della creazione dello stream Firehose. Per ulteriori informazioni, consulta [Configurare le impostazioni di destinazione](#). In alternativa, puoi anche utilizzare le operazioni [CreateDeliveryStream](#) [UpdateDestination](#) API per configurare l'autenticazione con Secrets Manager.

Firehose memorizza nella cache i segreti con una crittografia e li utilizza per ogni connessione alle destinazioni. Aggiorna la cache ogni 10 minuti per garantire che vengano utilizzate le credenziali più recenti.

Puoi scegliere di disattivare la funzionalità di recupero dei segreti da Secrets Manager in qualsiasi momento durante il ciclo di vita dello stream. Se non desideri utilizzare Secrets Manager per recuperare i segreti, puoi invece utilizzare la chiave username/password o API.

Note

Sebbene questa funzionalità di Firehose non preveda costi aggiuntivi, l'accesso e la manutenzione di Secrets Manager sono a pagamento. Per ulteriori informazioni, consulta la pagina dei prezzi [Gestione dei segreti AWS](#).

Concedi l'accesso a Firehose per recuperare il segreto

Affinché Firehose possa recuperare un segreto Gestione dei segreti AWS, è necessario fornire a Firehose le autorizzazioni necessarie per accedere al segreto e la chiave che crittografa il segreto.

Quando si utilizza Gestione dei segreti AWS per archiviare e recuperare i segreti, sono disponibili diverse opzioni di configurazione a seconda di dove è archiviato il segreto e di come è crittografato.

- Se il segreto è archiviato nello stesso AWS account del ruolo IAM ed è crittografato con la chiave AWS gestita predefinita (`aws/secretsmanager`), il ruolo IAM assunto da Firehose necessita solo `secretsmanager:GetSecretValue` dell'autorizzazione sul segreto.

```
// secret role policy
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "Secret ARN"
    }
  ]
}
```

Per ulteriori informazioni sulle politiche IAM, consulta Esempi di [policy di autorizzazione](#) per Gestione dei segreti AWS

- Se il segreto è archiviato nello stesso account del ruolo ma crittografato con una [chiave gestita dal cliente](#) (CMK), il ruolo richiede entrambe `secretsmanager:GetSecretValue` e `kms:Decrypt` autorizzazioni. La policy CMK deve inoltre consentire al ruolo IAM di funzionare. `kms:Decrypt`

- Se il segreto è archiviato in un AWS account diverso dal tuo ruolo ed è crittografato con la chiave AWS gestita predefinita, questa configurazione non è possibile in quanto Secrets Manager non consente l'accesso tra account quando il segreto è crittografato con una chiave AWS gestita.
- Se il segreto è archiviato in un account diverso e crittografato con una CMK, il ruolo IAM richiede l'`secretsmanager:GetSecretValue` autorizzazione sul segreto e l'`kms:Decrypt` autorizzazione sulla CMK. La politica delle risorse del segreto e la politica CMK dell'altro account devono inoltre consentire al ruolo IAM le autorizzazioni necessarie. Per ulteriori informazioni, consulta [Accesso tra account](#).

Ruota il segreto

La rotazione avviene quando aggiorni periodicamente un segreto. Puoi Gestione dei segreti AWS configurare la rotazione automatica del segreto secondo una pianificazione da te specificata. In questo modo, puoi sostituire i segreti a lungo termine con segreti a breve termine. Questo aiuta a ridurre il rischio di compromessi. Per ulteriori informazioni, consulta [Rotare Gestione dei segreti AWS secrets](#) nella Guida per l'Gestione dei segreti AWS utente.

Gestisci i ruoli IAM tramite la console Amazon Data Firehose

Amazon Data Firehose è un servizio completamente gestito che fornisce dati di streaming in tempo reale verso le destinazioni. È inoltre possibile configurare Firehose per trasformare e convertire il formato dei dati prima della consegna. Per utilizzare queste funzionalità, devi prima fornire ruoli IAM per concedere le autorizzazioni a Firehose quando crei o modifichi uno stream Firehose. Firehose utilizza questo ruolo IAM per tutte le autorizzazioni necessarie allo stream Firehose.

Ad esempio, si consideri uno scenario in cui si crea uno stream Firehose che fornisce dati ad Amazon S3 e questo flusso Firehose ha record di origine Transform con funzionalità abilitata. AWS Lambda in questo caso, è necessario fornire ruoli IAM per concedere a Firehose le autorizzazioni per accedere al bucket S3 e richiamare la funzione Lambda, come illustrato di seguito.

JSON

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

```

    "Action": ["lambda:InvokeFunction", "lambda:GetFunctionConfiguration"],
    "Resource": "arn:aws:lambda:us-east-1:123456789012:function:<lambda
function name>:<lambda function version>"
  }, {
    "Sid": "s3Permissions",
    "Effect": "Allow",
    "Action": ["s3:AbortMultipartUpload", "s3:GetBucketLocation",
"s3:GetObject", "s3:ListBucket", "s3:ListBucketMultipartUploads",
"s3:PutObject"],
    "Resource": ["arn:aws:s3:::<bucket name>", "arn:aws:s3:::<bucket name>/
*"]
  }
}

```

La console Firehose ti consente di scegliere come assegnare questi ruoli. Puoi scegliere tra una delle seguenti opzioni.

- [Scegli un ruolo IAM esistente](#)
- [Crea un nuovo ruolo IAM dalla console](#)

Scegli un ruolo IAM esistente

Puoi scegliere tra un ruolo IAM esistente. Con questa opzione, assicurati che il ruolo IAM che scegli abbia una policy di fiducia adeguata e le autorizzazioni necessarie per l'origine e la destinazione. Per ulteriori informazioni, consulta [Controllo dell'accesso con Amazon Data Firehose](#).

Crea un nuovo ruolo IAM dalla console

In alternativa, puoi anche utilizzare la console Firehose per creare un nuovo ruolo per tuo conto.

Quando Firehose crea un ruolo IAM per conto dell'utente, il ruolo include automaticamente tutte le policy di autorizzazione e fiducia che concedono le autorizzazioni richieste in base alla configurazione del flusso Firehose.

Ad esempio, se non hai abilitato la AWS Lambda funzionalità Transform source records with, la console genera la seguente dichiarazione nella politica di autorizzazione.

```

{
  "Sid": "lambdaProcessing",
  "Effect": "Allow",

```

```
"Action": [
  "lambda:InvokeFunction",
  "lambda:GetFunctionConfiguration"
],
"Resource": "arn:aws:lambda:us-east-1123456789012:function:
%FIREHOSE_POLICY_TEMPLATE_PLACEHOLDER%"
}
```

Note

È sicuro ignorare le dichiarazioni politiche che contengono in %FIREHOSE_POLICY_TEMPLATE_PLACEHOLDER% quanto non concedono autorizzazioni su alcuna risorsa.

La console di creazione e modifica dei flussi di lavoro Firehose stream crea inoltre una policy di fiducia e la collega al ruolo IAM. La policy di fiducia consente a Firehose di assumere il ruolo IAM. Di seguito è riportato un esempio di politica di fiducia.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "firehoseAssume",
    "Effect": "Allow",
    "Principal": {
      "Service": "firehose.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }]
}
```

Important

- È consigliabile evitare di utilizzare lo stesso ruolo IAM gestito dalla console per più flussi Firehose. In caso contrario, il ruolo IAM potrebbe diventare eccessivamente permissivo o causare errori.

- Per utilizzare dichiarazioni politiche diverse all'interno di una politica di autorizzazione da un ruolo IAM gestito dalla console, puoi creare il tuo ruolo IAM e copiare le istruzioni sulle policy in una policy di autorizzazione allegata al nuovo ruolo. Per collegare il ruolo allo stream Firehose, selezionare l'opzione Scegli il ruolo IAM esistente nell'accesso al servizio.
- La console gestisce qualsiasi ruolo IAM che contiene la stringa service-role nel relativo ARN. Quando scegli l'opzione del ruolo IAM esistente, assicurati di selezionare un ruolo IAM senza la stringa service-role nel relativo ARN in modo che la console non apporti alcuna modifica.

Passaggi per creare un ruolo IAM dalla console

1. Aprire la console Firehose all'indirizzo. <https://console.aws.amazon.com/firehose/>
2. Scegli Crea un flusso Firehose.
3. Scegli una fonte e una destinazione. Per ulteriori informazioni, consulta [Tutorial: Creare uno stream Firehose dalla console](#).
4. Scegli le impostazioni di destinazione. Per ulteriori informazioni, consulta [Configurare le impostazioni di destinazione](#).
5. In [Impostazioni avanzate](#), per l'accesso al servizio, scegli Crea o aggiorna il ruolo IAM.

Note

Questa è un'opzione predefinita. Per utilizzare un ruolo esistente, seleziona l'opzione Scegli il ruolo IAM esistente. La console Firehose non apporterà alcuna modifica al tuo ruolo.

6. Scegli Crea un flusso Firehose.

Modifica il ruolo IAM dalla console

Quando si modifica uno stream Firehose, Firehose aggiorna di conseguenza la politica di autorizzazione corrispondente per riflettere le modifiche alla configurazione e alle autorizzazioni.

Ad esempio, quando si modifica il flusso Firehose e si abilita la AWS Lambda funzionalità Transform source records with utilizzando la versione più recente della funzione Lambda

asexampleLambdaFunction, si ottiene la seguente dichiarazione di policy nella politica di autorizzazione.

```
{
  "Sid": "lambdaProcessing",
  "Effect": "Allow",
  "Action": [
    "lambda:InvokeFunction",
    "lambda:GetFunctionConfiguration"
  ],
  "Resource": "arn:aws:lambda:us-east-1:123456789012:function:exampleLambdaFunction:
$LATEST"
}
```

Important

Un ruolo IAM gestito da console è progettato per essere autonomo. Non è consigliabile modificare la politica di autorizzazione o la politica di attendibilità al di fuori della console.

Passaggi per modificare il ruolo IAM dalla console

1. Aprire la console Firehose all'indirizzo. <https://console.aws.amazon.com/firehose/>
2. Scegli Streams Firehose e scegli il nome di uno stream Firehose che desideri aggiornare.
3. Nella scheda Configurazione, nella sezione Accesso al server, scegli Modifica.
4. Aggiorna l'opzione del ruolo IAM.

Note

Per impostazione predefinita, la console aggiorna sempre un ruolo IAM con il pattern service-role nel relativo ARN. Quando scegli l'opzione del ruolo IAM esistente, assicurati di selezionare un ruolo IAM senza la stringa service-role nel relativo ARN in modo che la console non apporti alcuna modifica.

5. Scegli Save changes (Salva modifiche).

Comprendi la conformità per Amazon Data Firehose

I revisori di terze parti valutano la sicurezza e la conformità di Amazon Data Firehose nell'ambito di AWS diversi programmi di conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, consulta [AWS Services in Scope by Compliance Program](#). Per informazioni generali, consulta [Programmi di conformità di AWS](#).

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 quando utilizzate Data Firehose è determinata dalla sensibilità dei vostri dati, dagli obiettivi di conformità della vostra azienda e dalle leggi e dai regolamenti applicabili. Se l'utilizzo di Data Firehose è soggetto alla conformità a standard come HIPAA, PCI o FedRAMP, fornisce risorse per aiutare a: AWS

- Guide [introduttive su sicurezza e conformità: queste guide all'implementazione](#) illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e sulla conformità. AWS
- [Whitepaper sull'architettura per la sicurezza e la conformità HIPAA: questo white paper](#) descrive in che modo le aziende possono utilizzare per creare applicazioni conformi allo standard HIPAA. AWS
- [AWS Risorse per la conformità](#): questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- [AWS Config](#)— Questo AWS servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- [AWS Security Hub CSPM](#)— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente e consente AWS di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza in Amazon Data Firehose

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni 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, è possibile progettare e

gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

[Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS](#)

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

Ripristino di emergenza

Amazon Data Firehose funziona in modalità serverless e si occupa del deterioramento dell'host, della disponibilità delle zone di disponibilità e di altri problemi relativi all'infrastruttura eseguendo la migrazione automatica. Quando ciò accade, Amazon Data Firehose assicura che lo stream Firehose venga migrato senza alcuna perdita di dati.

Comprendi la sicurezza dell'infrastruttura in Amazon Data Firehose

In quanto servizio gestito, Amazon Data Firehose 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 chiamate API AWS pubblicate per accedere a Firehose attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Note

Per le richieste HTTPS in uscita, Amazon Data Firehose utilizza una libreria HTTP che seleziona automaticamente la versione del protocollo TLS più alta supportata sul lato di destinazione.

Utilizzo di Amazon Data Firehose con AWS PrivateLink

Puoi utilizzare un'interfaccia VPC endpoint (AWS PrivateLink) per accedere ad Amazon Data Firehose dal tuo VPC senza richiedere un Internet Gateway o un Gateway NAT. Gli endpoint VPC di interfaccia non richiedono un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione Direct Connect. Gli endpoint VPC di interfaccia sono basati su una AWS tecnologia che consente la comunicazione privata tra AWS i servizi utilizzando un'interfaccia di rete elastica con private nel IPs tuo Amazon VPC. AWS PrivateLink Per ulteriori informazioni, consulta [Amazon Virtual Private Cloud](#).

Utilizzo dell'interfaccia VPC endpoints (AWS PrivateLink per Firehose)

Per iniziare, crea un endpoint VPC di interfaccia in modo che il traffico Amazon Data Firehose proveniente dalle risorse Amazon VPC inizi a fluire attraverso l'endpoint VPC dell'interfaccia. Quando crei un endpoint, puoi allegare una policy per gli endpoint che controlli l'accesso ad Amazon Data Firehose. Per ulteriori informazioni sull'utilizzo delle policy per controllare l'accesso da un endpoint VPC ad Amazon Data Firehose, consulta [Controlling Access to Services](#) with VPC Endpoints.

L'esempio seguente mostra come configurare una AWS Lambda funzione in un VPC e creare un endpoint VPC per consentire alla funzione di comunicare in modo sicuro con il servizio Amazon Data Firehose. In questo esempio, si utilizza una policy che consente alla funzione Lambda di elencare i flussi Firehose nella regione corrente ma non di descrivere alcun flusso Firehose.

Creare un endpoint VPC

1. Accedi Console di gestione AWS e apri la console Amazon VPC all'indirizzo. <https://console.aws.amazon.com/vpc/>
2. Nel Pannello di controllo VPC scegliere Endpoint.
3. Scegliere Create Endpoint (Crea endpoint).
4. Nell'elenco dei nomi dei servizi scegliere `com.amazonaws.your_region.kinesis-firehose`.
5. Scegliere il VPC e una o più sottoreti in cui creare l'endpoint.
6. Scegliere uno o più gruppi di sicurezza da associare all'endpoint.
7. Per Policy, scegliere Personalizza e incollare la seguente policy:

```
{  
  "Statement": [  

```

```
{
  "Sid": "Allow-only-specific-PrivateAPIs",
  "Principal": "*",
  "Action": [
    "firehose:ListDeliveryStreams"
  ],
  "Effect": "Allow",
  "Resource": [
    "*"
  ]
},
{
  "Sid": "Allow-only-specific-PrivateAPIs",
  "Principal": "*",
  "Action": [
    "firehose:DescribeDeliveryStream"
  ],
  "Effect": "Deny",
  "Resource": [
    "*"
  ]
}
]
```

8. Seleziona Crea endpoint.

Creare un ruolo IAM da utilizzare con la funzione Lambda

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione sinistro scegli Ruoli, quindi Crea ruolo.
3. Per Seleziona il tipo di entità attendibile, lasci il valore predefinito Servizio AWS .
4. In Choose the service that will use this role (Scegli il servizio che utilizzerà questo ruolo), seleziona Lambda.
5. Seleziona Next: Permissions (Successivo: Autorizzazioni).
6. Nell'elenco delle policy, cercare e aggiungere le due policy denominate AWS LambdaVPCAccessExecutionRole e AmazonDataFirehoseReadOnlyAccess.

⚠ Important

Questo è un esempio. Potrebbero essere necessarie policy più rigorose per l'ambiente di produzione.

7. Scegli Successivo: Tag. Non è necessario aggiungere tag ai fini di questo esercizio. Scegli Prossimo: Rivedi.
8. Immetti un nome del ruolo, quindi scegli Crea ruolo.

Creare una funzione Lambda all'interno del VPC

1. Apri la AWS Lambda console all'indirizzo <https://console.aws.amazon.com/lambda/>.
2. Selezionare Create function (Crea funzione).
3. Scegli Author from scratch (Crea da zero).
4. Immettete un nome per la funzione, quindi impostate Runtime su Python 3.9 o superiore.
5. In Autorizzazioni, espandere Scegli o crea un ruolo di esecuzione.
6. Nell'elenco Ruolo di esecuzione scegliere Utilizza un ruolo esistente.
7. Nell'elenco Ruolo esistente scegliere il ruolo creato in precedenza.
8. Scegli Crea funzione.
9. In Codice della funzione, incollare il seguente codice.

```
import json
import boto3
import os
from botocore.exceptions import ClientError

def lambda_handler(event, context):
    REGION = os.environ['AWS_REGION']
    client = boto3.client(
        'firehose',
        REGION
    )
    print("Calling list_delivery_streams with ListDeliveryStreams allowed
policy.")
    delivery_stream_request = client.list_delivery_streams()
```

```
print("Successfully returned list_delivery_streams request %s." % (
    delivery_stream_request
))
describe_access_denied = False
try:
    print("Calling describe_delivery_stream with DescribeDeliveryStream
denied policy.")
    delivery_stream_info =
client.describe_delivery_stream(DeliveryStreamName='test-describe-denied')
except ClientError as e:
    error_code = e.response['Error']['Code']
    print ("Caught %s." % (error_code))
    if error_code == 'AccessDeniedException':
        describe_access_denied = True

if not describe_access_denied:
    raise
else:
    print("Access denied test succeeded.")
```

10. In Impostazioni di base, impostare il timeout su 1 minuto.
11. In Rete, scegliere il VPC in cui è stato creato l'endpoint in precedenza, quindi scegliere le sottoreti e il gruppo di sicurezza che è stato associato all'endpoint quando è stato creato.
12. Nella parte superiore della pagina, scegli Salva.
13. Scegli Test (Esegui test).
14. Immetti il nome di un evento e scegli Crea.
15. Scegliere Test di nuovo. In tal modo si avvia l'esecuzione della funzione. Quando viene visualizzato il risultato dell'esecuzione, espandere Dettagli e confrontare l'output del log con il codice della funzione. I risultati positivi mostrano un elenco degli stream Firehose nella regione, oltre al seguente output:

```
Calling describe_delivery_stream.
```

```
AccessDeniedException
```

```
Access denied test succeeded.
```

Supportato Regioni AWS

Gli endpoint VPC di interfaccia sono attualmente supportati nelle seguenti regioni.

- Stati Uniti orientali (Ohio)
- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti occidentali (California settentrionale)
- Stati Uniti occidentali (Oregon)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Seoul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Thailandia)
- Asia Pacifico (Tokyo)
- Asia Pacifico (Hong Kong)
- Canada (Centrale)
- Canada occidentale (Calgary)
- Cina (Pechino)
- Cina (Ningxia)
- Europa (Francoforte)
- Europa (Irlanda)
- Europa (Londra)
- Europa (Parigi)
- Messico (centrale)
- Sud America (San Paolo)
- AWS GovCloud (Stati Uniti orientali)
- AWS GovCloud (Stati Uniti occidentali)
- Europa (Spagna)
- Medio Oriente (Emirati Arabi Uniti)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Osaka)
- Israele (Tel Aviv)
- Asia Pacifico (Malesia)

Implementa le best practice di sicurezza per Amazon Data Firehose

Amazon Data Firehose offre una serie di funzionalità di sicurezza da prendere in considerazione durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

Implementazione dell'accesso con privilegi minimi

Quando concedi le autorizzazioni, sei tu a decidere chi deve ottenere quali autorizzazioni per quali risorse Amazon Data Firehose. È possibile abilitare operazioni specifiche che si desidera consentire su tali risorse. Pertanto è necessario concedere solo le autorizzazioni necessarie per eseguire un'attività. L'implementazione dell'accesso con privilegi minimi è fondamentale per ridurre i rischi di sicurezza e l'impatto risultante da errori o intenzioni dannose.

Uso di ruoli IAM

Le applicazioni Producer e Client devono disporre di credenziali valide per accedere ai flussi Firehose e lo stream Firehose deve disporre di credenziali valide per accedere alle destinazioni. Non è necessario archiviare AWS le credenziali direttamente in un'applicazione client o in un bucket Amazon S3. Si tratta di credenziali a lungo termine che non vengono automaticamente ruotate e potrebbero avere un impatto aziendale significativo se vengono compromesse.

Invece, è necessario utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni producer e client per accedere ai flussi Firehose. Quando utilizzi un ruolo, non devi necessariamente usare credenziali a lungo termine (ad esempio, nome utente e password o chiavi di accesso) per accedere ad altre risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente IAM:

- [Ruoli IAM](#)
- [Scenari comuni per ruoli: utenti, applicazioni e servizi](#)

Implementa la crittografia lato server nelle risorse dipendenti

I dati inattivi e i dati in transito possono essere crittografati in Amazon Data Firehose. Per ulteriori informazioni, consulta [Protezione dei dati in Amazon Data Firehose](#).

Utilizzato CloudTrail per monitorare le chiamate API

Amazon Data Firehose è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Amazon Data Firehose.

Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata ad Amazon Data Firehose, 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, consulta [the section called “Registra le chiamate API Firehose”](#).

Monitoraggio di Amazon Data Firehose

Puoi monitorare Amazon Data Firehose utilizzando le seguenti funzionalità:

Argomenti

- [Implementa le migliori pratiche con Alarms CloudWatch](#)
- [Monitora Amazon Data Firehose con parametri CloudWatch](#)
- [CloudWatch Metriche di accesso per Amazon Data Firehose](#)
- [Monitora Amazon Data Firehose utilizzando i log CloudWatch](#)
- [CloudWatch Log di accesso per Amazon Data Firehose](#)
- [Monitora lo stato di Kinesis Agent](#)
- [Registra le chiamate API Amazon Data Firehose con AWS CloudTrail](#)

Implementa le migliori pratiche con Alarms CloudWatch

Aggiungi CloudWatch allarmi per quando le seguenti metriche superano il limite di buffering (massimo 15 minuti).

- `DeliveryToS3.DataFreshness`
- `DeliveryToIceberg.DataFreshness`
- `DeliveryToSplunk.DataFreshness`
- `DeliveryToAmazonOpenSearchService.DataFreshness`
- `DeliveryToAmazonOpenSearchServerless.DataFreshness`
- `DeliveryToHttpEndpoint.DataFreshness`

Creare anche allarmi basati sulle seguenti espressioni matematiche dei parametri.

- `IncomingBytes (Sum per 5 Minutes) / 300` si avvicina a una percentuale di `BytesPerSecondLimit`.
- `IncomingRecords (Sum per 5 Minutes) / 300` si avvicina a una percentuale di `RecordsPerSecondLimit`.
- `IncomingPutRequests (Sum per 5 Minutes) / 300` si avvicina a una percentuale di `PutRequestsPerSecondLimit`.

Un altro parametro per il quale si consiglia un allarme è `ThrottledRecords`.

Per ulteriori informazioni sulla risoluzione dei problemi quando gli allarmi vanno in stato ALARM, consulta [Risoluzione degli errori](#).

Monitora Amazon Data Firehose con parametri CloudWatch

Important

Assicurati di abilitare gli allarmi su tutte le CloudWatch metriche che appartengono alla tua destinazione per identificare gli errori in modo tempestivo.

Amazon Data Firehose si integra con i CloudWatch parametri di Amazon per consentirti di raccogliere, visualizzare e analizzare i CloudWatch parametri per i tuoi flussi Firehose. Ad esempio, puoi monitorare le `IncomingRecords` metriche `IncomingBytes` and per tenere traccia dei dati importati in Amazon Data Firehose dai produttori di dati.

Amazon Data Firehose raccoglie e pubblica CloudWatch metriche ogni minuto. Tuttavia, se i picchi di dati in entrata si verificano solo per pochi secondi, potrebbero non essere completamente acquisiti o non essere visibili nei parametri di un minuto. Questo perché le CloudWatch metriche vengono aggregate da Amazon Data Firehose a intervalli di un minuto.

Le metriche raccolte per gli stream Firehose sono gratuite. Per informazioni sui parametri dell'agente Kinesis, consulta [Monitora lo stato di Kinesis Agent](#).

Argomenti

- [CloudWatch metriche per il partizionamento dinamico](#)
- [CloudWatch metriche per la distribuzione dei dati](#)
- [Metriche di ingestione dei dati](#)
- [Metriche a livello di API CloudWatch](#)
- [CloudWatch Metriche di trasformazione dei dati](#)
- [CloudWatch Registra le metriche di decompressione](#)
- [Metriche di conversione del formato CloudWatch](#)
- [Metriche di crittografia lato server \(SSE\) CloudWatch](#)
- [Dimensioni per Amazon Data Firehose](#)

- [Metriche di utilizzo di Amazon Data Firehose](#)

CloudWatch metriche per il partizionamento dinamico

Se il [partizionamento dinamico](#) è abilitato, lo spazio dei nomi AWS/Firehose include le seguenti metriche.

Metrica	Description
<code>ActivePartitionsLimit</code>	<p>Il numero massimo di partizioni attive che un flusso Firehose elabora prima di inviare dati al bucket di errori.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>PartitionCount</code>	<p>Il numero di partizioni che vengono elaborate, in altre parole, il numero di partizioni attive. Questo numero varia tra 1 e il limite del numero di partizioni di 500 (impostazione predefinita).</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>PartitionCountExceeded</code>	<p>Questo parametro indica se si sta superando il limite del numero di partizioni. Emette 1 o 0 a seconda che il limite venga violato o meno.</p>
<code>JQProcessing.Duration</code>	<p>Restituisce il tempo impiegato per eseguire l'espressione JQ nella funzione JQ Lambda.</p> <p>Unità: millisecondi</p>
<code>PerPartitionThroughput</code>	<p>Indica il throughput che viene elaborato per partizione. Questo parametro consente di monitorare la velocità di trasmissione effettiva per ciascuna partizione.</p> <p>Unità: StandardUnit BytesSecond</p>

Metrica	Description
<code>DeliveryToS3.ObjectCount</code>	<p>Indica il numero di oggetti che vengono distribuiti al bucket S3.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>

CloudWatch metriche per la distribuzione dei dati

Il namespace `AWS/Firehose` include i parametri a livello di servizio descritti di seguito.

Se riscontri lievi cali nella media di `BackupToS3.Success`, `DeliveryToS3.Success`, `DeliveryToSplunk.Success`, `DeliveryToAmazonOpenSearchService.Success` o `DeliveryToRedshift.Success`, ciò non indica che vi sia una perdita di dati. Amazon Data Firehose riprova gli errori di consegna e non procede finché i record non vengono consegnati correttamente alla destinazione configurata o al bucket S3 di backup.

Argomenti

- [OpenSearch Consegna al servizio](#)
- [Consegna a OpenSearch Serverless](#)
- [Distribuzione ad Amazon Redshift](#)
- [Distribuzione ad Amazon S3](#)
- [Consegna a Snowflake](#)
- [Consegna a Splunk](#)
- [Distribuzione agli endpoint HTTP](#)

OpenSearch Consegna al servizio

Metrica	Description
<code>DeliveryToAmazonOpenSearchService.Bytes</code>	<p>Il numero di byte indicizzati al OpenSearch Servizio nel periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p>

Metrica	Description
	Unità: byte
<code>DeliveryToAmazonOpenSearchService.DataFreshness</code>	<p>L'epoca (dall'ingresso in Amazon Data Firehose ad oggi) del record più vecchio in Amazon Data Firehose. Tutti i record più vecchi di questa età sono stati consegnati al OpenSearch Servizio.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: secondi</p>
<code>DeliveryToAmazonOpenSearchService.Records</code>	<p>Il numero di record indicizzati al OpenSearch Servizio nel periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>DeliveryToAmazonOpenSearchService.Success</code>	La somma dei record indicizzati correttamente.
<code>DeliveryToS3.Bytes</code>	<p>Il numero di byte distribuiti ad Amazon S3 durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro solo quando abiliti il backup per tutti i documenti.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>DeliveryToS3.DataFreshness</code>	<p>L'epoca (dall'ingresso in Amazon Data Firehose ad oggi) del record più vecchio in Amazon Data Firehose. Qualsiasi record più vecchio di questa età è stato consegnato al bucket S3. Amazon Data Firehose emette questo parametro solo quando abiliti il backup per tutti i documenti.</p> <p>Unità: secondi</p>

Metrica	Description
<code>DeliveryToS3.Records</code>	<p>Il numero di record distribuiti ad Amazon S3 durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro solo quando abiliti il backup per tutti i documenti.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>DeliveryToS3.Success</code>	<p>La somma dei comandi put di Amazon S3 riusciti. Amazon Data Firehose emette sempre questo parametro indipendentemente dal fatto che il backup sia abilitato solo per i documenti non riusciti o per tutti i documenti.</p>
<code>DeliveryToAmazonOpenSearchService.AuthFailure</code>	<p>Authentication/authorization error. Verify the OS/ESpolicy del cluster e autorizzazioni per i ruoli.</p> <p>0 indica che non c'è alcun problema. 1 indica un errore di autenticazione.</p>
<code>DeliveryToAmazonOpenSearchService.DeliveryRejected</code>	<p>Errore di distribuzione rifiutata. Verifica la politica del OS/ES cluster e le autorizzazioni dei ruoli.</p> <p>0 indica che non è presente alcun problema. 1 indica un errore di distribuzione.</p>

Consegna a OpenSearch Serverless

Metrica	Description
<code>DeliveryToAmazonOpenSearchServerless.Bytes</code>	<p>Il numero di byte indicizzati su OpenSearch Serverless nel periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>

Metrica	Description
DeliveryToAmazonOpenSearchServerless.DataFreshness	<p>L'epoca (dall'ingresso in Amazon Data Firehose ad oggi) del record più vecchio in Amazon Data Firehose. Tutti i record più vecchi di questa età sono stati consegnati a OpenSearch Serverless.</p> <p>Unità: secondi</p>
DeliveryToAmazonOpenSearchServerless.Records	<p>Il numero di record indicizzati su OpenSearch Serverless nel periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
DeliveryToAmazonOpenSearchServerless.Success	<p>La somma dei record indicizzati correttamente.</p>
DeliveryToS3.Bytes	<p>Il numero di byte distribuiti ad Amazon S3 durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro solo quando abiliti il backup per tutti i documenti.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
DeliveryToS3.DataFreshness	<p>L'epoca (dall'ingresso in Amazon Data Firehose ad oggi) del record più vecchio in Amazon Data Firehose. Qualsiasi record più vecchio di questa età è stato consegnato al bucket S3. Amazon Data Firehose emette questo parametro solo quando abiliti il backup per tutti i documenti.</p> <p>Unità: secondi</p>

Metrica	Description
<code>DeliveryToS3.Records</code>	<p>Il numero di record distribuiti ad Amazon S3 durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro solo quando abiliti il backup per tutti i documenti.</p> <p>Unità: numero</p>
<code>DeliveryToS3.Success</code>	<p>La somma dei comandi put di Amazon S3 riusciti. Amazon Data Firehose emette sempre questo parametro indipendentemente dal fatto che il backup sia abilitato solo per i documenti non riusciti o per tutti i documenti.</p>
<code>DeliveryToAmazonOpenSearchServerless.AuthFailure</code>	<p>Authentication/authorization error. Verify the OS/ESpolicy del cluster e autorizzazioni per i ruoli.</p> <p>0 indica che non c'è alcun problema. 1 indica un errore di autenticazione.</p>
<code>DeliveryToAmazonOpenSearchServerless.DeliveryRejected</code>	<p>Errore di distribuzione rifiutata. Verifica la politica del OS/ES cluster e le autorizzazioni dei ruoli.</p> <p>0 indica che non vi è alcun problema. 1 indica un errore di distribuzione.</p>

Distribuzione ad Amazon Redshift

Metrica	Description
<code>DeliveryToRedshift.Bytes</code>	<p>Il numero di byte copiati su Amazon Redshift durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>DeliveryToRedshift.Records</code>	<p>Il numero di record copiati su Amazon Redshift durante il periodo di tempo specificato.</p>

Metrica	Description
	<p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
DeliveryToRedshift .Success	La somma dei comandi Amazon Redshift COPY di successo.
DeliveryToS3.Bytes	<p>Il numero di byte distribuiti ad Amazon S3 durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
DeliveryToS3.DataFreshness	<p>L'epoca (dall'ingresso in Amazon Data Firehose ad oggi) del record più vecchio in Amazon Data Firehose. Qualsiasi record più vecchio di questa età viene inviato al bucket S3.</p> <p>Unità: secondi</p>
DeliveryToS3.Records	<p>Il numero di record distribuiti ad Amazon S3 durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
DeliveryToS3.Success	La somma dei comandi put di Amazon S3 riusciti.
DeliveryToRedshift .DataFreshness	L'epoca (dall'ingresso in Amazon Data Firehose ad oggi) del record più vecchio in Amazon Data Firehose. Tutti i record più vecchi di questa età vengono consegnati al cluster Amazon Redshift.

Metrica	Description
BackupToS3.Bytes	<p>Il numero di byte distribuiti ad Amazon S3 per il backup durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro quando è abilitato il backup su Amazon S3.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
BackupToS3.DataFreshness	<p>L'epoca (dall'ingresso in Amazon Data Firehose ad oggi) del record più vecchio in Amazon Data Firehose. Qualsiasi record più vecchio di questa età è stato distribuito al bucket Amazon S3 per il backup. Amazon Data Firehose emette questo parametro quando è abilitato il backup su Amazon S3.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
BackupToS3.Records	<p>Il numero di record distribuiti ad Amazon S3 per il backup durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro quando è abilitato il backup su Amazon S3.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
BackupToS3.Success	<p>La somma dei comandi put di Amazon S3 di successo per il backup. Amazon Data Firehose emette questo parametro quando è abilitato il backup su Amazon S3.</p>

Distribuzione ad Amazon S3

Le metriche nella tabella seguente si riferiscono alla consegna ad Amazon S3 quando è la destinazione principale dello stream Firehose.

Metrica	Description
<code>DeliveryToS3.Bytes</code>	<p>Il numero di byte distribuiti ad Amazon S3 durante il periodo di tempo specificato. Quando la trasformazione dei dati è abilitata, questa metrica riflette la dimensione dei byte preelaborati prima della trasformazione.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
<code>DeliveryToS3.DataFreshness</code>	<p>L'epoca (dall'ingresso in Amazon Data Firehose ad oggi) del record più vecchio in Amazon Data Firehose. Qualsiasi record più vecchio di questa età è stato consegnato al bucket S3.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
<code>DeliveryToS3.Records</code>	<p>Il numero di record distribuiti ad Amazon S3 durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>DeliveryToS3.Success</code>	<p>La somma dei comandi put di Amazon S3 riusciti.</p>
<code>BackupToS3.Bytes</code>	<p>Il numero di byte distribuiti ad Amazon S3 per il backup durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro quando il backup è abilitato (il che è possibile solo quando è abilitata anche la trasformazione dei dati).</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>

Metrica	Description
BackupToS3.DataFreshness	<p>Età (dall'ingresso in Amazon Data Firehose a oggi) del record più vecchio di Amazon Data Firehose. Qualsiasi record più vecchio di questa età è stato distribuito al bucket Amazon S3 per il backup. Amazon Data Firehose emette questo parametro quando il backup è abilitato (il che è possibile solo quando è abilitata anche la trasformazione dei dati).</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
BackupToS3.Records	<p>Il numero di record distribuiti ad Amazon S3 per il backup durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro quando il backup è abilitato (il che è possibile solo quando è abilitata anche la trasformazione dei dati).</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
BackupToS3.Success	<p>La somma dei comandi put di Amazon S3 di successo per il backup. Amazon Data Firehose emette questo parametro quando il backup è abilitato (il che è possibile solo quando è abilitata anche la trasformazione dei dati).</p>

Consegna a Snowflake

Metrica	Description
DeliveryToSnowflake.Bytes	<p>Il numero di byte consegnati a Snowflake nel periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p>

Metrica	Description
	Unità: byte
DeliveryToSnowflake.DataFreshness	<p>L'età (dall'ingresso in Firehose a oggi) del disco più antico di Firehose. Qualsiasi disco più vecchio di questa età è stato consegnato a Snowflake. Tieni presente che possono essere necessari alcuni secondi per salvare i dati su Snowflake dopo che la chiamata di inserimento di Firehose ha avuto esito positivo. Per il tempo necessario per salvare i dati su Snowflake, fate riferimento alla metrica <code>DeliveryToSnowflake.DataCommitLatency</code></p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
DeliveryToSnowflake.DataCommitLatency	<p>Il tempo necessario per il commit dei dati su Snowflake dopo che Firehose ha inserito correttamente i record.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
DeliveryToSnowflake.Records	<p>Il numero di record consegnati a Snowflake nel periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
DeliveryToSnowflake.Success	<p>La somma delle chiamate di inserimento riuscite effettuate a Snowflake.</p>

Metrica	Description
DeliveryToS3.Bytes	<p>Il numero di byte distribuiti ad Amazon S3 durante il periodo di tempo specificato. Questa metrica è disponibile solo quando la consegna a Snowflake fallisce e Firehose tenta di eseguire il backup dei dati non riusciti su S3.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
DeliveryToS3.Records	<p>Il numero di record distribuiti ad Amazon S3 durante il periodo di tempo specificato. Questa metrica è disponibile solo quando la consegna a Snowflake fallisce e Firehose tenta di eseguire il backup dei dati non riusciti su S3.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
DeliveryToS3.Success	<p>La somma dei comandi put di Amazon S3 riusciti. Questa metrica è disponibile solo quando la consegna a Snowflake fallisce e Firehose tenta di eseguire il backup dei dati non riusciti su S3.</p>
BackupToS3.DataFreshness	<p>L'età (da Firehose a oggi) del disco più antico di Firehose. Tutti i record più vecchi di questa età vengono sottoposti a backup nel bucket Amazon S3. Questa metrica è disponibile quando il flusso Firehose è configurato per il backup di tutti i dati.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>

Metrica	Description
BackupToS3.Records	<p>Il numero di record distribuiti ad Amazon S3 per il backup durante il periodo di tempo specificato. Questa metrica è disponibile quando il flusso Firehose è configurato per il backup di tutti i dati.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: conta</p>
BackupToS3.Bytes	<p>Il numero di byte distribuiti ad Amazon S3 per il backup durante il periodo di tempo specificato. Questa metrica è disponibile quando il flusso Firehose è configurato per il backup di tutti i dati.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: conta</p>
BackupToS3.Success	<p>La somma dei comandi put di Amazon S3 di successo per il backup. Firehose emette questa metrica quando il flusso Firehose è configurato per il backup di tutti i dati.</p>

Consegna a Splunk

Metrica	Description
DeliveryToSplunk.Bytes	<p>Il numero di byte consegnati a Splunk durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
DeliveryToSplunk.DataAckLatency	<p>La durata approssimativa necessaria per ricevere una conferma da Splunk dopo che Amazon Data Firehose gli ha inviato i dati. La tendenza in aumento o in diminuzione per questo parametro è più utile del valore approssimativo.</p>

Metrica	Description
	<p>ativo assoluto. Le tendenze in aumento possono indicare tassi di indicizzazione e riconoscimento da parte degli indicizzatori Splunk.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
<p><code>DeliveryToSplunk.DataFreshness</code></p>	<p>Età (dall'ingresso in Amazon Data Firehose a oggi) del record più vecchio di Amazon Data Firehose. Qualsiasi record più vecchio di questa età è stato consegnato a Splunk.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
<p><code>DeliveryToSplunk.Records</code></p>	<p>Il numero di record consegnati a Splunk durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<p><code>DeliveryToSplunk.Success</code></p>	<p>La somma dei record indicizzati correttamente.</p>
<p><code>DeliveryToS3.Success</code></p>	<p>La somma dei comandi put di Amazon S3 riusciti. Questo parametro viene emesso quando il backup su Amazon S3 è abilitato.</p>
<p><code>BackupToS3.Bytes</code></p>	<p>Il numero di byte distribuiti ad Amazon S3 per il backup durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro quando lo stream Firehose è configurato per il backup di tutti i documenti.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>

Metrica	Description
<code>BackupToS3.DataFreshness</code>	<p>Età (dall'ingresso in Amazon Data Firehose a oggi) del record più vecchio di Amazon Data Firehose. Qualsiasi record più vecchio di questa età è stato distribuito al bucket Amazon S3 per il backup. Amazon Data Firehose emette questo parametro quando lo stream Firehose è configurato per il backup di tutti i documenti.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
<code>BackupToS3.Records</code>	<p>Il numero di record distribuiti ad Amazon S3 per il backup durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro quando lo stream Firehose è configurato per il backup di tutti i documenti.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>BackupToS3.Success</code>	<p>Somma dei comandi put di Amazon S3 eseguiti con successo per il backup. Amazon Data Firehose emette questo parametro quando lo stream Firehose è configurato per il backup di tutti i documenti.</p>

Distribuzione agli endpoint HTTP

Metrica	Description
<code>DeliveryToHttpEndpoint.Bytes</code>	<p>Il numero di byte distribuiti correttamente all'endpoint HTTP.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>

Metrica	Description
<code>DeliveryToHttpEndpoint.Records</code>	<p>Il numero di record distribuiti correttamente all'endpoint HTTP. Questa metrica viene emessa solo per i tentativi di consegna riusciti e non viene emessa quando un tentativo di consegna fallisce.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>DeliveryToHttpEndpoint.DataFreshness</code>	<p>Età del record più vecchio in Amazon Data Firehose.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
<code>DeliveryToHttpEndpoint.Success</code>	<p>Il numero di record inviati correttamente all'endpoint HTTP per tentativo di consegna. Al contrario <code>DeliveryToHttpEndpoint.Records</code>, questa metrica viene emessa per ogni tentativo di consegna. In caso di successo, il valore è uguale al numero di record nel tentativo di consegna. In caso di fallimento di tutti i record del tentativo di consegna, il valore è 0. Utilizza la statistica a Minimum per monitorare gli errori di consegna.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>DeliveryToHttpEndpoint.ProcessedBytes</code>	<p>Il numero di byte che si è tentato di elaborare, inclusi i nuovi tentativi.</p>
<code>DeliveryToHttpEndpoint.ProcessedRecords</code>	<p>Il numero di record tentati, inclusi i nuovi tentativi.</p>

Metriche di ingestione dei dati

Argomenti

- [Inserimento di dati tramite Kinesis Data Streams](#)
- [Inserimento di dati tramite Direct PUT](#)
- [Inserimento di dati da MSK](#)

Inserimento di dati tramite Kinesis Data Streams

Metrica	Description
<code>DataReadFromKinesisStream.Bytes</code>	<p>Quando l'origine dati è un flusso di dati Kinesis, questo parametro indica il numero di byte letti dal flusso. Questo numero include le riletture dovute a failover.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
<code>DataReadFromKinesisStream.Records</code>	<p>Quando l'origine dati è un flusso di dati Kinesis, questo parametro indica il numero di record letti dal flusso di dati. Questo numero include le riletture dovute a failover.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>ThrottledDescribeStream</code>	<p>Il numero totale di volte in cui l'operazione <code>DescribeStream</code> viene limitata quando l'origine dati è un flusso di dati Kinesis.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>ThrottledGetRecords</code>	<p>Il numero totale di volte in cui l'operazione <code>GetRecords</code> viene limitata quando l'origine dati è un flusso di dati Kinesis.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>

Metrica	Description
<code>ThrottledGetShardIterator</code>	<p>Il numero totale di volte in cui l'operazione <code>GetShardIterator</code> viene limitata quando l'origine dati è un flusso di dati Kinesis.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>KinesisMillisBehindLatest</code>	<p>Quando l'origine dati è un flusso di dati Kinesis, questo parametro indica il numero di millisecondi di ritardo dell'ultimo record letto rispetto al record più recente nel flusso di dati Kinesis.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: millisecondi</p>

Inserimento di dati tramite Direct PUT

Metrica	Description
<code>BackupToS3.Bytes</code>	<p>Il numero di byte distribuiti ad Amazon S3 per il backup durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro quando la trasformazione dei dati è abilitata per le destinazioni Amazon S3 o Amazon Redshift.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
<code>BackupToS3.DataFreshness</code>	<p>Età (dall'ingresso in Amazon Data Firehose a oggi) del record più vecchio di Amazon Data Firehose. Qualsiasi record più vecchio di questa età è stato distribuito al bucket Amazon S3 per il backup. Amazon Data Firehose emette questo parametro quando la trasformazione dei</p>

Metrica	Description
	<p>dati è abilitata per le destinazioni Amazon S3 o Amazon Redshift.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
BackupToS3.Records	<p>Il numero di record distribuiti ad Amazon S3 per il backup durante il periodo di tempo specificato. Amazon Data Firehose emette questo parametro quando la trasformazione dei dati è abilitata per le destinazioni Amazon S3 o Amazon Redshift.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
BackupToS3.Success	<p>Somma dei comandi put di Amazon S3 eseguiti con successo per il backup. Amazon Data Firehose emette questo parametro quando la trasformazione dei dati è abilitata per le destinazioni Amazon S3 o Amazon Redshift.</p>
BytesPerSecondLimit	<p>Il numero massimo attuale di byte al secondo che uno stream Firehose può acquisire prima del throttling. Per richiedere un aumento fino a questo limite, vai al Centro di supporto AWS e scegli Crea caso, quindi scegli Aumento del limite dei servizi.</p>
DeliveryToAmazonOpenSearchService.Bytes	<p>Il numero di byte indicizzati al servizio nel periodo di tempo specificato. OpenSearch</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>

Metrica	Description
<code>DeliveryToAmazonOpenSearchService.DataFreshness</code>	<p>L'epoca (dall'ingresso in Amazon Data Firehose ad oggi) del record più vecchio in Amazon Data Firehose. Tutti i record più vecchi di questa età sono stati consegnati al OpenSearch Servizio.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
<code>DeliveryToAmazonOpenSearchService.Records</code>	<p>Il numero di record indicizzati al OpenSearch Servizio nel periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>DeliveryToAmazonOpenSearchService.Success</code>	<p>La somma dei record indicizzati correttamente.</p>
<code>DeliveryToRedshift.Bytes</code>	<p>Il numero di byte copiati su Amazon Redshift durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
<code>DeliveryToRedshift.Records</code>	<p>Il numero di record copiati su Amazon Redshift durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>DeliveryToRedshift.Success</code>	<p>La somma dei comandi Amazon Redshift COPY di successo.</p>

Metrica	Description
DeliveryToS3.Bytes	<p>Il numero di byte distribuiti ad Amazon S3 durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
DeliveryToS3.DataFreshness	<p>L'epoca (dall'ingresso in Amazon Data Firehose ad oggi) del record più vecchio in Amazon Data Firehose. Qualsiasi record più vecchio di questa età è stato consegnato al bucket S3.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
DeliveryToS3.Records	<p>Il numero di record distribuiti ad Amazon S3 durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
DeliveryToS3.Success	<p>La somma dei comandi put di Amazon S3 riusciti.</p>
DeliveryToSplunk.Bytes	<p>Il numero di byte consegnati a Splunk durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>

Metrica	Description
<code>DeliveryToSplunk.DataAckLatency</code>	<p>La durata approssimativa necessaria per ricevere una conferma da Splunk dopo che Amazon Data Firehose gli ha inviato i dati. La tendenza in aumento o in diminuzione per questo parametro è più utile del valore approssimativo assoluto. Le tendenze in aumento possono indicare tassi di indicizzazione e riconoscimento da parte degli indicizzatori Splunk.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
<code>DeliveryToSplunk.DataFreshness</code>	<p>Età (dall'ingresso in Amazon Data Firehose a oggi) del record più vecchio di Amazon Data Firehose. Qualsiasi record più vecchio di questa età è stato consegnato a Splunk.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: secondi</p>
<code>DeliveryToSplunk.Records</code>	<p>Il numero di record consegnati a Splunk durante il periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
<code>DeliveryToSplunk.Success</code>	<p>La somma dei record indicizzati correttamente.</p>

Metrica	Description
IncomingBytes	<p>Il numero di byte inseriti con successo nel flusso Firehose nel periodo di tempo specificato. L'ingestione dei dati potrebbe essere limitata quando supera uno dei limiti di flusso di Firehose. I dati limitati non verranno conteggiati per IncomingBytes .</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
IncomingPutRequests	<p>Il numero di richieste riuscite PutRecord e di PutRecord Batch richieste in un determinato periodo di tempo.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
IncomingRecords	<p>Il numero di record inseriti con successo nel flusso Firehose nel periodo di tempo specificato. L'ingestione dei dati potrebbe essere limitata quando supera uno dei limiti di flusso di Firehose. I dati limitati non verranno conteggiati per IncomingRecords .</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
RecordsPerSecondLimit	<p>L'attuale numero massimo di record al secondo che uno stream Firehose può acquisire prima della limitazione.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>

Metrica	Description
ThrottledRecords	<p>Il numero di record che sono stati limitati perché l'ingestione dei dati ha superato uno dei limiti di flusso di Firehose.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>

Inserimento di dati da MSK

Metrica	Description
DataReadFromSource .Records	<p>Il numero di record letti dall'argomento Kafka di origine.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
DataReadFromSource.Bytes	<p>Il numero di byte letti dall'argomento Kafka di origine.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
SourceThrottled.Delay	<p>Il ritardo con cui il cluster Kafka di origine restituisce i record dall'argomento Kafka di origine.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: millisecondi</p>
BytesPerSecondLimit	<p>Il limite attuale di velocità di trasmissione effettiva al quale Firehose leggerà da ogni partizione dell'argomento Kafka di origine.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte/secondo</p>

Metrica	Description
KafkaOffsetLag	<p>La differenza tra l'offset più grande del record che Firehose ha letto dall'argomento Kafka di origine e l'offset più grande del record disponibile dall'argomento Kafka di origine.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
FailedValidation.Records	<p>Il numero di record che non hanno superato la convalida del record.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
FailedValidation.Bytes	<p>Il numero di byte che non hanno superato la convalida del record.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
DataReadFromSource .Backpressured	<p>Indica che uno stream Firehose subisce un ritardo nella lettura dei record dalla partizione di origine o perché BytesPerSecondLimit per partizione è stato superato il limite del normale flusso di distribuzione o perché il normale flusso di distribuzione è lento o si è interrotto</p> <p>Unità: booleane</p>

Metriche a livello di API CloudWatch

Il namespace `AWS/Firehose` include i seguenti parametri a livello di API.

Metrica	Description
DescribeDeliveryStream.Latency	<p>Il tempo necessario per operazione DescribeDeliveryStream , misurato durante il periodo specificato.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: millisecondi</p>
DescribeDeliveryStream.Requests	<p>Il numero totale di richieste DescribeDeliveryStream .</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
ListDeliveryStreams.Latency	<p>Il tempo necessario per operazione ListDeliveryStreams , misurato durante il periodo specificato.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: millisecondi</p>
ListDeliveryStreams.Requests	<p>Il numero totale di richieste ListFirehose .</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
PutRecord.Bytes	<p>Il numero di byte immessi nello stream Firehose PutRecord utilizzato nel periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
PutRecord.Latency	<p>Il tempo necessario per operazione PutRecord , misurato durante il periodo specificato.</p> <p>Statistiche: minimo, massimo, media, esempi</p>

Metrica	Description
	Unità: millisecondi
PutRecord.Requests	<p>Il numero totale di richieste PutRecord , che equivale al numero totale di record da operazioni PutRecord .</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
PutRecordBatch.Bytes	<p>Il numero di byte immessi nello stream Firehose PutRecordBatch utilizzato nel periodo di tempo specificato.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: byte</p>
PutRecordBatch.Latency	<p>Il tempo necessario per operazione PutRecordBatch , misurato durante il periodo specificato.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: millisecondi</p>
PutRecordBatch.Records	<p>Il numero totale di record da operazioni PutRecordBatch .</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
PutRecordBatch.Requests	<p>Il numero totale di richieste PutRecordBatch .</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>

Metrica	Description
PutRequestsPerSecondLimit	<p>Il numero massimo di richieste put al secondo che uno stream Firehose può gestire prima del throttling. Questo numero include PutRecord e richiede. PutRecordBatch</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
ThrottledDescribeStream	<p>Il numero totale di volte in cui l'operazione DescribeStream viene limitata quando l'origine dati è un flusso di dati Kinesis.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
ThrottledGetRecords	<p>Il numero totale di volte in cui l'operazione GetRecords viene limitata quando l'origine dati è un flusso di dati Kinesis.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
ThrottledGetShardIterator	<p>Il numero totale di volte in cui l'operazione GetShardIterator viene limitata quando l'origine dati è un flusso di dati Kinesis.</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>
UpdateDeliveryStream.Latency	<p>Il tempo necessario per operazione UpdateDeliveryStream, misurato durante il periodo specificato.</p> <p>Statistiche: minimo, massimo, media, esempi</p> <p>Unità: millisecondi</p>

Metrica	Description
UpdateDeliveryStream.Requests	<p>Il numero totale di richieste UpdateDeliveryStream .</p> <p>Statistiche: minimo, massimo, media, somma, esempi</p> <p>Unità: numero</p>

CloudWatch Metriche di trasformazione dei dati

Se la trasformazione dei dati con Lambda è abilitata, lo spazio dei nomi AWS/Firehose include i seguenti parametri.

Metrica	Description
ExecuteProcessing.Duration	<p>Il tempo necessario per ogni chiamata della funzione Lambda eseguita da Firehose.</p> <p>Unità: millisecondi</p>
ExecuteProcessing.Success	<p>La somma delle invocazioni della funzione Lambda riuscite rispetto alla somma delle invocazioni totali della funzione Lambda.</p>
SucceedProcessing.Records	<p>Il numero di record elaborati correttamente durante il periodo di tempo specificato.</p> <p>Unità: numero</p>
SucceedProcessing.Bytes	<p>Il numero di byte elaborati correttamente durante il periodo di tempo specificato.</p> <p>Unità: byte</p>

CloudWatch Registra le metriche di decompressione

Se la decompressione è abilitata per la consegna CloudWatch dei registri, lo spazio dei nomi AWS/Firehose include le seguenti metriche.

Metrica	Description
OutputDecompressedBytes.Success	Dati decompressi in byte con successo Statistiche: minimo, massimo, media, somma, esempi Unità: byte
OutputDecompressedBytes.Failed	Dati decompressi in byte non riuscita Statistiche: minimo, massimo, media, somma, esempi Unità: byte
OutputDecompressedRecords.Success	Numero di record decompressi con successo Statistiche: minimo, massimo, media, somma, esempi Unità: numero
OutputDecompressedRecords.Failed	Numero di record decompressi non riusciti Statistiche: minimo, massimo, media, somma, esempi Unità: numero

Metriche di conversione del formato CloudWatch

Se la conversione del formato è abilitata, lo spazio dei nomi di AWS/Firehose include i seguenti parametri.

Metrica	Description
SucceedConversion.Records	Il numero di record convertiti correttamente. Unità: numero
SucceedConversion.Bytes	La dimensione dei record convertiti correttamente. Unità: byte

Metrica	Description
FailedConversion.Records	Il numero di record che non è stato possibile convertire. Unità: numero
FailedConversion.Bytes	La dimensione dei record che non è stato possibile convertire. Unità: byte

Metriche di crittografia lato server (SSE) CloudWatch

Lo spazio dei nomi `AWS/Firehose` include le seguenti metriche correlate a SSE.

Metrica	Description
KMSKeyAccessDenied	Il numero di volte in cui il servizio incontra uno stream <code>KMSAccessDeniedException</code> Firehose. Statistiche: minimo, massimo, media, somma, esempi Unità: numero
KMSKeyDisabled	Il numero di volte in cui il servizio incontra uno stream <code>KMSDisabledException</code> Firehose. Statistiche: minimo, massimo, media, somma, esempi Unità: numero
KMSKeyInvalidState	Il numero di volte in cui il servizio incontra uno stream <code>KMSInvalidStateException</code> Firehose. Statistiche: minimo, massimo, media, somma, esempi Unità: numero
KMSKeyNotFound	Il numero di volte in cui il servizio incontra uno stream <code>KMSNotFoundException</code> Firehose.

Metrica	Description
	Statistiche: minimo, massimo, media, somma, esempi
	Unità: numero

Dimensioni per Amazon Data Firehose

Per filtrare le metriche in base al flusso Firehose, utilizzate `DeliveryStreamName` la dimensione.

Metriche di utilizzo di Amazon Data Firehose

Puoi utilizzare i parametri di CloudWatch utilizzo per fornire visibilità sull'utilizzo delle risorse da parte del tuo account. Utilizza queste metriche per visualizzare l'utilizzo corrente del servizio su CloudWatch grafici e dashboard.

Le metriche sull'utilizzo della quota di servizio si trovano nello spazio dei nomi `AWS/Usage` e vengono raccolte ogni tre minuti.

Attualmente, l'unico nome di metrica in questo spazio dei nomi che viene pubblicato è `CloudWatchResourceCount`. Questo parametro viene pubblicato con le dimensioni `Service`, `Class`, `Type` e `Resource`.

Metrica	Descrizione
<code>ResourceCount</code>	<p>Il numero delle risorse specificate in esecuzione nell'account. Le risorse sono definite dalle dimensioni associate al parametro.</p> <p>La statistica più utile per questa metrica è <code>MAXIMUM</code>, che rappresenta il numero massimo di risorse utilizzate durante il periodo di 3 minuti.</p>

Le seguenti dimensioni vengono utilizzate per perfezionare le metriche di utilizzo pubblicate da Amazon Data Firehose.

Dimensione	Description
Service	Il nome del AWS servizio che contiene la risorsa. Per i parametri di utilizzo di Amazon Data Firehose, il valore per questa dimensione è <code>Firehose</code> .
Class	La classe della risorsa monitorata. I parametri di utilizzo dell'API Amazon Data Firehose utilizzano questa dimensione con un valore di <code>None</code> .
Type	Il tipo di risorsa monitorata. Attualmente, quando la dimensione <code>Service</code> è <code>Firehose</code> , l'unico valore valido per <code>Type</code> è <code>Resource</code> .
Resource	Il nome della risorsa. AWS Attualmente, quando la dimensione <code>Service</code> è <code>Firehose</code> , l'unico valore valido per <code>Resource</code> è <code>DeliveryStreams</code> .

CloudWatch Metriche di accesso per Amazon Data Firehose

Puoi monitorare i parametri per Amazon Data Firehose utilizzando CloudWatch la console, la riga di comando o l'API. CloudWatch Le procedure seguenti mostrano come accedere ai parametri utilizzando questi diversi metodi.

Per accedere alle metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nella barra di navigazione, scegliere una regione.
3. Nel riquadro di navigazione, seleziona Parametri.
4. Selezionare lo spazio dei nomi Firehose.
5. Scegliete Firehose stream Metrics o Firehose Metrics.
6. Selezionare un parametro da aggiungere al grafico.

Per accedere alle metriche utilizzando il AWS CLI

Usa le [metriche e i comandi dell'elenco](#). [get-metric-statistics](#)

```
aws cloudwatch list-metrics --namespace "AWS/Firehose"
```

```
aws cloudwatch get-metric-statistics --namespace "AWS/Firehose" \  
--metric-name DescribeDeliveryStream.Latency --statistics Average --period 3600 \  
--start-time 2017-06-01T00:00:00Z --end-time 2017-06-30T00:00:00Z
```

Monitora Amazon Data Firehose utilizzando i log CloudWatch

Amazon Data Firehose si integra con Amazon CloudWatch Logs in modo da poter visualizzare i log degli errori specifici quando la chiamata Lambda per la trasformazione o la consegna dei dati fallisce. Puoi abilitare la registrazione degli errori di Amazon Data Firehose quando crei lo stream Firehose.

Se abiliti la registrazione degli errori di Amazon Data Firehose nella console Amazon Data Firehose, per tuo conto vengono creati un gruppo di log e i flussi di log corrispondenti per il flusso Firehose. Il formato del nome del gruppo di log è `aws/kinesisfirehose/delivery-stream-name`, dove *delivery-stream-name* è il nome del flusso Firehose corrispondente. `DestinationDelivery` è il flusso di log creato e utilizzato per registrare eventuali errori relativi alla consegna alla destinazione principale. Un altro flusso di log chiamato `BackupDelivery` viene creato solo se il backup S3 è abilitato per la destinazione. Il flusso di log `BackupDelivery` viene utilizzato per registrare eventuali errori relativi alla distribuzione al backup S3.

Ad esempio, se crei uno stream Firehose "MyStream" con Amazon Redshift come destinazione e abiliti la registrazione degli errori di Amazon Data Firehose, vengono creati per tuo conto: un gruppo di log denominato `aws/kinesisfirehose/MyStream` e due flussi di log denominati `DestinationDelivery` e `BackupDelivery`. In questo esempio, `DestinationDelivery` verrà utilizzato per registrare eventuali errori relativi alla distribuzione alla destinazione Amazon Redshift e anche alla destinazione S3 intermedia. `BackupDelivery`, nel caso in cui il backup S3 sia abilitato, verrà utilizzato per registrare eventuali errori relativi alla distribuzione al bucket di backup S3.

Puoi abilitare la registrazione degli errori di Amazon Data Firehose tramite AWS CLI, l'API o CloudFormation utilizzando la configurazione `CloudWatchLoggingOptions`. A tale scopo, creare un gruppo di log e un flusso di log in anticipo. Consigliamo di riservare il gruppo e il flusso di log esclusivamente per la registrazione degli errori di Amazon Data Firehose. Verifica anche che la policy IAM associata disponga dell'autorizzazione `"logs:putLogEvents"`. Per ulteriori informazioni, consulta [Controllo dell'accesso con Amazon Data Firehose](#).

Tieni presente che Amazon Data Firehose non garantisce che tutti i log degli errori di consegna vengano inviati a Logs. CloudWatch In circostanze in cui il tasso di errori di consegna è elevato, Amazon Data Firehose campiona i log degli errori di consegna prima di inviarli a Logs. CloudWatch

È previsto un costo nominale per i log di errore inviati a Logs. CloudWatch Per ulteriori informazioni, consulta la pagina [CloudWatch dei prezzi di Amazon](#).

Indice

- [Errori di consegna dei dati](#)

Errori di consegna dei dati

Di seguito è riportato un elenco di codici e messaggi di errore di consegna dei dati per ogni destinazione Amazon Data Firehose. Ogni messaggio di errore, inoltre, descrive la modalità di intervento opportuna per risolvere il problema.

Errori

- [Errori di consegna dei dati di Amazon S3](#)
- [Errori di consegna dei dati di Apache Iceberg Tables](#)
- [Errori di consegna dei dati di Amazon Redshift](#)
- [Errori di consegna dei dati Snowflake](#)
- [Errori di consegna dei dati Splunk](#)
- [ElasticSearch Errori di consegna dei dati](#)
- [Errori di consegna dei dati degli endpoint HTTPS](#)
- [Errori di consegna dei dati di Amazon OpenSearch Service](#)
- [Errori di invocazione Lambda](#)
- [Errori di invocazione Kinesis](#)
- [Errori di invocazione Kinesis DirectPut](#)
- [AWS Glue errori di invocazione](#)
- [DataFormatConversion errori di invocazione](#)

Errori di consegna dei dati di Amazon S3

Amazon Data Firehose può inviare i seguenti errori relativi ad Amazon S3 ai log. CloudWatch

Codice di errore	Messaggio di errore e informazioni
<code>S3.KMS.NotFoundException</code>	«La AWS KMS chiave fornita non è stata trovata. Se stai usando quella che ritieni essere una AWS KMS chiave valida con il ruolo corretto, controlla se c'è un problema con l'account a cui è associata la AWS KMS chiave.»
<code>S3.KMS.RequestLimitExceeded</code>	"Il limite di richieste KMS al secondo è stato superato durante il tentativo di crittografare gli oggetti S3. Aumenta il limite di richieste al secondo". Per ulteriori informazioni, consulta la sezione Limiti nella Guida per sviluppatori di AWS Key Management Service .
<code>S3.AccessDenied</code>	"L'accesso è stato negato. Assicurati che la policy di fiducia per il ruolo IAM fornito consenta ad Amazon Data Firehose di assumere il ruolo e che la policy di accesso consenta l'accesso al bucket S3».
<code>S3.AccountProblem</code>	«C'è un problema con il tuo AWS account che impedisce il corretto completamento dell'operazione. Contatta il supporto AWS ".
<code>S3.AllAccessDisabled</code>	"L'accesso all'account fornito è stato disabilitato. Contatta l' AWS assistenza».
<code>S3.InvalidPayer</code>	"L'accesso all'account fornito è stato disabilitato. Contatta l' AWS assistenza».
<code>S3.NotSignedUp</code>	"L'account non è registrato per Amazon S3. Registra l'account o utilizzane uno diverso".
<code>S3.NoSuchBucket</code>	"Il bucket specificato non esiste. Crea il bucket o utilizzane un altro esistente".
<code>S3.MethodNotAllowed</code>	"Il metodo specificato non è consentito su questa risorsa. Modifica la policy del bucket per consentire le corrette autorizzazioni dell'operazione Amazon S3".
<code>InternalServerError</code>	"Si è verificato un errore interno durante il tentativo di distribuire i dati. La consegna verrà ritentata; se l'errore persiste, verrà segnalato AWS per la risoluzione.»

Codice di errore	Messaggio di errore e informazioni
S3.KMS.KeyDisabled	"La chiave KMS fornita è disabilitata. Abilita la chiave o usa una chiave diversa".
S3.KMS.InvalidStateException	"La chiave KMS fornita è in uno stato non valido. Utilizza una chiave diversa".
KMS.InvalidStateException	"La chiave KMS fornita è in uno stato non valido. Utilizza una chiave diversa".
KMS.DisabledException	"La chiave KMS fornita è disabilitata. Correggi la chiave o utilizza una chiave diversa".
S3.SlowDown	"La frequenza di richiesta put al bucket specificato era troppo alta. Aumentate le dimensioni del buffer di flusso Firehose o riducete le richieste di put da altre applicazioni».
S3.SubscriptionRequired	"L'accesso è stato negato durante la chiamata a S3. Assicurati che il ruolo IAM e la chiave KMS (se fornita) trasmessi abbiano un abbonamento Amazon S3".
S3.InvalidToken	"Il token fornito ha un formato errato o comunque non è valido. Controlla le credenziali fornite".
S3.KMS.KeyNotConfigured	"Chiave KMS non configurata. Configura il tuo KMSMaster KeyID o disabilita la crittografia per il tuo bucket S3».
S3.KMS.AsymmetricCMKNotSupported	«Amazon S3 supporta solo sistemi simmetrici. CMKs Non è possibile utilizzare una chiave CMK asimmetrica per crittografare i dati in Amazon S3. Per ottenere il tipo di CMK, utilizza l'operazione KMS.» DescribeKey
S3.IllegalLocationConstraintException	"Attualmente Firehose utilizza l'endpoint globale s3 per la distribuzione dei dati al bucket s3 configurato. La regione del bucket s3 configurato non supporta l'endpoint globale s3. Crea uno stream Firehose nella stessa regione del bucket s3 o usa il bucket s3 nella regione che supporta l'endpoint globale.»

Codice di errore	Messaggio di errore e informazioni
<code>S3.InvalidPrefixConfigurationException</code>	"Il prefisso s3 personalizzato utilizzato per la valutazione del timestamp non è valido. Verifica che il prefisso s3 contenga espressioni valide per la data e l'ora correnti dell'anno".
<code>DataFormatConversion.MalformedData</code>	"È stato trovato un carattere non valido tra i token".

Errori di consegna dei dati di Apache Iceberg Tables

Per gli errori di consegna dei dati di Apache Iceberg Tables, vedi. [Fornisci dati a Apache Iceberg Tables](#)

Errori di consegna dei dati di Amazon Redshift

Amazon Data Firehose può inviare i seguenti errori relativi ad Amazon Redshift ai log. CloudWatch

Codice di errore	Messaggio di errore e informazioni
<code>Redshift.TableNotFound</code>	<p>"La tabella su cui caricare i dati non è stata trovata. Verifica l'esistenza della tabella specificata".</p> <p>La tabella di destinazione in Amazon Redshift su cui i dati devono essere copiati da S3 non è stata trovata. Tieni presente che Amazon Data Firehose non crea la tabella Amazon Redshift se non esiste.</p>
<code>Redshift.SyntaxError</code>	"Il comando COPY contiene un errore di sintassi. Ripeti il comando".
<code>Redshift.AuthenticationFailed</code>	"Il nome utente e la password immessi non hanno superato l'autenticazione. Inserisci un nome utente e una password validi".

Codice di errore	Messaggio di errore e informazioni
Redshift. AccessDenied	"L'accesso è stato negato. Assicurati che la policy di fiducia per il ruolo IAM fornito consenta ad Amazon Data Firehose di assumere il ruolo.»
Redshift. S3BucketAccessDenied	"Il comando COPY non è stato in grado di accedere al bucket S3. Verifica che la policy di accesso per il ruolo IAM fornito consenta l'accesso al bucket S3".
Redshift. DataLoadFailed	"Caricamento dati nella tabella non riuscito. Controlla la tabella di sistema STL_LOAD_ERRORS per i dettagli".
Redshift. ColumnNotFound	"Una colonna nel comando COPY non esiste nella tabella. Specificar un nome di colonna valido".
Redshift. DatabaseNotFound	"Il database specificato nella configurazione della destinazione Amazon Redshift o nell'URL JDBC non è stato trovato. Specifica un nome del database valido".
Redshift. IncorrectCopyOptions	<p>"Sono state fornite opzioni COPY in conflitto o ridondanti. Alcune opzioni non sono compatibili in determinate combinazioni. Controlla le informazioni di riferimento per il comando COPY per ulteriori informazioni".</p> <p>Per ulteriori informazioni, consulta la sezione relativa al comando COPY di Amazon Redshift nella Guida per gli sviluppatori di Amazon Redshift.</p>
Redshift. MissingColumn	"C'è una colonna definita nello schema della tabella come NOT NULL senza un valore DEFAULT e non inclusa nell'elenco delle colonne. Escludi questa colonna, verifica che i dati caricati forniscano sempre un valore per questa colonna o aggiungi un valore predefinito allo schema di Amazon Redshift per questa tabella".
Redshift. ConnectionFailed	"La connessione al cluster Amazon Redshift specificato non è riuscita. Assicurati che le impostazioni di sicurezza consentano le connessioni Amazon Data Firehose, che il cluster o il database specificato nella configurazione di destinazione di Amazon Redshift o nell'URL JDBC sia corretto e che il cluster sia disponibile».

Codice di errore	Messaggio di errore e informazioni
Redshift. ColumnMismatch	"Il numero di jsonpath nel comando COPY e il numero di colonne nella tabella di destinazione devono corrispondere. Ripeti il comando".
Redshift. Incorrect OrMissing Region	"Amazon Redshift ha tentato di utilizzare l'endpoint di regione sbagliato per accedere al bucket S3. Specifica un valore di regione corretto nelle opzioni del comando COPY o verifica che il bucket S3 si trovi nella stessa regione del database Amazon Redshift".
Redshift. Incorrect JsonPathsFile	"Il file jsonpaths fornito non è in un formato JSON supportato. Ripeti il comando".
Redshift. MissingS3File	"Uno o più file S3 richiesti da Amazon Redshift sono stati rimossi dal bucket S3. Controlla le policy del bucket S3 per rimuovere l'eliminazione automatica di file S3".
Redshift. Insuffici entPrivilege	"L'utente non dispone delle autorizzazione per caricare dati nella tabella. Controlla le autorizzazione dell'utente Amazon Redshift per il privilegio INSERT".
Redshift. ReadOnlyC luster	"La query non può essere eseguita perché il sistema è in modalità di ridimensionamento. Riprova la query in un secondo momento".
Redshift. DiskFull	"Non è stato possibile caricare i dati perché il disco è pieno. Aumenta la capacità del cluster Amazon Redshift o elimina i dati inutilizzati per liberare spazio su disco".
InternalError	"Si è verificato un errore interno durante il tentativo di distribuire i dati. La consegna verrà ritentata; se l'errore persiste, verrà segnalato a noi per la risoluzione.» AWS
Redshift. ArgumentN otSupported	"Il comando COPY contiene opzioni non supportate".

Codice di errore	Messaggio di errore e informazioni
Redshift. AnalyzeTableAccess Denied	"Accesso negato. La copia da S3 a Redshift non riesce perché l'analisi della tabella può essere eseguita solo dal proprietario della tabella o del database".
Redshift. SchemaNotFound	«Lo schema specificato nella configurazione DataTableName di destinazione di Amazon Redshift non è stato trovato. Specificare un nome di schema valido».
Redshift. ColumnSpecifiedMoreThanOnce	"Esiste una colonna specificata più volte nell'elenco di colonne. Assicurati che le colonne duplicate vengano rimosse".
Redshift. ColumnNotNullWithoutDefault	"Esiste una colonna non nulla senza valore DEFAULT che non è inclusa nell'elenco di colonne. Assicurati che tali colonne siano incluse nell'elenco di colonne".
Redshift. IncorrectBucketRegion	"Redshift ha tentato di utilizzare un bucket in una regione diversa dal cluster. Specifica un bucket all'interno della stessa regione del cluster".
Redshift. S3SlowDown	"Alta frequenza di richieste per S3. Riduci la frequenza per evitare limitazioni".
Redshift. InvalidCopyOptionForJson	"Utilizza auto o un percorso S3 valido per json copyOption".
Redshift. InvalidCopyOptionJSONPathFormat	«COPIA non riuscita con errore\" Formato non valido JSONPath . L'indice dell'array non è compreso nell'intervallo\". Correggi l' JSONPath espressione.»

Codice di errore	Messaggio di errore e informazioni
Redshift. InvalidCopyOptionRBACNotAllowed	"Comando COPY non riuscito con errore \"Impossibile utilizzare il framework RBAC a cl se la propagazione delle autorizzazioni non è abilitata.\""
Redshift. DiskSpaceQuotaExceeded	"Transazione interrotta a causa del superamento della quota di spazio su disco. Libera spazio su disco o richiedi una quota maggiore per gli schemi".
Redshift. ConnectionsLimitExceeded	"Limite di connessione superato per l'utente".
Redshift. SSLNotSupported	"La connessione al cluster Amazon Redshift specificato non è riuscita perché il server non supporta SSL. Controlla le impostazioni del cluster".
Redshift. HoseNotFound	"L'hose è stato eliminato. Controlla lo stato dell'hose".
Redshift. Delimiter	"Il delimitatore CopyOptions in CopyCommand non è valido. Assicurati che si tratti di un singolo carattere".
Redshift. QueryCancelled	"L'utente ha annullato l'operazione COPY".
Redshift. CompressionMismatch	"L'hose è configurato con UNCOMPRESSED, ma CopyOption include un formato di compressione".
Redshift. EncryptionCredentials	"L'opzione ENCRYPTED richiede le credenziali nel formato: 'aws_iam_role=...;master_symmetric_key=...' or 'aws_access_key_id=...;aws_secret_access_key=...[;token=...];master_symmetric_key=...'"

Codice di errore	Messaggio di errore e informazioni
Redshift. InvalidCopyOptions	"Opzioni di configurazione COPY non valide".
Redshift. InvalidMessageFormat	"Il comando Copy contiene un carattere non valido".
Redshift. TransactionIdLimitReached	"È stato raggiunto il limite di ID transazione".
Redshift. DestinationRemoved	"Verifica che la destinazione redshift esista e sia configurata correttamente nella configurazione Firehose".
Redshift. OutOfMemory	"La memoria del cluster Redshift è quasi esaurita. Assicurati che il cluster abbia una capacità sufficiente".
Redshift. Cannot Fork Process	"La memoria del cluster Redshift è quasi esaurita. Assicurati che il cluster abbia una capacità sufficiente".
Redshift. SslFailure	"La connessione SSL è stata chiusa durante l'handshake".
Redshift.Resize	"Il cluster Redshift viene ridimensionato. Firehose non sarà in grado di distribuire dati durante il ridimensionamento del cluster".
Redshift. ImproperQualifiedName	"Il nome completo non è corretto (troppi nomi punteggiati)".
Redshift. InvalidJsonPathFormat	« JSONPath Formato non valido».

Codice di errore	Messaggio di errore e informazioni
Redshift. TooManyConnectionsException	"Troppe connessioni a Redshift".
Redshift. PSQLException	«PSQIEccezione osservata da Redshift».
Redshift. DuplicateSecondsSpecification	«Specificazione dei secondi duplicati nel date/time formato».
Redshift. RelationCouldNotBeOpened	"Errore Redshift rilevato, non è stato possibile aprire la relazione. Controlla i log di Redshift per il DB specificato".
Redshift. TooManyClients	"Troppe eccezioni per i client di Redshift. Riesamina il numero massimo di connessioni al database se ci sono più produttori che scrivono sul database contemporaneamente".

Errori di consegna dei dati Snowflake

Firehose può inviare i seguenti errori relativi a Snowflake ai registri. CloudWatch

Codice di errore	Messaggio di errore e informazioni
Snowflake .InvalidUrl	«Firehose non è in grado di connettersi a Snowflake. Assicurati che l'URL dell'account sia specificato correttamente nella configurazione di destinazione di Snowflake.»
Snowflake .InvalidUser	«Firehose non è in grado di connettersi a Snowflake. Assicurati che l'utente sia specificato correttamente nella configurazione di destinazione di Snowflake.»

Codice di errore	Messaggio di errore e informazioni
Snowflake .InvalidRole	«Il ruolo snowflake specificato non esiste o non è autorizzato. Assicurati che il ruolo sia concesso all'utente specificato»
Snowflake .InvalidTable	«La tabella fornita non esiste o non è autorizzata»
Snowflake .InvalidSchema	«Lo schema fornito non esiste o non è autorizzato»
Snowflake .InvalidDatabase	«Il database fornito non esiste o non è autorizzato»
Snowflake .InvalidPrivateKeyOrPassphrase	«La chiave privata o la passphrase specificata non è valida. Nota che la chiave privata fornita deve essere una chiave privata PEM RSA valida»
Snowflake .MissingColumns	«La richiesta di inserimento viene rifiutata a causa della mancanza di colonne nel payload di input. Assicurati che i valori siano specificati per tutte le colonne non annullabili»
Snowflake .ExtraColumns	«La richiesta di inserimento viene rifiutata a causa di colonne aggiuntive. Le colonne non presenti nella tabella non devono essere specificate»
Snowflake .InvalidInput	«Consegna non riuscita a causa di un formato di input non valido. Assicurati che il payload di input fornito sia nel formato JSON accettabile»
Snowflake .IncorrectValue	«Consegna non riuscita a causa di un tipo di dati errato nel payload di input. Assicurati che i valori JSON specificati nel payload di input aderiscano al tipo di dati dichiarato nella definizione della tabella Snowflake»

Errori di consegna dei dati Splunk

Amazon Data Firehose può inviare i seguenti errori relativi a SPLUNK ai log. CloudWatch

Codice di errore	Messaggio di errore e informazioni
<code>Splunk.ProxyWithoutStickySessions</code>	«Se disponi di un proxy (ELB o altro) tra Amazon Data Firehose e il nodo HEC, devi abilitare le sessioni permanenti per supportare HEC.» ACKs
<code>Splunk.DisabledToken</code>	"Il token HEC è disabilitato. Abilita il token per consentire la distribuzione di dati a Splunk".
<code>Splunk.InvalidToken</code>	"Il token HEC non è valido. Aggiorna Amazon Data Firehose con un token HEC valido.»
<code>Splunk.InvalidDataFormat</code>	"Il formato dei dati non è corretto. Per vedere come formattare correttamente i dati per gli endpoint HEC Raw o Event, consulta Dai di eventi Splunk ".
<code>Splunk.InvalidIndex</code>	"Il token o l'input HEC è configurato con un indice non valido. Controlla la configurazione dell'indice e riprova".
<code>Splunk.ServerError</code>	"La distribuzione dei dati a Splunk non è riuscita a causa di un errore del server dal nodo HEC. Amazon Data Firehose riproverà a inviare i dati se la durata del nuovo tentativo in Amazon Data Firehose è superiore a 0. Se tutti i nuovi tentativi falliscono, Amazon Data Firehose esegue il backup dei dati su Amazon S3.»
<code>Splunk.DisabledAck</code>	"Il riconoscimento dell'indicizzatore è disabilitato per il token HEC". Abilita il riconoscimento dell'indicizzatore e riprova. Per ulteriori informazioni, consulta Abilita riconoscimento dell'indicizzatore ".
<code>Splunk.AckTimeout</code>	"Non è stato ricevuto un riconoscimento da HEC prima della scadenza del timeout di riconoscimento HEC. Nonostante il timeout delle conferme, è possibile che i dati siano stati indicizzati correttamente in Splunk. Amazon Data Firehose esegue il backup dei dati di Amazon S3 per i quali il timeout di riconoscimento è scaduto.»

Codice di errore	Messaggio di errore e informazioni
<code>Splunk.MaxRetriesFailed</code>	"La distribuzione dei dati a Splunk o la ricezione del riconoscimento non sono riusciti. Controlla lo stato HEC e riprova".
<code>Splunk.ConnectionTimeout</code>	"La connessione a Splunk è scaduta. Potrebbe trattarsi di un errore temporaneo e la richiesta verrà riprovata. Amazon Data Firehose esegue il backup dei dati su Amazon S3 se tutti i tentativi falliscono.»
<code>Splunk.InvalidEndpoint</code>	"Impossibile connettersi all'endpoint HEC. Assicurati che l'URL dell'endpoint HEC sia valido e raggiungibile da Amazon Data Firehose».
<code>Splunk.ConnectionClosed</code>	"Impossibile inviare dati su Splunk a causa di un errore di connessione. Potrebbe trattarsi di un errore temporaneo. L'aumento della durata dei tentativi nella configurazione di Amazon Data Firehose potrebbe proteggere da tali errori transitori».
<code>Splunk.SSLUnverified</code>	"Impossibile connettersi all'endpoint HEC. L'host non corrisponde al certificato fornito dal peer. Verifica che il certificato e l'host siano validi".
<code>Splunk.SSLHandshake</code>	"Impossibile connettersi all'endpoint HEC. Verifica che il certificato e l'host siano validi".
<code>Splunk.URLNotFound</code>	"L'URL richiesto non è stato trovato sul server Splunk. Controlla il cluster Splunk e assicurati che sia configurato correttamente".
<code>Splunk.ServerError.ContentTooLarge</code>	"La distribuzione dei dati a Splunk non è riuscita a causa di un errore del server con uno StatusCode: 413, messaggio: la richiesta inviata dal client era troppo grande. Consulta i documenti di splunk per configurare max_content_length".
<code>Splunk.IndexerBusy</code>	"La distribuzione dei dati a Splunk non è riuscita a causa di un errore del server dal nodo HEC. Assicurati che l'endpoint HEC o l'Elastic Load Balancer siano raggiungibili e funzionino correttamente".
<code>Splunk.ConnectionRecycled</code>	"La connessione da Firehose a Splunk è stata riciclata. La distribuzione verrà riprovata".

Codice di errore	Messaggio di errore e informazioni
<code>Splunk.AcknowledgmentsDisabled</code>	"Impossibile ricevere conferme su POST. Assicurati che le conferme siano abilitate sull'endpoint HEC".
<code>Splunk.InvalidHecResponseCharacter</code>	"Sono stati trovati caratteri non validi nella risposta HEC, assicurati di controllare il servizio e la configurazione HEC".

ElasticSearch Errori di consegna dei dati

Amazon Data Firehose può inviare i seguenti ElasticSearch errori ai CloudWatch log.

Codice di errore	Messaggio di errore e informazioni
<code>ES.AccessDenied</code>	"L'accesso è stato negato. Assicurati che il ruolo IAM fornito associato a Firehose non venga eliminato".
<code>ES.ResourceNotFound</code>	«Il dominio AWS Elasticsearch specificato non esiste».

Errori di consegna dei dati degli endpoint HTTPS

Amazon Data Firehose può inviare i seguenti errori relativi agli endpoint HTTP ai log. CloudWatch
Se nessuno di questi errori corrisponde al problema riscontrato, l'errore predefinito è il seguente: "Si è verificato un errore interno durante il tentativo di distribuire dati. La consegna verrà ritentata; se l'errore persiste, verrà segnalato per la risoluzione.» AWS

Codice di errore	Messaggio di errore e informazioni
<code>HttpEndpoint.RequestTimeout</code>	La distribuzione è andata in timeout prima della ricezione di una risposta e verrà riprovata. Se l'errore persiste, contatta il team di assistenza di AWS Firehose.

Codice di errore	Messaggio di errore e informazioni
<code>HttpEndpoint.ResponseTooLarge</code>	"La risposta ricevuta dall'endpoint è troppo grande. Contatta il proprietario dell'endpoint per risolvere il problema".
<code>HttpEndpoint.InvalidResponseFromDestination</code>	"La risposta ricevuta dall'endpoint specificato non è valida. Contatta il proprietario dell'endpoint per risolvere il problema".
<code>HttpEndpoint.DestinationException</code>	"La seguente risposta è stata ricevuta dalla destinazione endpoint".
<code>HttpEndpoint.ConnectionFailed</code>	"Impossibile connettersi all'endpoint di destinazione. Contatta il proprietario dell'endpoint per risolvere il problema".
<code>HttpEndpoint.ConnectionReset</code>	"Impossibile mantenere la connessione con l'endpoint. Contatta il proprietario dell'endpoint per risolvere il problema".
<code>HttpEndpoint.ConnectionReset</code>	"Problemi nel mantenimento della connessione con l'endpoint. Contatta il proprietario dell'endpoint".
<code>HttpEndpoint.ResponseReasonPhraseExceededLimit</code>	"La frase del motivo della risposta ricevuta dall'endpoint supera il limite configurato di 64 caratteri".

Codice di errore	Messaggio di errore e informazioni
<code>HttpEndpoint.InvalidResponseFromDestination</code>	"La risposta ricevuta dall'endpoint non è valida. Per ulteriori informazioni, vedi Risoluzione dei problemi relativi agli endpoint HTTP nella documentazione di Firehose. Motivo: "
<code>HttpEndpoint.DestinationException</code>	"La distribuzione all'endpoint non è riuscita. Per ulteriori informazioni, vedi Risoluzione dei problemi relativi agli endpoint HTTP nella documentazione di Firehose. Risposta ricevuta con codice di stato"
<code>HttpEndpoint.InvalidStatusCode</code>	"Ricevuto un codice di stato della risposta non valido".
<code>HttpEndpoint.SSLHandshakeFailure</code>	"Impossibile completare un handshake SSL con l'endpoint. Contatta il proprietario dell'endpoint per risolvere il problema".
<code>HttpEndpoint.SSLHandshakeFailure</code>	"Impossibile completare un handshake SSL con l'endpoint. Contatta il proprietario dell'endpoint per risolvere il problema".
<code>HttpEndpoint.SSLFailure</code>	"Impossibile completare un handshake TLS con l'endpoint. Contatta il proprietario dell'endpoint per risolvere il problema".
<code>HttpEndpoint.SSLHandshakeCertificatePathFailure</code>	"Impossibile completare un handshake SSL con l'endpoint a causa di un percorso di certificazione non valido. Contatta il proprietario dell'endpoint per risolvere il problema".

Codice di errore	Messaggio di errore e informazioni
<code>HttpEndpoint.SSLHandshakeCertificatePathValidationFailure</code>	"Impossibile completare un handshake SSL con l'endpoint a causa di un errore di convalida del percorso di certificazione. Contatta il proprietario dell'endpoint per risolvere il problema".
<code>HttpEndpoint.MakeRequestFailure.IllegalUriException</code>	«HttpEndpoint richiesta non riuscita a causa di un inserimento non valido nell'URI. Assicurati che tutti i caratteri nell'URI di input siano validi".
<code>HttpEndpoint.MakeRequestFailure.IllegalCharacterInHeaderValue</code>	«HttpEndpoint richiesta non riuscita a causa di un errore di risposta illegale. Carattere non valido '\n' nel valore d'intestazione".
<code>HttpEndpoint.IllegalResponseFailure</code>	«HttpEndpoint richiesta non riuscita a causa di un errore di risposta illegale. Il messaggio HTTP non deve contenere più di un header Content-Type".
<code>HttpEndpoint.IllegalMessageStart</code>	«HttpEndpoint richiesta non riuscita a causa di un errore di risposta illegale. Avvio non valido del messaggio HTTP. Per ulteriori informazioni, consulta Risoluzione dei problemi relativi agli endpoint HTTP nella documentazione di Firehose".

Errori di consegna dei dati di Amazon OpenSearch Service

Per la destinazione del OpenSearch Servizio, Amazon Data Firehose invia gli errori ai CloudWatch log non appena vengono restituiti dal Servizio. OpenSearch

Oltre agli errori che possono ripresentarsi dai OpenSearch cluster, è possibile che si verifichino i due errori seguenti:

- Authentication/authorization error occurs during attempt to deliver data to destination OpenSearch Service cluster. This can happen due to any permission issues and/orin modo intermittente quando la configurazione del dominio del OpenSearch servizio di destinazione Amazon Data Firehose viene modificata. Controlla la policy del cluster e le autorizzazioni dei ruoli.
- I dati non possono essere consegnati al cluster di OpenSearch servizio di destinazione a causa di errori. authentication/authorization Ciò può accadere a causa di problemi di autorizzazione in modo and/or intermittente quando la configurazione del dominio del OpenSearch servizio di destinazione Amazon Data Firehose viene modificata. Controlla la policy del cluster e le autorizzazioni dei ruoli.

Codice di errore	Messaggio di errore e informazioni
OS.AccessDenied	"L'accesso è stato negato. Assicurati che la policy di fiducia per il ruolo IAM fornito consenta a Firehose di assumere il ruolo e che la policy di accesso consenta l'accesso all'API Amazon OpenSearch Service».
OS.AccessDenied	"L'accesso è stato negato. Assicurati che la policy di fiducia per il ruolo IAM fornito consenta a Firehose di assumere il ruolo e che la policy di accesso consenta l'accesso all'API Amazon OpenSearch Service».
OS.AccessDenied	"L'accesso è stato negato. Assicurati che il ruolo IAM fornito associato a Firehose non venga eliminato".
OS.AccessDenied	"L'accesso è stato negato. Assicurati che il ruolo IAM fornito associato a Firehose non venga eliminato".
OS.ResourceNotFound	«Il dominio Amazon OpenSearch Service specificato non esiste».
OS.ResourceNotFound	«Il dominio Amazon OpenSearch Service specificato non esiste».

Codice di errore	Messaggio di errore e informazioni
OS.AccessDenied	"L'accesso è stato negato. Assicurati che la policy di fiducia per il ruolo IAM fornito consenta a Firehose di assumere il ruolo e che la policy di accesso consenta l'accesso all'API Amazon OpenSearch Service».
OS.RequestTimeout	«La richiesta al cluster Amazon OpenSearch Service o alla raccolta OpenSearch Serverless è scaduta. Assicurati che il cluster o la raccolta abbiano una capacità sufficiente per il carico di lavoro corrente".
OS.ClusterError	«Il cluster Amazon OpenSearch Service ha restituito un errore non specificato».
OS.RequestTimeout	«La richiesta al cluster Amazon OpenSearch Service è scaduta. Assicurati che il cluster abbia una capacità sufficiente per il carico di lavoro corrente".
OS.ConnectionFailed	«Problemi di connessione al cluster Amazon OpenSearch Service o alla raccolta OpenSearch Serverless. Assicurati che il cluster o la raccolta siano integri e raggiungibili".
OS.ConnectionReset	«Impossibile mantenere la connessione con il cluster Amazon OpenSearch Service o la raccolta OpenSearch Serverless. Contatta il proprietario del cluster o della raccolta per risolvere il problema".
OS.ConnectionReset	«Problemi nel mantenere la connessione con il cluster Amazon OpenSearch Service o la raccolta OpenSearch Serverless. Assicurati che il cluster o la raccolta siano integri e abbiano una capacità sufficiente per il carico di lavoro corrente".
OS.ConnectionReset	«Problemi nel mantenere la connessione con il cluster Amazon OpenSearch Service o la raccolta OpenSearch Serverless. Assicurati che il cluster o la raccolta siano integri e abbiano una capacità sufficiente per il carico di lavoro corrente".
OS.AccessDenied	"L'accesso è stato negato. Assicurati che la politica di accesso sul cluster Amazon OpenSearch Service conceda l'accesso al ruolo IAM configurato.»

Codice di errore	Messaggio di errore e informazioni
<code>OS.ValidationException</code>	«Il OpenSearch cluster ha restituito un <code>ESServiceException</code> . Uno dei motivi è che il cluster è stato aggiornato a OS 2.x o versione successiva, ma il <code>Type</code> parametro è ancora configurato sul tubo. Aggiorna la configurazione dell'hose impostandola <code>Type</code> su una stringa vuota o modifica l'endpoint con il cluster, che supporta il parametro <code>Type</code> .»
<code>OS.ValidationException</code>	"Il membro deve soddisfare lo schema di espressione regolare: <code>[a-z][a-z0-9\-\-]+</code> "
<code>OS.JsonParseException</code>	«Il cluster Amazon OpenSearch Service ha restituito un <code>JsonParseException</code> . Assicurati che i dati inseriti siano validi".
<code>OS.AmazonOpenSearchServiceParseException</code>	«Il cluster Amazon OpenSearch Service ha restituito un <code>AmazonOpenSearchServiceParseException</code> . Assicurati che i dati inseriti siano validi".
<code>OS.ExplicitIndexBulkNotAllowed</code>	«Assicurati che <code>rest.action.multi.allow_explicit_index</code> sia impostato su <code>true</code> nel cluster Amazon Service». OpenSearch
<code>OS.ClusterError</code>	«Il cluster Amazon OpenSearch Service o la raccolta OpenSearch Serverless hanno restituito un errore non specificato».
<code>OS.ClusterBlockException</code>	«Il cluster ha restituito un <code>ClusterBlockException</code> Potrebbe essere sovraccarico".
<code>OS.InvalidARN</code>	«L'ARN del OpenSearch servizio Amazon fornito non è valido. Controlla la tua <code>DeliveryStream</code> configurazione».
<code>OS.MalformedData</code>	"Il formato di uno o più record non è corretto. Assicurati che ogni record sia un singolo oggetto JSON valido e che non contenga nuove righe".
<code>OS.InternalError</code>	"Si è verificato un errore interno durante il tentativo di distribuire i dati. La consegna verrà ritentata; se l'errore persiste, verrà segnalato AWS per la risoluzione.»

Codice di errore	Messaggio di errore e informazioni
<code>OS.AliasWithMultipleIndicesNotAllowed</code>	"L'alias ha più di un indice associato. Assicurati che all'alias sia associato un solo indice".
<code>OS.UnsupportedVersion</code>	«Amazon OpenSearch Service 6.0 non è attualmente supportato da Amazon Data Firehose. Contatta l' AWS assistenza per ulteriori informazioni».
<code>OS.CharacterConversionException</code>	"Uno o più record contenevano un carattere non valido".
<code>OS.InvalidDomainNameLength</code>	"La lunghezza del nome di dominio non rientra nei limiti validi del sistema operativo".
<code>OS.VPCDomainNotSupported</code>	«I domini Amazon OpenSearch Service all'interno non VPCs sono attualmente supportati».
<code>OS.ConnectionError</code>	«Il server http ha chiuso la connessione in modo imprevisto, verifica lo stato del cluster Amazon OpenSearch Service o della raccolta OpenSearch Serverless».
<code>OS.LargeFieldData</code>	«Il cluster Amazon OpenSearch Service ha interrotto la richiesta poiché conteneva dati di campo più grandi di quelli consentiti».
<code>OS.BadGateway</code>	«Il cluster Amazon OpenSearch Service o la raccolta OpenSearch Serverless hanno interrotto la richiesta con una risposta: 502 Bad Gateway».
<code>OS.ServiceException</code>	«Errore ricevuto dal cluster Amazon OpenSearch Service o dalla raccolta OpenSearch Serverless. Se il cluster o la raccolta è protetto da un VPC, assicurati che la configurazione di rete consenta la connettività».

Codice di errore	Messaggio di errore e informazioni
<code>OS.GatewayTimeout</code>	«Firehose ha riscontrato errori di timeout durante la connessione al cluster Amazon OpenSearch Service o alla raccolta OpenSearch Serverless».
<code>OS.MalformedData</code>	«Amazon Data Firehose non supporta i comandi dell'API Amazon OpenSearch Service Bulk all'interno del record Firehose».
<code>OS.ResponseEntryCountMismatch</code>	"La risposta dell'API bulk conteneva più voci del numero di record inviati. Assicurati che ogni record contenga un solo oggetto JSON e che non ci siano nuove righe".

Errori di invocazione Lambda

Amazon Data Firehose può inviare i seguenti errori di chiamata Lambda ai log. CloudWatch

Codice di errore	Messaggio di errore e informazioni
<code>Lambda.AssumeRoleAccessDenied</code>	"L'accesso è stato negato. Assicurati che la policy di fiducia per il ruolo IAM fornito consenta ad Amazon Data Firehose di assumere il ruolo.»
<code>Lambda.InvokeAccessDenied</code>	"L'accesso è stato negato. Verifica che la policy di accesso consenta l'accesso alla funzione Lambda".
<code>Lambda.JsonProcessingException</code>	"Si è verificato un errore durante l'analisi dei record restituiti dalla funzione Lambda. Assicurati che i record restituiti seguano il modello di stato richiesto da Amazon Data Firehose.» Per ulteriori informazioni, consulta Parametri richiesti per la trasformazione dei dati .
<code>Lambda.InvokeLimitExceeded</code>	"Il limite di esecuzioni simultanee di Lambda è stato superato. Aumenta il limite di esecuzioni simultanee".

Codice di errore	Messaggio di errore e informazioni
	Per ulteriori informazioni, consulta la sezione Limiti di AWS Lambda nella Guida per sviluppatori di AWS Lambda .
Lambda.DuplicatedRecordId	"Sono stati restituiti più record con lo stesso ID. Assicurati che la funzione Lambda restituisca un record univoco IDs per ogni record.» Per ulteriori informazioni, consulta Parametri richiesti per la trasformazione dei dati .
Lambda.MissingRecordId	«Uno o più record non IDs sono stati restituiti. Assicurati che la funzione Lambda restituisca tutti i record IDs ricevuti.» Per ulteriori informazioni, consulta Parametri richiesti per la trasformazione dei dati .
Lambda.ResourceNotFound	"La funzione Lambda specificata non esiste. Utilizza un'altra funzione esistente".
Lambda.InvalidSubnetIDException	"L'ID sottorete specificato nella configurazione VPC della funzione Lambda non è valido. Verifica che l'ID sottorete sia valido".
Lambda.InvalidSecurityGroupIDException	"L'ID del gruppo di sicurezza specificato nella configurazione VPC della funzione Lambda non è valido. Verifica che l'ID del gruppo di sicurezza sia valido".
Lambda.SubnetIPAddressLimitReachedException	«non AWS Lambda è stato in grado di configurare l'accesso VPC per la funzione Lambda perché una o più sottoreti configurate non hanno indirizzi IP disponibili. Aumenta il limite di indirizzi IP". Per ulteriori informazioni, consulta Limiti di Amazon VPC - VPC e sottoreti nella Guida per l'utente di Amazon VPC.

Codice di errore	Messaggio di errore e informazioni
<code>Lambda.ENILimitReachedException</code>	<p>«non AWS Lambda è stato in grado di creare un'interfaccia di rete elastica (ENI) nel VPC, specificata come parte della configurazione della funzione Lambda, perché è stato raggiunto il limite per le interfacce di rete. Aumenta il limite di interfacce di rete».</p> <p>Per ulteriori informazioni, consulta Limiti di Amazon VPC - Interfacce di rete nella Guida per l'utente di Amazon VPC.</p>
<code>Lambda.FunctionTimeout</code>	<p>Si è verificato il timeout dell'invocazione della funzione Lambda. Aumenta l'impostazione Timeout nella funzione Lambda. Per ulteriori informazioni, consulta Configurazione del timeout della funzione.</p>
<code>Lambda.FunctionError</code>	<p>Può essere dovuto a uno dei seguenti errori:</p> <ul style="list-style-type: none"> • Struttura di output non valida. Controlla la funzione e assicurati che l'output sia nel formato richiesto. Inoltre, assicurati che i record elaborati contengano uno stato di risultato valido pari a <code>Dropped</code>, <code>Ok</code> o <code>ProcessingFailed</code>. • La funzione Lambda è stata richiamata correttamente ma ha restituito un risultato di errore. • Lambda non è riuscito a decrittografare le variabili di ambiente perché l'accesso a KMS è stato negato. Controlla le impostazioni delle chiavi KMS della funzione e la policy delle chiavi. Per ulteriori informazioni, consulta Risoluzione dei problemi di accesso con chiave.
<code>Lambda.FunctionRequestTimeout</code>	<p>Amazon Data Firehose ha rilevato che la richiesta non è stata completata prima dell'errore di configurazione del timeout della richiesta durante l'invocazione di Lambda. Rivedi il codice Lambda per verificare se il codice Lambda deve essere eseguito oltre il timeout configurato. In tal caso, valuta la possibilità di ottimizzare le impostazioni di configurazione di Lambda, inclusa la memoria, il timeout. Per ulteriori informazioni, consulta Configurazione delle opzioni della funzione Lambda.</p>

Codice di errore	Messaggio di errore e informazioni
<code>Lambda.TargetServerFailedToRespond</code>	Amazon Data Firehose ha riscontrato un errore. Il server di destinazione non è riuscito a rispondere all'errore durante la chiamata al AWS servizio Lambda.
<code>Lambda.InvalidZipFileException</code>	Amazon Data Firehose rilevato <code>InvalidZipFileException</code> durante l'invocazione della funzione Lambda. Controlla le impostazioni di configurazione della funzione Lambda e il file zip del codice Lambda.
<code>Lambda.InternalServerError</code>	«Amazon Data Firehose rilevato <code>InternalServerError</code> durante la chiamata al servizio Lambda AWS . Amazon Data Firehose riproverà a inviare i dati un numero fisso di volte. Puoi specificare o ignorare le opzioni di nuovo tentativo utilizzando o. <code>CreateDeliveryStream</code> <code>UpdateDestination</code> APIs Se l'errore persiste, contatta il team di supporto AWS Lambda.
<code>Lambda.ServiceUnavailable</code>	Amazon Data Firehose rilevato <code>ServiceUnavailableException</code> durante la chiamata al servizio Lambda AWS . Amazon Data Firehose riproverà a inviare i dati un numero fisso di volte. Puoi specificare o ignorare le opzioni di nuovo tentativo utilizzando o. <code>CreateDeliveryStream</code> <code>UpdateDestination</code> APIs Se l'errore persiste, contatta l'assistenza AWS Lambda.
<code>Lambda.InvalidSecurityToken</code>	Impossibile richiamare la funzione Lambda a causa di un token di sicurezza non valido. L'invocazione Lambda tra partizioni non è supportata.

Codice di errore	Messaggio di errore e informazioni
<code>Lambda.InvocationFailure</code>	<p>Può essere dovuto a uno dei seguenti errori:</p> <ul style="list-style-type: none"> • Amazon Data Firehose ha riscontrato errori durante la chiamata a AWS Lambda. La distribuzione verrà riprovata; se l'errore persiste, verrà segnalato ad AWS affinché sia risolto". • Amazon Data Firehose ha rilevato un messaggio da <code>KMSInvalidStateException</code> Lambda. Lambda non è riuscito a decrittografare le variabili di ambiente perché la chiave KMS utilizzata è in uno stato non valido per Decrittografa. Controlla la chiave KMS della funzione Lambda. • Amazon Data Firehose ha incontrato un utente proveniente da AWS <code>LambdaException</code> Lambda. Lambda non è riuscita a inizializzare l'immagine del container fornita. Verifica l'immagine. • Amazon Data Firehose ha riscontrato errori di timeout durante la chiamata a Lambda. AWS Il timeout massimo della funzione supportato è di 5 minuti. Per ulteriori informazioni consulta Durata dell'esecuzione della trasformazioni dei dati.
<code>Lambda.JsonMappingException</code>	Si è verificato un errore durante l'analisi dei record restituiti dalla funzione Lambda. Assicurati che il campo dati sia codificato in base 64.

Errori di invocazione Kinesis

Amazon Data Firehose può inviare i seguenti errori di invocazione Kinesis ai log. CloudWatch

Codice di errore	Messaggio di errore e informazioni
<code>Kinesis.AccessDenied</code>	"L'accesso è stato negato durante la chiamata a Kinesis. Assicurati che la policy di accesso sul ruolo IAM utilizzato consenta l'accesso al Kinesis APIs appropriato».

Codice di errore	Messaggio di errore e informazioni
<code>Kinesis.ResourceNotFound</code>	"Firehose non è riuscito a leggere il flusso. Se il Firehose è collegato al flusso Kinesis, il flusso potrebbe non esistere o la partizione potrebbe essere stata unita o divisa. Se il Firehose è di DirectPut tipo, il Firehose potrebbe non esistere più.»
<code>Kinesis.SubscriptionRequired</code>	"L'accesso è stato negato durante la chiamata a Kinesis. Assicurati che il ruolo IAM assegnato per l'accesso allo stream Kinesis includa un abbonamento AWS Kinesis».
<code>Kinesis.Throttling</code>	"Si è verificato un errore di limitazione durante la chiamata a Kinesis. Ciò può essere dovuto al fatto che altre applicazioni chiamano lo APIs stesso flusso Firehose o al fatto che sono stati creati troppi stream Firehose con lo stesso flusso Kinesis come sorgente.»
<code>Kinesis.Throttling</code>	"Si è verificato un errore di limitazione durante la chiamata a Kinesis. Ciò può essere dovuto al fatto che altre applicazioni chiamano lo APIs stesso flusso Firehose o al fatto che sono stati creati troppi stream Firehose con lo stesso flusso Kinesis come sorgente.»
<code>Kinesis.AccessDenied</code>	"L'accesso è stato negato durante la chiamata a Kinesis. Assicurati che la policy di accesso sul ruolo IAM utilizzato consenta l'accesso al Kinesis APIs appropriato».
<code>Kinesis.AccessDenied</code>	«L'accesso è stato negato durante il tentativo di richiamare le operazioni API sul Kinesis Stream sottostante. Assicurati che il ruolo IAM sia diffuso e valido».
<code>Kinesis.KMS.AccessDeniedException</code>	«Firehose non ha accesso alla chiave KMS utilizzata per encrypt/decrypt Kinesis Stream. Concedi al ruolo di distribuzione di Firehose l'accesso alla chiave".
<code>Kinesis.KMS.KeyDisabled</code>	«Firehose non è in grado di leggere dal Kinesis Stream sorgente perché la chiave KMS utilizzata è disabilitata. encrypt/decrypt Abilita la chiave in modo che le letture possano continuare".

Codice di errore	Messaggio di errore e informazioni
<code>Kinesis.KMS.InvalidStateException</code>	"Firehose non è in grado di leggere dal flusso Kinesis di origine perché la chiave KMS utilizzata per crittografarlo è in uno stato non valido".
<code>Kinesis.KMS.NotFoundException</code>	"Firehose non è in grado di leggere dal flusso Kinesis di origine perché la chiave KMS utilizzata per crittografarlo non è stata trovata".

Errori di invocazione Kinesis DirectPut

Amazon Data Firehose può inviare i seguenti errori di DirectPut invocazione Kinesis ai log. CloudWatch

Codice di errore	Messaggio di errore e informazioni
<code>Firehose.KMS.AccessDeniedException</code>	"Firehose non ha accesso alla chiave KMS. Controlla la policy delle chiavi".
<code>Firehose.KMS.InvalidStateException</code>	"Firehose non è in grado di decrittografare i dati perché la chiave KMS utilizzata per crittografarli è in uno stato non valido".
<code>Firehose.KMS.NotFoundException</code>	"Firehose non è in grado di decrittografare i dati perché la chiave KMS utilizzata per crittografarli non è stata trovata".
<code>Firehose.KMS.KeyDisabled</code>	"Firehose non è in grado di decrittografare i dati perché la chiave KMS utilizzata per crittografare i dati è disabilitata. Abilita la chiave in modo che la distribuzione dei dati possa continuare".

AWS Glue errori di invocazione

Amazon Data Firehose può inviare i seguenti errori di AWS Glue chiamata ai log. CloudWatch

Codice di errore	Messaggio di errore e informazioni
DataFormatConversion.InvalidSchema	"Lo schema non è valido".
DataFormatConversion.EntityNotFound	«L'oggetto specificato non è table/database stato trovato. Assicurati che table/database esista e che i valori forniti nella configurazione dello schema siano corretti, in particolare per quanto riguarda l'involucro.»
DataFormatConversion.InvalidInput	"Impossibile trovare uno schema corrispondente su Glue. Assicurati che il database specificato con l'ID di catalogo fornito esista".
DataFormatConversion.InvalidInput	"Impossibile trovare uno schema corrispondente su Glue. Assicurati che l'ARN trasmesso sia nel formato corretto".
DataFormatConversion.InvalidInput	"Impossibile trovare uno schema corrispondente su Glue. Assicurati che il catalogId fornito sia valido".
DataFormatConversion.InvalidVersionId	"Impossibile trovare uno schema corrispondente su Glue. Assicurati che la versione specificata della tabella esista".
DataFormatConversion	"Impossibile trovare uno schema corrispondente su Glue. Assicurati che la tabella sia configurata con un descrittore di archiviazione non nullo contenente le colonne di destinazione".

Codice di errore	Messaggio di errore e informazioni
<code>on.NonExistentColumns</code>	
<code>DataFormatConversion.AccessDenied</code>	"L'accesso è stato negato quando si è assunto il ruolo. Assicurati che il ruolo specificato nella configurazione di conversione del formato dei dati abbia concesso al servizio Firehose l'autorizzazione ad assumerlo".
<code>DataFormatConversion.ThrottledByGlue</code>	"Si è verificato un errore di limitazione durante la chiamata a Glue. Aumenta il limite di frequenza delle richieste o riduci l'attuale frequenza di chiamate a Glue tramite altre applicazioni".
<code>DataFormatConversion.AccessDenied</code>	"L'accesso è stato negato durante la chiamata a Glue. Assicurati che il ruolo specificato nella configurazione di conversione del formato dei dati abbia le autorizzazioni necessarie".
<code>DataFormatConversion.InvalidGlueRole</code>	"Ruolo non valido. Assicurati che il ruolo specificato nella configurazione di conversione del formato dei dati esista".
<code>DataFormatConversion.InvalidGlueRole</code>	"Il token di sicurezza incluso nella richiesta non è valido. Assicurati che il ruolo IAM fornito associato a Firehose non venga eliminato".
<code>DataFormatConversion.GlueNotAvailableInRegion</code>	«AWS Glue non è ancora disponibile nella regione specificata; specifica un'altra regione».

Codice di errore	Messaggio di errore e informazioni
<code>DataFormatConversion.GlueEncryptionException</code>	"Si è verificato un errore durante il recupero della chiave master. Assicurati che la chiave esista e disponga delle autorizzazioni di accesso corrette".
<code>DataFormatConversion.SchemaValidationTimeout</code>	"Timeout durante il recupero della tabella da Glue. Se hai un gran numero di versioni della tabella Glue, aggiungi l'autorizzazione «glue:GetTableVersion» (consigliata) o elimina le versioni di tabella non utilizzate. Se non disponi di un numero elevato di tabelle in Glue, contatta l' AWS assistenza.»
<code>DataFirehose.InternalError</code>	"Timeout durante il recupero della tabella da Glue. Se hai un gran numero di versioni della tabella Glue, aggiungi l'autorizzazione «glue:GetTableVersion» (consigliata) o elimina le versioni di tabella non utilizzate. Se non disponi di un numero elevato di tabelle in Glue, contatta l' AWS assistenza.»
<code>DataFormatConversion.GlueEncryptionException</code>	"Si è verificato un errore durante il recupero della chiave master. Assicurati che la chiave esista e che lo stato sia corretto".

DataFormatConversion errori di invocazione

Amazon Data Firehose può inviare i seguenti errori di DataFormatConversion chiamata ai log. CloudWatch

Codice di errore	Messaggio di errore e informazioni
<code>DataFormatConversion.InvalidSchema</code>	"Lo schema non è valido".

Codice di errore	Messaggio di errore e informazioni
<code>DataFormatConversion.ValidationException</code>	"I nomi e i tipi di colonna devono essere stringhe non vuote".
<code>DataFormatConversion.ParseError</code>	"È stato rilevato un codice JSON di formato non valido".
<code>DataFormatConversion.MalformedData</code>	"I dati non corrispondono allo schema".
<code>DataFormatConversion.MalformedData</code>	"La lunghezza della chiave json non deve essere maggiore di 262144"
<code>DataFormatConversion.MalformedData</code>	"I dati non possono essere decodificati come UTF-8".
<code>DataFormatConversion.MalformedData</code>	"È stato trovato un carattere non valido tra i token".
<code>DataFormatConversion.InvalidTypeFormat</code>	"Il formato del tipo non è valido. Controlla la sintassi del tipo".

Codice di errore	Messaggio di errore e informazioni
<code>DataFormatConversion.InvalidSchema</code>	"Schema non valido. Assicuratevi che non vi siano caratteri speciali o spazi bianchi nei nomi delle colonne».
<code>DataFormatConversion.InvalidRecord</code>	"Il record non è conforme allo schema. Una o più chiavi della mappa non erano valide per la mappa <string,string>".
<code>DataFormatConversion.MalformedData</code>	"Il JSON di input conteneva una primitiva al livello superiore. Il livello superiore deve essere un oggetto o un array".
<code>DataFormatConversion.MalformedData</code>	"Il JSON di input conteneva una primitiva al livello superiore. Il livello superiore deve essere un oggetto o un array".
<code>DataFormatConversion.MalformedData</code>	"Il record era vuoto o conteneva solo spazi bianchi".
<code>DataFormatConversion.MalformedData</code>	"Sono stati rilevati caratteri non validi".
<code>DataFormatConversion.MalformedData</code>	"È stato rilevato un formato di timestamp non valido o non supportato. Consulta la guida per sviluppatori di Firehose per i formati di timestamp supportati".

Codice di errore	Messaggio di errore e informazioni
<code>DataFormatConversion.MalformedData</code>	"Nei dati è stato trovato un tipo scalare, ma nello schema è stato specificato un tipo complesso".
<code>DataFormatConversion.MalformedData</code>	"I dati non corrispondono allo schema".
<code>DataFormatConversion.MalformedData</code>	"Nei dati è stato trovato un tipo scalare, ma nello schema è stato specificato un tipo complesso".
<code>DataFormatConversion.ConversionFailureException</code>	"ConversionFailureException"
<code>DataFormatConversion.DataFormatException</code>	"DataFormatException"

Codice di errore	Messaggio di errore e informazioni
<code>DataFormatConversion.CustomerErrorException</code>	"DataFormatConversionCustomerErrorException"
<code>DataFormatConversion.MalformedData</code>	"I dati non corrispondono allo schema".
<code>DataFormatConversion.InvalidSchema</code>	"Lo schema non è valido".
<code>DataFormatConversion.MalformedData</code>	"I dati non corrispondono allo schema. Formato non valido per una o più date".
<code>DataFormatConversion.MalformedData</code>	"I dati contengono una struttura JSON altamente annidata che non è supportata".
<code>DataFormatConversion.EntityNotFound</code>	«L'oggetto specificato table/database non è stato trovato. Assicurati che table/database esista e che i valori forniti nella configurazione dello schema siano corretti, in particolare per quanto riguarda l'involucro.»

Codice di errore	Messaggio di errore e informazioni
DataFormatConversion.InvalidInput	"Impossibile trovare uno schema corrispondente su Glue. Assicurati che il database specificato con l'ID di catalogo fornito esista".
DataFormatConversion.InvalidInput	"Impossibile trovare uno schema corrispondente su Glue. Assicurati che l'ARN trasmesso sia nel formato corretto".
DataFormatConversion.InvalidInput	"Impossibile trovare uno schema corrispondente su Glue. Assicurati che il catalogId fornito sia valido".
DataFormatConversion.InvalidVersionId	"Impossibile trovare uno schema corrispondente su Glue. Assicurati che la versione specificata della tabella esista".
DataFormatConversion.NonExistentColumns	"Impossibile trovare uno schema corrispondente su Glue. Assicurati che la tabella sia configurata con un descrittore di archiviazione non nullo contenente le colonne di destinazione".
DataFormatConversion.AccessDenied	"L'accesso è stato negato quando si è assunto il ruolo. Assicurati che il ruolo specificato nella configurazione di conversione del formato dei dati abbia concesso al servizio Firehose l'autorizzazione ad assumerlo".
DataFormatConversion.ThrottledByGlue	"Si è verificato un errore di limitazione durante la chiamata a Glue. Aumenta il limite di frequenza delle richieste o riduci l'attuale frequenza di chiamate a Glue tramite altre applicazioni".

Codice di errore	Messaggio di errore e informazioni
<code>DataFormatConversion.AccessDenied</code>	"L'accesso è stato negato durante la chiamata a Glue. Assicurati che il ruolo specificato nella configurazione di conversione del formato dei dati abbia le autorizzazioni necessarie".
<code>DataFormatConversion.InvalidGlueRole</code>	"Ruolo non valido. Assicurati che il ruolo specificato nella configurazione di conversione del formato dei dati esista".
<code>DataFormatConversion.GlueNotAvailableInRegion</code>	«AWS Glue non è ancora disponibile nella regione specificata; specifica un'altra regione».
<code>DataFormatConversion.GlueEncryptionException</code>	"Si è verificato un errore durante il recupero della chiave master. Assicurati che la chiave esista e disponga delle autorizzazioni di accesso corrette".
<code>DataFormatConversion.SchemaValidationTimeout</code>	"Timeout durante il recupero della tabella da Glue. Se hai un gran numero di versioni della tabella Glue, aggiungi l'autorizzazione «glue:GetTableVersion» (consigliata) o elimina le versioni di tabella non utilizzate. Se non disponi di un numero elevato di tabelle in Glue, contatta l' AWS assistenza.»
<code>DataFirehose.InternalError</code>	"Timeout durante il recupero della tabella da Glue. Se hai un gran numero di versioni della tabella Glue, aggiungi l'autorizzazione «glue:GetTableVersion» (consigliata) o elimina le versioni di tabella non utilizzate. Se non disponi di un numero elevato di tabelle in Glue, contatta l' AWS assistenza.»

Codice di errore	Messaggio di errore e informazioni
DataFormatConversion.MalformedData	"Uno o più campi hanno un formato errato".

CloudWatch Log di accesso per Amazon Data Firehose

Puoi visualizzare i log degli errori relativi all'errore di consegna dei dati di Amazon Data Firehose utilizzando la console o la console Amazon Data Firehose. CloudWatch Le procedure seguenti mostrano come accedere ai log di errore utilizzando questi due metodi.

Per accedere ai log degli errori utilizzando la console Amazon Data Firehose

1. Accedere Console di gestione AWS e aprire la console Firehose all'indirizzo /Firehose <https://console.aws.amazon.com>
2. Nella barra di navigazione, scegli una regione. AWS
3. Scegli il nome di uno stream Firehose per accedere alla pagina dei dettagli dello stream Firehose.
4. Scegliere Error Log (Log errori) per visualizzare un elenco dei log di errori correlati a una mancata distribuzione di dati.

Per accedere ai log degli errori tramite la console CloudWatch

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nella barra di navigazione, scegli una regione.
3. Nel riquadro di navigazione scegli Logs (Log).
4. Scegliere un gruppo e un flusso di log per visualizzare un elenco dei log di errori correlati a una mancata distribuzione di dati.

Monitora lo stato di Kinesis Agent

Kinesis Agent pubblica CloudWatch metriche personalizzate con uno spazio dei nomi di `AWS KinesisAgent`. Aiuta a valutare se l'agente è integro, a inviare dati ad Amazon Data Firehose come specificato e a consumare la quantità appropriata di CPU e risorse di memoria sul produttore di dati.

Metriche come il numero di record e di byte inviati sono utili per comprendere la velocità con cui l'agente invia i dati al flusso Firehose. Quando questi parametri si trovano al di sotto delle soglie previste in alcune percentuali o passano a zero, potrebbe trattarsi di problemi di configurazione, di errori di rete o di problemi correlati allo stato dell'agente. I parametri come il consumo di CPU e memoria di host e i contatori di errore dell'agente indicano l'utilizzo delle risorse da parte del producer e forniscono informazioni utili in merito a possibili errori di configurazione o di host. Infine, l'agente registra anche le eccezioni di servizio per aiutare a verificare i problemi dell'agente.

I parametri dell'agente vengono riportati nella regione specificata nell'impostazione di configurazione dell'agente `cloudwatch.endpoint`. Per ulteriori informazioni, consulta [Specificare le impostazioni di configurazione dell'agente](#).

I parametri di Cloudwatch pubblicati da più Kinesis Agent vengono aggregati o combinati.

Esiste un addebito nominale per i parametri emessi da Kinesis Agent, che sono abilitati per impostazione predefinita. Per ulteriori informazioni, consulta la pagina [CloudWatch dei prezzi di Amazon](#).

Monitora con CloudWatch

Kinesis Agent invia le seguenti metriche a CloudWatch

Metrica	Description
<code>BytesSent</code>	Il numero di byte inviati allo stream Firehose nel periodo di tempo specificato. Unità: byte
<code>RecordSendAttempts</code>	Il numero di record tentati (sia per la prima volta che come nuovo tentativo) in una chiamata a <code>PutRecordBatch</code> durante il periodo di tempo specificato.

Metrica	Description
	Unità: numero
RecordSendErrors	Il numero di record che hanno restituito uno stato di errore in una chiamata a PutRecordBatch , inclusi i nuovi tentativi, durante il periodo di tempo specificato. Unità: numero
ServiceErrors	Il numero di chiamate a PutRecordBatch che hanno causato un errore di servizio (diverso da un errore di throttling) durante il periodo di tempo specificato. Unità: numero

Registra le chiamate API Amazon Data Firehose con AWS CloudTrail

Amazon Data Firehose è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Amazon Data Firehose. CloudTrail acquisisce tutte le chiamate API per Amazon Data Firehose come eventi. Le chiamate acquisite includono chiamate dalla console Amazon Data Firehose e chiamate in codice alle operazioni dell'API Amazon Data Firehose. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon Data Firehose. 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 ad Amazon Data Firehose, 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, incluso come configurarlo e abilitarlo, consulta la [Guida per l'AWS CloudTrail utente](#).

Informazioni su Firehose in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività di evento supportata in Amazon Data Firehose, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. È possibile

visualizzare, cercare e scaricare gli eventi recenti nell'account AWS . Per ulteriori informazioni, consulta [Visualizzazione di eventi mediante la cronologia eventi di CloudTrail](#).

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Amazon Data Firehose, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. 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 trail](#)
- [CloudTrail Servizi e integrazioni supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Amazon Data Firehose supporta la registrazione delle seguenti azioni come eventi nei CloudTrail file di registro:

- [CreateDeliveryStream](#)
- [DeleteDeliveryStream](#)
- [DescribeDeliveryStream](#)
- [ListDeliveryStreams](#)
- [ListTagsForDeliveryStream](#)
- [TagDeliveryStream](#)
- [StartDeliveryStreamEncryption](#)
- [StopDeliveryStreamEncryption](#)
- [UntagDeliveryStream](#)
- [UpdateDestination](#)

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, consulta [Elemento CloudTrail userIdentity](#).

Esempio: voci del file di registro Firehose

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 da qualsiasi sorgente e include informazioni sull'azione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. I file di log di CloudTrail non sono una traccia di stack ordinata delle chiamate API pubbliche, pertanto non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra le DeleteDeliveryStream azioni

CreateDeliveryStreamDescribeDeliveryStream,ListDeliveryStreams,UpdateDestination, e.

```
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/CloudTrail_Test_User",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "CloudTrail_Test_User"
      },
      "eventTime": "2016-02-24T18:08:22Z",
      "eventSource": "firehose.amazonaws.com",
      "eventName": "CreateDeliveryStream",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "aws-internal/3",
```

```

    "requestParameters":{
      "deliveryStreamName":"TestRedshiftStream",
      "redshiftDestinationConfiguration":{
        "s3Configuration":{
          "compressionFormat":"GZIP",
          "prefix":"prefix",
          "bucketARN":"arn:aws:s3:::amzn-s3-demo-bucket",
          "roleARN":"arn:aws:iam::111122223333:role/Firehose",
          "bufferingHints":{
            "sizeInMBs":3,
            "intervalInSeconds":900
          },
          "encryptionConfiguration":{
            "kMSEncryptionConfig":{
              "aWSKMSKeyARN":"arn:aws:kms:us-east-1:key"
            }
          }
        },
        "clusterJDBCURL":"jdbc:redshift://example.abc123.us-
west-2.redshift.amazonaws.com:5439/dev",
        "copyCommand":{
          "copyOptions":"copyOptions",
          "dataTableName":"dataTable"
        },
        "password":"","
        "username":"","
        "roleARN":"arn:aws:iam::111122223333:role/Firehose"
      }
    },
    "responseElements":{
      "deliveryStreamARN":"arn:aws:firehose:us-
east-1:111122223333:deliverystream/TestRedshiftStream"
    },
    "requestID":"958abf6a-db21-11e5-bb88-91ae9617edf5",
    "eventID":"875d2d68-476c-4ad5-bbc6-d02872cfc884",
    "eventType":"AwsApiCall",
    "recipientAccountId":"111122223333"
  },
  {
    "eventVersion":"1.02",
    "userIdentity":{
      "type":"IAMUser",
      "principalId":"AKIAIOSFODNN7EXAMPLE",
      "arn":"arn:aws:iam::111122223333:user/CloudTrail_Test_User",

```

```

        "accountId":"111122223333",
        "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
        "userName":"CloudTrail_Test_User"
    },
    "eventTime":"2016-02-24T18:08:54Z",
    "eventSource":"firehose.amazonaws.com",
    "eventName":"DescribeDeliveryStream",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"127.0.0.1",
    "userAgent":"aws-internal/3",
    "requestParameters":{"
        "deliveryStreamName":"TestRedshiftStream"
    },
    "responseElements":null,
    "requestID":"aa6ea5ed-db21-11e5-bb88-91ae9617edf5",
    "eventID":"d9b285d8-d690-4d5c-b9fe-d1ad5ab03f14",
    "eventType":"AwsApiCall",
    "recipientAccountId":"111122223333"
},
{
    "eventVersion":"1.02",
    "userIdentity":{"
        "type":"IAMUser",
        "principalId":"AKIAIOSFODNN7EXAMPLE",
        "arn":"arn:aws:iam::111122223333:user/CloudTrail_Test_User",
        "accountId":"111122223333",
        "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
        "userName":"CloudTrail_Test_User"
    },
    "eventTime":"2016-02-24T18:10:00Z",
    "eventSource":"firehose.amazonaws.com",
    "eventName":"ListDeliveryStreams",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"127.0.0.1",
    "userAgent":"aws-internal/3",
    "requestParameters":{"
        "limit":10
    },
    "responseElements":null,
    "requestID":"d1bf7f86-db21-11e5-bb88-91ae9617edf5",
    "eventID":"67f63c74-4335-48c0-9004-4ba35ce00128",
    "eventType":"AwsApiCall",
    "recipientAccountId":"111122223333"
},

```

```

{
  "eventVersion":"1.02",
  "userIdentity":{
    "type":"IAMUser",
    "principalId":"AKIAIOSFODNN7EXAMPLE",
    "arn":"arn:aws:iam::111122223333:user/CloudTrail_Test_User",
    "accountId":"111122223333",
    "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
    "userName":"CloudTrail_Test_User"
  },
  "eventTime":"2016-02-24T18:10:09Z",
  "eventSource":"firehose.amazonaws.com",
  "eventName":"UpdateDestination",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"127.0.0.1",
  "userAgent":"aws-internal/3",
  "requestParameters":{
    "destinationId":"destinationId-0000000000001",
    "deliveryStreamName":"TestRedshiftStream",
    "currentDeliveryStreamVersionId":"1",
    "redshiftDestinationUpdate":{
      "roleARN":"arn:aws:iam::111122223333:role/Firehose",
      "clusterJDBCURL":"jdbc:redshift://example.abc123.us-
west-2.redshift.amazonaws.com:5439/dev",
      "password":"",
      "username":"",
      "copyCommand":{
        "copyOptions":"copyOptions",
        "dataTableName":"dataTable"
      }
    },
    "s3Update":{
      "bucketARN":"arn:aws:s3:::amzn-s3-demo-bucket-update",
      "roleARN":"arn:aws:iam::111122223333:role/Firehose",
      "compressionFormat":"GZIP",
      "bufferingHints":{
        "sizeInMBs":3,
        "intervalInSeconds":900
      }
    },
    "encryptionConfiguration":{
      "kMSEncryptionConfig":{
        "aWSKMSKeyARN":"arn:aws:kms:us-east-1:key"
      }
    }
  },
  "prefix":"arn:aws:s3:::amzn-s3-demo-bucket"
}

```

```
    }
  },
  "responseElements":null,
  "requestID":"d549428d-db21-11e5-bb88-91ae9617edf5",
  "eventID":"1cb21e0b-416a-415d-bbf9-769b152a6585",
  "eventType":"AwsApiCall",
  "recipientAccountId":"111122223333"
},
{
  "eventVersion":"1.02",
  "userIdentity":{
    "type":"IAMUser",
    "principalId":"AKIAIOSFODNN7EXAMPLE",
    "arn":"arn:aws:iam::111122223333:user/CloudTrail_Test_User",
    "accountId":"111122223333",
    "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
    "userName":"CloudTrail_Test_User"
  },
  "eventTime":"2016-02-24T18:10:12Z",
  "eventSource":"firehose.amazonaws.com",
  "eventName":"DeleteDeliveryStream",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"127.0.0.1",
  "userAgent":"aws-internal/3",
  "requestParameters":{
    "deliveryStreamName":"TestRedshiftStream"
  },
  "responseElements":null,
  "requestID":"d85968c1-db21-11e5-bb88-91ae9617edf5",
  "eventID":"dd46bb98-b4e9-42ff-a6af-32d57e636ad1",
  "eventType":"AwsApiCall",
  "recipientAccountId":"111122223333"
}
]
}
```

Esempi di codice per l'utilizzo di Firehose AWS SDKs

I seguenti esempi di codice mostrano come utilizzare Firehose con un kit di sviluppo AWS software (SDK).

Le azioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le azioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati.

Scenari: esempi di codice che mostrano come eseguire un'attività specifica chiamando più funzioni all'interno dello stesso servizio o combinate con altri Servizi AWS.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di Firehose con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

- [Esempi di base per l'utilizzo di Firehose AWS SDKs](#)
 - [Azioni per l'utilizzo di Firehose AWS SDKs](#)
 - [Utilizzo PutRecord con un AWS SDK o una CLI](#)
 - [Utilizzo PutRecordBatch con un AWS SDK o una CLI](#)
- [Scenari per l'utilizzo di Firehose AWS SDKs](#)
 - [Utilizzare Amazon Data Firehose per elaborare record singoli e batch](#)

Esempi di base per l'utilizzo di Firehose AWS SDKs

I seguenti esempi di codice mostrano come utilizzare le nozioni di base di Amazon Data AWS SDKs Firehose con.

Esempi

- [Azioni per l'utilizzo di Firehose AWS SDKs](#)
 - [Utilizzo PutRecord con un AWS SDK o una CLI](#)
 - [Utilizzo PutRecordBatch con un AWS SDK o una CLI](#)

Azioni per l'utilizzo di Firehose AWS SDKs

I seguenti esempi di codice mostrano come eseguire singole azioni di Firehose con AWS SDKs. Ogni esempio include un collegamento a GitHub, dove è possibile trovare le istruzioni per la configurazione e l'esecuzione del codice.

Questi estratti chiamano l'API Firehose e sono estratti di codice da programmi più grandi che devono essere eseguiti in modo contestuale. È possibile visualizzare le azioni nel contesto in [Scenari per l'utilizzo di Firehose AWS SDKs](#).

Gli esempi seguenti includono solo le azioni più comunemente utilizzate. Per un elenco completo, consulta la [documentazione di riferimento dell'API Amazon Data Firehose](#).

Esempi

- [Utilizzo PutRecord con un AWS SDK o una CLI](#)
- [Utilizzo PutRecordBatch con un AWS SDK o una CLI](#)

Utilizzo **PutRecord** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare PutRecord.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- [Inserire i record in Firehose](#)

CLI

AWS CLI

Come scrivere un record in un flusso

L'esempio `put-record` seguente scrive dati in un flusso. I dati sono codificati nel formato Base64.

```
aws firehose put-record \  
  --delivery-stream-name my-stream \  
  --record '{"Data": "SGVsbG8gd29ybGQ="}'
```

Output:

```
{
  "RecordId": "RjB5K/nnoGFHqwTsZ1Nd/
TTqvjE8V5dsyXZTQn2JXrdpMT0wssyEb6nfC8fwf1whhwnItt4mvrn+gsqeK5jB7QjuLg283+Ps4Sz/
j1Xujv31iDhnPdaLw4B0yM9Amv7PcCuB2079RuM0NhoakbyUymlwY8yt20G8X2420wu1j1Fafhci4erAt7QhDEvpw
  "Encrypted": false
}
```

Per ulteriori informazioni, consulta [Invio di dati a un flusso di distribuzione Amazon Kinesis Data Firehose](#) nella Guida per sviluppatori di Amazon Kinesis Data Firehose.

- Per i dettagli sull'API, consulta [PutRecord AWS CLI Command Reference](#).

Java

SDK per Java 2.x

Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
/**
 * Puts a record to the specified Amazon Kinesis Data Firehose delivery
 * stream.
 *
 * @param record The record to be put to the delivery stream. The record must
 * be a {@link Map} of String keys and Object values.
 * @param deliveryStreamName The name of the Amazon Kinesis Data Firehose
 * delivery stream to which the record should be put.
 * @throws IllegalArgumentException if the input record or delivery stream
 * name is null or empty.
 * @throws RuntimeException if there is an error putting the record to the
 * delivery stream.
 */
public static void putRecord(Map<String, Object> record, String
deliveryStreamName) {
    if (record == null || deliveryStreamName == null ||
deliveryStreamName.isEmpty()) {
        throw new IllegalArgumentException("Invalid input: record or delivery
stream name cannot be null/empty");
    }
}
```

```

    }
    try {
        String jsonRecord = new ObjectMapper().writeValueAsString(record);
        Record firehoseRecord = Record.builder()

.data(SdkBytes.fromByteArray(jsonRecord.getBytes(StandardCharsets.UTF_8)))
        .build();

        PutRecordRequest putRecordRequest = PutRecordRequest.builder()
            .deliveryStreamName(deliveryStreamName)
            .record(firehoseRecord)
            .build();

        getFirehoseClient().putRecord(putRecordRequest);
        System.out.println("Record sent: " + jsonRecord);
    } catch (Exception e) {
        throw new RuntimeException("Failed to put record: " + e.getMessage(),
e);
    }
}

```

- Per i dettagli sull'API, consulta la [PutRecord](#) sezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```

class FirehoseClient:
    """
    AWS Firehose client to send records and monitor metrics.

    Attributes:
        config (object): Configuration object with delivery stream name and
region.
        delivery_stream_name (str): Name of the Firehose delivery stream.

```

```
    region (str): AWS region for Firehose and CloudWatch clients.
    firehose (boto3.client): Boto3 Firehose client.
    cloudwatch (boto3.client): Boto3 CloudWatch client.
"""

def __init__(self, config):
    """
    Initialize the FirehoseClient.

    Args:
        config (object): Configuration object with delivery stream name and
region.
    """
    self.config = config
    self.delivery_stream_name = config.delivery_stream_name
    self.region = config.region
    self.firehose = boto3.client("firehose", region_name=self.region)
    self.cloudwatch = boto3.client("cloudwatch", region_name=self.region)

@backoff.on_exception(
    backoff.expo, Exception, max_tries=5, jitter=backoff.full_jitter
)
def put_record(self, record: dict):
    """
    Put individual records to Firehose with backoff and retry.

    Args:
        record (dict): The data record to be sent to Firehose.

    This method attempts to send an individual record to the Firehose
delivery stream.
    It retries with exponential backoff in case of exceptions.
    """
    try:
        entry = self._create_record_entry(record)
        response = self.firehose.put_record(
            DeliveryStreamName=self.delivery_stream_name, Record=entry
        )
        self._log_response(response, entry)
    except Exception:
        logger.info(f"Fail record: {record}.")
        raise
```

- Per i dettagli sull'API, consulta [PutRecord AWSSDK for Python \(Boto3\) API Reference](#).

SAP ABAP

SDK per SAP ABAP

Note

C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
TRY.  
  DATA(lo_record) = NEW /aws1/cl_frhrecord( iv_data = iv_data ).  
  
  DATA(lo_result) = lo_frh->putrecord(  
    iv_deliverystreamname = iv_deliv_stream_name  
    io_record              = lo_record ).  
  
  MESSAGE 'Record sent to Firehose delivery stream.' TYPE 'I'.  
CATCH /aws1/cx_frhresourceindex.  
  MESSAGE 'Delivery stream not found.' TYPE 'E'.  
CATCH /aws1/cx_frhinvalidargumentex.  
  MESSAGE 'Invalid argument provided.' TYPE 'E'.  
CATCH /aws1/cx_frhserviceunavailex.  
  MESSAGE 'Service temporarily unavailable.' TYPE 'E'.  
ENDTRY.
```

- Per i dettagli sulle API, [PutRecord](#) consulta AWS SDK for SAP ABAP API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di Firehose con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **PutRecordBatch** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare PutRecordBatch.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- [Inserire i record in Firehose](#)

CLI

AWS CLI

Come scrivere più record in un flusso

L'esempio `put-record-batch` seguente scrive tre record in un flusso. I dati sono codificati nel formato Base64.

```
aws firehose put-record-batch \
  --delivery-stream-name my-stream \
  --records file://records.json
```

Contenuto di `myfile.json`:

```
[
  {"Data": "Rmlyc3QgdGhpbmc="},
  {"Data": "U2Vjb25kIHRoaW5n"},
  {"Data": "VGhpcmQgdGhpbmc="}
]
```

Output:

```
{
  "FailedPutCount": 0,
  "Encrypted": false,
  "RequestResponses": [
    {
      "RecordId": "9D20J6t2EqCTZTXwGzeSv/EVHxRoRCw89xd+o3+sXg8DhY0aWKPSmZy/CG1RVEys1u1xbeKh6VofEYKkoeiDrcjrxhQp9iF7sUW7pujiMEQ5LzlrzCkGosxQn+3boDnURDEaD42V7Giixp0yLJkYZcae1i7HzlCEoy9LJhMr8EjDSi40m/9Vc2uhwwuAtGE0XKpxJ2WD7ZRwtAnY1K",
    },
    {
      "RecordId": "jFirejqxCLlK5xjH/UNm1MvckjktEN76I7916X9PaZ+PVa0SXDFu1WG0qEZhxq2js7xcZ552eoeDxsuTU1MSq9nZTbVfb6cQTIXnm/GsuF37Uhg67GkmR5z9016XKJ+/"
    }
  ]
}
```

```
+pD1oFv7Hh9a3oUS6wYm3DcNRLTHHAimANp1PhkQvWpvLRfzbuCUkBphR2QVzhp90iHLbzGwy8/
DfH8sqWEUYASNJKS8GXP5s"
    },
    {
        "RecordId":
        "oy0amQ40o5Y2YV4vxzufdcM00w6n3EPr3tpPJGoYVNHK4APPVqNcbUgefo1stEFRg4hTLrf2k6eliHu/9+YJ5R3
DTBt3qBlmTj7Xq8SKVb01S7YvMTpWkMKA86f8JfmT8BMKoMb4XZS/s0kQLe+qh0sYKXW1"
    }
]
}
```

Per ulteriori informazioni, consulta [Invio di dati a un flusso di distribuzione Amazon Kinesis Data Firehose](#) nella Guida per sviluppatori di Amazon Kinesis Data Firehose.

- Per i dettagli sull'API, consulta [PutRecordBatch AWS CLI Command Reference](#).

Java

SDK per Java 2.x

Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
/**
 * Puts a batch of records to an Amazon Kinesis Data Firehose delivery
 * stream.
 *
 * @param records          a list of maps representing the records to be
 * sent
 * @param batchSize       the maximum number of records to include in each
 * batch
 * @param deliveryStreamName the name of the Kinesis Data Firehose delivery
 * stream
 * @throws IllegalArgumentException if the input parameters are invalid (null
 * or empty)
 * @throws RuntimeException       if there is an error putting the record
 * batch
 */
```

```
public static void putRecordBatch(List<Map<String, Object>> records, int
batchSize, String deliveryStreamName) {
    if (records == null || records.isEmpty() || deliveryStreamName == null ||
deliveryStreamName.isEmpty()) {
        throw new IllegalArgumentException("Invalid input: records or
delivery stream name cannot be null/empty");
    }
    ObjectMapper objectMapper = new ObjectMapper();

    try {
        for (int i = 0; i < records.size(); i += batchSize) {
            List<Map<String, Object>> batch = records.subList(i, Math.min(i +
batchSize, records.size()));

            List<Record> batchRecords = batch.stream().map(record -> {
                try {
                    String jsonRecord =
objectMapper.writeValueAsString(record);
                    return Record.builder()
.data(SdkBytes.fromByteArray(jsonRecord.getBytes(StandardCharsets.UTF_8)))
                    .build();
                } catch (Exception e) {
                    throw new RuntimeException("Error creating Firehose
record", e);
                }
            }).collect(Collectors.toList());

            PutRecordBatchRequest request = PutRecordBatchRequest.builder()
                .deliveryStreamName(deliveryStreamName)
                .records(batchRecords)
                .build();

            PutRecordBatchResponse response =
getFirehoseClient().putRecordBatch(request);

            if (response.failedPutCount() > 0) {
                response.requestResponses().stream()
                    .filter(r -> r.errorCode() != null)
                    .forEach(r -> System.err.println("Failed record: " +
r.errorMessage()));
            }
            System.out.println("Batch sent with size: " +
batchRecords.size());
        }
    }
}
```

```

    }
    } catch (Exception e) {
        throw new RuntimeException("Failed to put record batch: " +
e.getMessage(), e);
    }
}

```

- Per i dettagli sull'API, consulta la [PutRecordBatch](#) sezione AWS SDK for Java 2.x API Reference.

Python

SDK per Python (Boto3)

Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```

class FirehoseClient:
    """
    AWS Firehose client to send records and monitor metrics.

    Attributes:
        config (object): Configuration object with delivery stream name and
region.
        delivery_stream_name (str): Name of the Firehose delivery stream.
        region (str): AWS region for Firehose and CloudWatch clients.
        firehose (boto3.client): Boto3 Firehose client.
        cloudwatch (boto3.client): Boto3 CloudWatch client.
    """

    def __init__(self, config):
        """
        Initialize the FirehoseClient.

        Args:
            config (object): Configuration object with delivery stream name and
region.

```

```

"""
self.config = config
self.delivery_stream_name = config.delivery_stream_name
self.region = config.region
self.firehose = boto3.client("firehose", region_name=self.region)
self.cloudwatch = boto3.client("cloudwatch", region_name=self.region)

@backoff.on_exception(
    backoff.expo, Exception, max_tries=5, jitter=backoff.full_jitter
)
def put_record_batch(self, data: list, batch_size: int = 500):
    """
    Put records in batches to Firehose with backoff and retry.

    Args:
        data (list): List of data records to be sent to Firehose.
        batch_size (int): Number of records to send in each batch. Default is
500.

    This method attempts to send records in batches to the Firehose delivery
stream.
It retries with exponential backoff in case of exceptions.
    """
    for i in range(0, len(data), batch_size):
        batch = data[i : i + batch_size]
        record_dicts = [{"Data": json.dumps(record)} for record in batch]
        try:
            response = self.firehose.put_record_batch(
                DeliveryStreamName=self.delivery_stream_name,
                Records=record_dicts
            )
            self._log_batch_response(response, len(batch))
        except Exception as e:
            logger.info(f"Failed to send batch of {len(batch)} records.
Error: {e}")

```

- Per i dettagli sull'API, consulta [PutRecordBatch AWS SDK for Python \(Boto3\) API Reference](#).

Rust

SDK per Rust

Note

C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
async fn put_record_batch(
    client: &Client,
    stream: &str,
    data: Vec<Record>,
) -> Result<PutRecordBatchOutput, SdkError<PutRecordBatchError>> {
    client
        .put_record_batch()
        .delivery_stream_name(stream)
        .set_records(Some(data))
        .send()
        .await
}
```

- Per i dettagli sulle API, consulta la [PutRecordBatch](#) guida di riferimento all'API AWS SDK for Rust.

SAP ABAP

SDK per SAP ABAP

Note

C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
TRY.
    DATA(lo_result) = lo_frh->putrecordbatch(
```

```
        iv_deliverystreamname = iv_deliv_stream_name
        it_records             = it_records ).

DATA(lv_failed_count) = lo_result->get_failedputcount( ).

IF lv_failed_count > 0.
    MESSAGE |{ lv_failed_count } records failed to send.| TYPE 'I'.
ELSE.
    MESSAGE 'All records sent successfully to Firehose delivery stream.'
TYPE 'I'.
ENDIF.
CATCH /aws1/cx_frhresourcefoundex.
    MESSAGE 'Delivery stream not found.' TYPE 'E'.
CATCH /aws1/cx_frhinvalidargumentex.
    MESSAGE 'Invalid argument provided.' TYPE 'E'.
CATCH /aws1/cx_frhserviceunavaillex.
    MESSAGE 'Service temporarily unavailable.' TYPE 'E'.
ENDTRY.
```

- Per i dettagli sulle API, [PutRecordBatch](#) consulta AWS SDK for SAP ABAP API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di Firehose con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Scenari per l'utilizzo di Firehose AWS SDKs

I seguenti esempi di codice mostrano come implementare scenari comuni in Firehose con AWS SDKs. Questi scenari illustrano come eseguire attività specifiche chiamando più funzioni all'interno di Firehose o in combinazione con altri Servizi AWS. Ogni scenario include un collegamento al codice sorgente completo, dove è possibile trovare le istruzioni su come configurare ed eseguire il codice.

Gli scenari sono relativi a un livello intermedio di esperienza per aiutarti a comprendere le azioni di servizio nel contesto.

Esempi

- [Utilizzare Amazon Data Firehose per elaborare record singoli e batch](#)

Utilizzare Amazon Data Firehose per elaborare record singoli e batch

Gli esempi di codice seguenti mostrano come utilizzare Firehose per elaborare record singoli e batch.

Java

SDK per Java 2.x

Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

Questo esempio inserisce record singoli e batch in Firehose.

```
/**
 * Amazon Firehose Scenario example using Java V2 SDK.
 *
 * Demonstrates individual and batch record processing,
 * and monitoring Firehose delivery stream metrics.
 */
public class FirehoseScenario {

    private static FirehoseClient firehoseClient;
    private static CloudWatchClient cloudWatchClient;

    public static void main(String[] args) {
        final String usage = ""
            Usage:
                <deliveryStreamName>
            Where:
                deliveryStreamName - The Firehose delivery stream name.
            "";

        if (args.length != 1) {
            System.out.println(usage);
            return;
        }

        String deliveryStreamName = args[0];
```

```
    try {
        // Read and parse sample data.
        String jsonContent = readJsonFile("sample_records.json");
        ObjectMapper objectMapper = new ObjectMapper();
        List<Map<String, Object>> sampleData =
objectMapper.readValue(jsonContent, new TypeReference<>() {});

        // Process individual records.
        System.out.println("Processing individual records...");
        sampleData.subList(0, 100).forEach(record -> {
            try {
                putRecord(record, deliveryStreamName);
            } catch (Exception e) {
                System.err.println("Error processing record: " +
e.getMessage());
            }
        });

        // Monitor metrics.
        monitorMetrics(deliveryStreamName);

        // Process batch records.
        System.out.println("Processing batch records...");
        putRecordBatch(sampleData.subList(100, sampleData.size()), 500,
deliveryStreamName);
        monitorMetrics(deliveryStreamName);

    } catch (Exception e) {
        System.err.println("Scenario failed: " + e.getMessage());
    } finally {
        closeClients();
    }
}

private static FirehoseClient getFirehoseClient() {
    if (firehoseClient == null) {
        firehoseClient = FirehoseClient.builder()
            .region(Region.US_EAST_1)
            .build();
    }
    return firehoseClient;
}

private static CloudWatchClient getCloudWatchClient() {
```

```
        if (cloudWatchClient == null) {
            cloudWatchClient = CloudWatchClient.builder()
                .region(Region.US_EAST_1)
                .build();
        }
        return cloudWatchClient;
    }

    /**
     * Puts a record to the specified Amazon Kinesis Data Firehose delivery
     * stream.
     *
     * @param record The record to be put to the delivery stream. The record must
     * be a {@link Map} of String keys and Object values.
     * @param deliveryStreamName The name of the Amazon Kinesis Data Firehose
     * delivery stream to which the record should be put.
     * @throws IllegalArgumentException if the input record or delivery stream
     * name is null or empty.
     * @throws RuntimeException if there is an error putting the record to the
     * delivery stream.
     */
    public static void putRecord(Map<String, Object> record, String
    deliveryStreamName) {
        if (record == null || deliveryStreamName == null ||
    deliveryStreamName.isEmpty()) {
            throw new IllegalArgumentException("Invalid input: record or delivery
    stream name cannot be null/empty");
        }
        try {
            String jsonRecord = new ObjectMapper().writeValueAsString(record);
            Record firehoseRecord = Record.builder()

                .data(SdkBytes.fromByteArray(jsonRecord.getBytes(StandardCharsets.UTF_8)))
                .build();

            PutRecordRequest putRecordRequest = PutRecordRequest.builder()
                .deliveryStreamName(deliveryStreamName)
                .record(firehoseRecord)
                .build();

            getFirehoseClient().putRecord(putRecordRequest);
            System.out.println("Record sent: " + jsonRecord);
        } catch (Exception e) {
```

```
        throw new RuntimeException("Failed to put record: " + e.getMessage(),
e);
    }
}

/**
 * Puts a batch of records to an Amazon Kinesis Data Firehose delivery
stream.
 *
 * @param records          a list of maps representing the records to be
sent
 * @param batchSize       the maximum number of records to include in each
batch
 * @param deliveryStreamName the name of the Kinesis Data Firehose delivery
stream
 * @throws IllegalArgumentException if the input parameters are invalid (null
or empty)
 * @throws RuntimeException       if there is an error putting the record
batch
 */
public static void putRecordBatch(List<Map<String, Object>> records, int
batchSize, String deliveryStreamName) {
    if (records == null || records.isEmpty() || deliveryStreamName == null ||
deliveryStreamName.isEmpty()) {
        throw new IllegalArgumentException("Invalid input: records or
delivery stream name cannot be null/empty");
    }
    ObjectMapper objectMapper = new ObjectMapper();

    try {
        for (int i = 0; i < records.size(); i += batchSize) {
            List<Map<String, Object>> batch = records.subList(i, Math.min(i +
batchSize, records.size()));

            List<Record> batchRecords = batch.stream().map(record -> {
                try {
                    String jsonRecord =
objectMapper.writeValueAsString(record);
                    return Record.builder()
                        .data(SdkBytes.fromByteArray(jsonRecord.getBytes(StandardCharsets.UTF_8)))
                        .build();
                } catch (Exception e) {
```

```
        throw new RuntimeException("Error creating Firehose
record", e);
    }
}).collect(Collectors.toList());

PutRecordBatchRequest request = PutRecordBatchRequest.builder()
    .deliveryStreamName(deliveryStreamName)
    .records(batchRecords)
    .build();

PutRecordBatchResponse response =
getFirehoseClient().putRecordBatch(request);

    if (response.failedPutCount() > 0) {
        response.requestResponses().stream()
            .filter(r -> r.errorCode() != null)
            .forEach(r -> System.err.println("Failed record: " +
r.errorMessage()));
    }
    System.out.println("Batch sent with size: " +
batchRecords.size());
}
} catch (Exception e) {
    throw new RuntimeException("Failed to put record batch: " +
e.getMessage(), e);
}
}

public static void monitorMetrics(String deliveryStreamName) {
    Instant endTime = Instant.now();
    Instant startTime = endTime.minusSeconds(600);

    List<String> metrics = List.of("IncomingBytes", "IncomingRecords",
"FailedPutCount");
    metrics.forEach(metric -> monitorMetric(metric, startTime, endTime,
deliveryStreamName));
}

private static void monitorMetric(String metricName, Instant startTime,
Instant endTime, String deliveryStreamName) {
    try {
        GetMetricStatisticsRequest request =
GetMetricStatisticsRequest.builder()
            .namespace("AWS/Firehose")
```

```
        .metricName(metricName)

        .dimensions(Dimension.builder().name("DeliveryStreamName").value(deliveryStreamName).build())
        .startTime(startTime)
        .endTime(endTime)
        .period(60)
        .statistics(Statistic.SUM)
        .build();

        GetMetricStatisticsResponse response =
getCloudWatchClient().getMetricStatistics(request);
        double totalSum =
response.datapoints().stream().mapToDouble(Datapoint::sum).sum();
        System.out.println(metricName + ": " + totalSum);
    } catch (Exception e) {
        System.err.println("Failed to monitor metric " + metricName + ": " +
e.getMessage());
    }
}

public static String readJsonFile(String fileName) throws IOException {
    try (InputStream inputStream =
FirehoseScenario.class.getResourceAsStream("/" + fileName);
        Scanner scanner = new Scanner(inputStream, StandardCharsets.UTF_8))
    {
        return scanner.useDelimiter("\\\\A").next();
    } catch (Exception e) {
        throw new RuntimeException("Error reading file: " + fileName, e);
    }
}

private static void closeClients() {
    try {
        if (firehoseClient != null) firehoseClient.close();
        if (cloudWatchClient != null) cloudWatchClient.close();
    } catch (Exception e) {
        System.err.println("Error closing clients: " + e.getMessage());
    }
}
}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella documentazione di riferimento dell'API AWS SDK for Java 2.x .
 - [PutRecord](#)
 - [PutRecordBatch](#)

Python

SDK per Python (Boto3)

Note

C'è dell'altro GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

Questo script inserisce record singoli e batch in Firehose.

```
import json
import logging
import random
from datetime import datetime, timedelta

import backoff
import boto3

from config import get_config

def load_sample_data(path: str) -> dict:
    """
    Load sample data from a JSON file.

    Args:
        path (str): The file path to the JSON file containing sample data.

    Returns:
        dict: The loaded sample data as a dictionary.
    """
    with open(path, "r") as f:
        return json.load(f)
```

```
# Configure logging
logging.basicConfig(level=logging.INFO)
logger = logging.getLogger(__name__)

class FirehoseClient:
    """
    AWS Firehose client to send records and monitor metrics.

    Attributes:
        config (object): Configuration object with delivery stream name and
        region.
        delivery_stream_name (str): Name of the Firehose delivery stream.
        region (str): AWS region for Firehose and CloudWatch clients.
        firehose (boto3.client): Boto3 Firehose client.
        cloudwatch (boto3.client): Boto3 CloudWatch client.
    """

    def __init__(self, config):
        """
        Initialize the FirehoseClient.

        Args:
            config (object): Configuration object with delivery stream name and
            region.
        """
        self.config = config
        self.delivery_stream_name = config.delivery_stream_name
        self.region = config.region
        self.firehose = boto3.client("firehose", region_name=self.region)
        self.cloudwatch = boto3.client("cloudwatch", region_name=self.region)

    @backoff.on_exception(
        backoff.expo, Exception, max_tries=5, jitter=backoff.full_jitter
    )
    def put_record(self, record: dict):
        """
        Put individual records to Firehose with backoff and retry.

        Args:
            record (dict): The data record to be sent to Firehose.
        """
```

```

    This method attempts to send an individual record to the Firehose
    delivery stream.
    It retries with exponential backoff in case of exceptions.
    """
    try:
        entry = self._create_record_entry(record)
        response = self.firehose.put_record(
            DeliveryStreamName=self.delivery_stream_name, Record=entry
        )
        self._log_response(response, entry)
    except Exception:
        logger.info(f"Fail record: {record}.")
        raise

    @backoff.on_exception(
        backoff.expo, Exception, max_tries=5, jitter=backoff.full_jitter
    )
    def put_record_batch(self, data: list, batch_size: int = 500):
        """
        Put records in batches to Firehose with backoff and retry.

        Args:
            data (list): List of data records to be sent to Firehose.
            batch_size (int): Number of records to send in each batch. Default is
            500.

        This method attempts to send records in batches to the Firehose delivery
        stream.
        It retries with exponential backoff in case of exceptions.
        """
        for i in range(0, len(data), batch_size):
            batch = data[i : i + batch_size]
            record_dicts = [{"Data": json.dumps(record)} for record in batch]
            try:
                response = self.firehose.put_record_batch(
                    DeliveryStreamName=self.delivery_stream_name,
                    Records=record_dicts
                )
                self._log_batch_response(response, len(batch))
            except Exception as e:
                logger.info(f"Failed to send batch of {len(batch)} records.
                Error: {e}")

```

```

def get_metric_statistics(
    self,
    metric_name: str,
    start_time: datetime,
    end_time: datetime,
    period: int,
    statistics: list = ["Sum"],
) -> list:
    """
    Retrieve metric statistics from CloudWatch.

    Args:
        metric_name (str): The name of the metric.
        start_time (datetime): The start time for the metric statistics.
        end_time (datetime): The end time for the metric statistics.
        period (int): The granularity, in seconds, of the returned data
points.
        statistics (list): A list of statistics to retrieve. Default is
['Sum'].

    Returns:
        list: List of datapoints containing the metric statistics.
    """
    response = self.cloudwatch.get_metric_statistics(
        Namespace="AWS/Firehose",
        MetricName=metric_name,
        Dimensions=[
            {"Name": "DeliveryStreamName", "Value":
self.delivery_stream_name},
        ],
        StartTime=start_time,
        EndTime=end_time,
        Period=period,
        Statistics=statistics,
    )
    return response["Datapoints"]

def monitor_metrics(self):
    """
    Monitor Firehose metrics for the last 5 minutes.

    This method retrieves and logs the 'IncomingBytes', 'IncomingRecords',
and 'FailedPutCount' metrics

```

```

from CloudWatch for the last 5 minutes.
"""
end_time = datetime.utcnow()
start_time = end_time - timedelta(minutes=10)
period = int((end_time - start_time).total_seconds())

metrics = {
    "IncomingBytes": self.get_metric_statistics(
        "IncomingBytes", start_time, end_time, period
    ),
    "IncomingRecords": self.get_metric_statistics(
        "IncomingRecords", start_time, end_time, period
    ),
    "FailedPutCount": self.get_metric_statistics(
        "FailedPutCount", start_time, end_time, period
    ),
}

for metric, datapoints in metrics.items():
    if datapoints:
        total_sum = sum(datapoint["Sum"] for datapoint in datapoints)
        if metric == "IncomingBytes":
            logger.info(
                f"{metric}: {round(total_sum)} ({total_sum / (1024 *
1024):.2f} MB)"
            )
        else:
            logger.info(f"{metric}: {round(total_sum)}")
    else:
        logger.info(f"No data found for {metric} over the last 5
minutes")

def _create_record_entry(self, record: dict) -> dict:
    """
    Create a record entry for Firehose.

    Args:
        record (dict): The data record to be sent.

    Returns:
        dict: The record entry formatted for Firehose.

    Raises:

```

```
        Exception: If a simulated network error occurs.
    """
    if random.random() < 0.2:
        raise Exception("Simulated network error")
    elif random.random() < 0.1:
        return {"Data": '{"malformed": "data"}'}
    else:
        return {"Data": json.dumps(record)}

def _log_response(self, response: dict, entry: dict):
    """
    Log the response from Firehose.

    Args:
        response (dict): The response from the Firehose put_record API call.
        entry (dict): The record entry that was sent.
    """
    if response["ResponseMetadata"]["HTTPStatusCode"] == 200:
        logger.info(f"Sent record: {entry}")
    else:
        logger.info(f"Fail record: {entry}")

def _log_batch_response(self, response: dict, batch_size: int):
    """
    Log the batch response from Firehose.

    Args:
        response (dict): The response from the Firehose put_record_batch API
    call.
        batch_size (int): The number of records in the batch.
    """
    if response.get("FailedPutCount", 0) > 0:
        logger.info(
            f'Failed to send {response["FailedPutCount"]} records in batch of
    {batch_size}'
        )
    else:
        logger.info(f"Successfully sent batch of {batch_size} records")

if __name__ == "__main__":
    config = get_config()
    data = load_sample_data(config.sample_data_file)
    client = FirehoseClient(config)
```

```
# Process the first 100 sample network records
for record in data[:100]:
    try:
        client.put_record(record)
    except Exception as e:
        logger.info(f"Put record failed after retries and backoff: {e}")
client.monitor_metrics()

# Process remaining records using the batch method
try:
    client.put_record_batch(data[100:])
except Exception as e:
    logger.info(f"Put record batch failed after retries and backoff: {e}")
client.monitor_metrics()
```

Questo file contiene la configurazione per lo script precedente.

```
class Config:
    def __init__(self):
        self.delivery_stream_name = "ENTER YOUR DELIVERY STREAM NAME HERE"
        self.region = "us-east-1"
        self.sample_data_file = (
            "../../../../../scenarios/features/firehose/resources/
sample_records.json"
        )

def get_config():
    return Config()
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella documentazione di riferimento dell'API AWS SDK per Python (Boto3).
 - [PutRecord](#)
 - [PutRecordBatch](#)

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di Firehose con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Risolvi gli errori in Amazon Data Firehose

Se Firehose riscontra errori durante la consegna o l'elaborazione dei dati, riprova fino alla scadenza della durata del nuovo tentativo configurata. Se la durata del nuovo tentativo termina prima che i dati vengano consegnati correttamente, Firehose esegue il backup dei dati nel bucket di backup S3 configurato. Se la destinazione è Amazon S3 e la consegna non riesce o se la consegna al bucket S3 di backup fallisce, Firehose continua a riprovare fino al termine del periodo di conservazione.

Per informazioni sul tracciamento degli errori di consegna utilizzando, consulta [CloudWatch the section called "Monitoraggio con log CloudWatch"](#)

Direct PUT

Per gli stream `DirectPut` Firehose, Firehose conserva i record per 24 ore. Per uno stream Firehose la cui origine dati è un flusso di dati Kinesis, è possibile modificare il periodo di conservazione come descritto in [Modifica del periodo di conservazione dei dati](#). In questo caso, Firehose riprova le seguenti operazioni all'infinito: `DescribeStream`, e `GetRecords` `GetShardIterator`

Se lo stream Firehose utilizza `DirectPut`, controlla le `IncomingRecords` metriche `IncomingBytes` and per vedere se c'è traffico in entrata. Se utilizzi `PutRecord` o `PutRecordBatch`, assicurati di rilevare le eccezioni e riprova. Consigliamo una policy di tentativi con back-off esponenziale con jitter e diversi tentativi. Inoltre, se utilizzi l'`PutRecordBatchAPI`, assicurati che il codice controlli il valore di [FailedPutCount](#) nella risposta anche quando la chiamata API ha esito positivo.

Kinesis Data Stream

Se il flusso Firehose utilizza un flusso di dati Kinesis come origine, controlla le `IncomingRecords` metriche `IncomingBytes` e per il flusso di dati di origine. Inoltre, assicuratevi che le `DataReadFromKinesisStream.Records` metriche `DataReadFromKinesisStream.Bytes` and vengano emesse per lo stream Firehose.

Problemi comuni

Di seguito sono riportati alcuni suggerimenti per la risoluzione dei problemi più comuni durante l'utilizzo di uno stream Firehose.

Stream Firehose non disponibile

Lo stream Firehose non è disponibile come destinazione per CloudWatch Logs, CloudWatch Events o AWS IoT poiché alcuni AWS servizi possono inviare messaggi ed eventi solo a un flusso Firehose che si trova nello stesso. Regione AWS Verifica che lo stream di Firehose si trovi nella stessa regione degli altri servizi.

Nessun dato a destinazione

Se non ci sono problemi di inserimento dei dati e le metriche emesse per lo stream Firehose sembrano buone, ma non vedi i dati nella destinazione, controlla la logica del lettore. Assicurati che il lettore stia analizzando correttamente tutti i dati.

La metrica di freschezza dei dati aumenta o non viene emessa

La freschezza dei dati è una misura dell'attualità dei dati all'interno del flusso Firehose. È l'epoca del record di dati più vecchio del flusso Firehose, misurato dal momento in cui Firehose ha ingerito i dati fino ai giorni nostri. Firehose fornisce metriche che è possibile utilizzare per monitorare l'aggiornamento dei dati. Per identificare il parametro di aggiornamento dei dati per una determinata destinazione, consulta [the section called “Monitoraggio con metriche CloudWatch”](#).

Se abiliti il backup per tutti gli eventi o tutti i documenti, monitora due parametri distinti dell'aggiornamento dei dati: uno per la destinazione principale e uno per il backup.

Se la metrica di aggiornamento dei dati non viene emessa, significa che non esiste una distribuzione attiva per il flusso Firehose. Ciò accade quando la distribuzione dei dati è completamente bloccata o quando non ci sono dati in entrata.

Se il parametro di aggiornamento dei dati è in costante aumento significa che la distribuzione dei dati è in ritardo. Questo può accadere per uno dei seguenti motivi.

- La destinazione non può gestire il tasso di distribuzione. Se Firehose riscontra errori transitori dovuti all'elevato traffico, la consegna potrebbe subire ritardi. Questo può accadere per destinazioni diverse da Amazon S3 (può succedere per OpenSearch Service, Amazon Redshift o Splunk). Assicurati che la destinazione abbia una capacità sufficiente per gestire il traffico in entrata.
- La destinazione è lenta. La consegna dei dati potrebbe subire ritardi se Firehose riscontra una latenza elevata. Monitora il parametro di latenza della destinazione.
- La funzione Lambda è lenta. Ciò potrebbe portare a una velocità di consegna dei dati inferiore alla velocità di ingestione dei dati per il flusso Firehose. Se possibile, migliora l'efficienza della funzione

Lambda. Ad esempio, se la funzione esegue l'I/O di rete, utilizza più thread o l'I/O asincrono per aumentare il parallelismo. Inoltre, valuta l'opportunità di aumentare la dimensione della memoria della funzione Lambda in modo che l'allocazione della CPU possa incrementare di conseguenza. Questo potrebbe portare a invocazioni Lambda più veloci. Per informazioni sulla configurazione delle funzioni Lambda, consulta [Configurazione AWS](#) delle funzioni Lambda.

- Si sono verificati errori durante la distribuzione dei dati. Per informazioni su come monitorare gli errori utilizzando Amazon CloudWatch Logs, consulta [the section called “Monitoraggio con log CloudWatch”](#).
- Se l'origine dati del flusso Firehose è un flusso di dati Kinesis, è possibile che si verifichi una limitazione. Controlla i parametri `ThrottledGetRecords`, `ThrottledGetShardIterator` e `ThrottledDescribeStream`. Se al flusso di dati Kinesis sono associati più utenti, considera quanto segue:
 - Se i parametri `ThrottledGetRecords` e `ThrottledGetShardIterator` sono elevati, è consigliabile aumentare il numero di partizioni allestite per il flusso di dati.
 - Se il valore `ThrottledDescribeStream` è elevato, ti consigliamo di aggiungere `kinesis:listshards` autorizzazione al ruolo configurato in [KinesisStreamSourceConfiguration](#).
- Hint di buffering insufficienti per la destinazione. Ciò potrebbe aumentare il numero di viaggi di andata e ritorno che Firehose deve effettuare verso la destinazione, il che potrebbe causare ritardi nella consegna. Valuta l'opportunità di aumentare il valore degli hint di buffering. Per ulteriori informazioni, consulta [BufferingHints](#).
- Una durata elevata per i tentativi potrebbe causare un ritardo nella destinazione quando gli errori sono frequenti. Valuta l'opportunità di ridurre la durata dei tentativi. Inoltre, monitora gli errori e cerca di ridurli. Per informazioni su come monitorare gli errori utilizzando Amazon CloudWatch Logs, consulta [the section called “Monitoraggio con log CloudWatch”](#).
- Se la destinazione è `Splunk` e `DeliveryToSplunk.DataFreshness` è alto ma `DeliveryToSplunk.Success` sembra buono, il cluster Splunk potrebbe essere occupato. Libera il cluster Splunk, se possibile. In alternativa, contatta AWS Support e richiedi un aumento del numero di canali utilizzati da Firehose per comunicare con il cluster Splunk.

La conversione del formato di registrazione in Apache Parquet non riesce

Ciò accade se si prendono dati DynamoDB che includono `Set` il tipo, li si trasmette tramite Lambda a un flusso Firehose e si utilizza AWS Glue Data Catalog an per convertire il formato di record in Apache Parquet.

Quando il AWS Glue crawler indicizza i tipi di dati del set DynamoDB StringSet (NumberSet,, BinarySet and), li archivia nel catalogo dati rispettivamente come, e. SET<STRING> SET<BIGINT> SET<BINARY> Tuttavia, per convertire i record di dati nel formato Apache Parquet, Firehose richiede i tipi di dati Apache Hive. Poiché i tipi di set non sono tipi di dati Apache Hive validi, la conversione ha esito negativo. Per ottenere la conversione in modo che funzioni, aggiorna il catalogo dati con i tipi di dati Apache Hive. È possibile svolgere questa operazione modificando set in array nel catalogo dati.

Per modificare uno o più tipi di dati da **set** a **array** in un catalogo di dati AWS Glue

1. Accedi a Console di gestione AWS e apri la AWS Glue console all'indirizzo <https://console.aws.amazon.com/glue/>.
2. Nel riquadro a sinistra, sotto l'intestazione Data catalog (Catalogo dati), scegliere Tables (Tabelle).
3. Nell'elenco delle tabelle, scegliere il nome della tabella in cui è necessario modificare uno o più tipi di dati. In questo modo si accede alla pagina dei dettagli per il backup.
4. Scegli il pulsante Modifica schema nell'angolo in alto a destra della pagina dei dettagli.
5. Nella colonna Data type (Tipo di dati) scegliere il primo tipo di dati set.
6. Nell'elenco a discesa Column type (Tipo di colonna), modificare il tipo da set a array.
7. Nel ArraySchemacampo, inserisci o `array<string>` `array<int>` `array<binary>`, a seconda del tipo di dati appropriato per lo scenario.
8. Scegliere Aggiorna.
9. Ripetere i passaggi precedenti per convertire altri tipi set in tipi array.
10. Scegli Save (Salva).

Campi mancanti per l'oggetto trasformato per Lambda

Quando si utilizza la trasformazione dei dati Lambda per modificare i dati JSON in un oggetto Parquet, alcuni campi potrebbero mancare dopo la trasformazione. Ciò accade se l'oggetto JSON ha lettere maiuscole e la distinzione tra maiuscole e minuscole è impostata su `false`, il che può portare a una mancata corrispondenza delle chiavi JSON dopo la trasformazione dei dati, causando la mancanza di dati nell'oggetto Parquet risultante nel bucket s3.

Per risolvere questo problema, assicuratevi che la configurazione del tubo sia `deserializationOption: case.insensitive` impostata su `true` modo che le chiavi JSON corrispondano dopo la trasformazione.

Risoluzione dei problemi Amazon S3

Controlla quanto segue se i dati non vengono distribuiti al bucket Amazon Simple Storage Service (Amazon S3).

- Controlla Firehose `IncomingBytes` e le `IncomingRecords` metriche per assicurarti che i dati vengano inviati correttamente al tuo stream Firehose. Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose con parametri CloudWatch](#).
- Se la trasformazione dei dati con Lambda è abilitata, controlla la `ExecuteProcessingSuccess` metrica Firehose per assicurarti che Firehose abbia provato a richiamare la tua funzione Lambda. Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose con parametri CloudWatch](#).
- Controlla la `DeliveryToS3.Success` metrica Firehose per assicurarti che Firehose abbia provato a inserire dati nel tuo bucket Amazon S3. Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose con parametri CloudWatch](#).
- Abilitare la registrazione degli errori, se non è già attivata, e controllare i log di errore per gli errori di distribuzione. Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose utilizzando i log CloudWatch](#).
- Se nel registro viene visualizzato un messaggio di errore che dice «Firehose si è verificato un problema `InternalServerError` durante la chiamata al servizio Amazon S3. L'operazione verrà ritentata; se l'errore persiste, contatta S3 per la risoluzione.» , potrebbe essere dovuto al significativo aumento dei tassi di richiesta su una singola partizione in S3. Puoi ottimizzare i modelli di progettazione dei prefissi S3 per mitigare il problema. Per ulteriori informazioni, consulta [Modelli di progettazione basati sulle best practice: ottimizzazione delle prestazioni di Amazon S3](#). Se il problema persiste, contatta il AWS Supporto per ulteriore assistenza.
- Assicurati che il bucket Amazon S3 specificato nel tuo stream Firehose esista ancora.
- Se la trasformazione dei dati con Lambda è abilitata, assicuratevi che la funzione Lambda specificata nel flusso Firehose esista ancora.
- Assicurati che il ruolo IAM specificato nel tuo stream Firehose abbia accesso al tuo bucket S3 e alla funzione Lambda (se la trasformazione dei dati è abilitata). Inoltre, assicurati che il ruolo IAM abbia accesso al gruppo di log e ai flussi di CloudWatch log per controllare i log degli errori. Per ulteriori informazioni, consulta [Concedi a Firehose l'accesso a una destinazione Amazon S3](#).
- Se utilizzi la trasformazione dei dati, verifica che la funzione Lambda non restituisca mai risposte con dimensioni del payload che superino i 6 MB. Per ulteriori informazioni, consulta [Amazon Data FirehoseData Transformation](#).

Risoluzione dei problemi di Amazon Redshift

Controlla quanto segue se i dati non vengono distribuiti al cluster con provisioning Amazon Redshift o al gruppo di lavoro Amazon Redshift serverless.

Prima di essere caricati in Amazon Redshift, i dati vengono distribuiti al bucket S3. Se i dati non sono stati distribuiti sul bucket S3, consulta [Risoluzione dei problemi Amazon S3](#).

- Controlla la `DeliveryToRedshift.Success` metrica Firehose per assicurarti che Firehose abbia provato a copiare i dati dal tuo bucket S3 al cluster con provisioning di Amazon Redshift o al gruppo di lavoro Amazon Redshift Serverless. Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose con parametri CloudWatch](#).
- Abilitare la registrazione degli errori, se non è già attivata, e controllare i log di errore per gli errori di distribuzione. Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose utilizzando i log CloudWatch](#).
- Consulta la `STL_CONNECTION_LOG` tabella Amazon Redshift per vedere se Firehose è in grado di effettuare connessioni di successo. In questa tabella si dovrebbero poter vedere le connessioni e il loro stato in base a un nome utente. Per ulteriori informazioni, consulta [STL_CONNECTION_LOG](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- Se il controllo precedente mostra che le connessioni sono state stabilite, controlla la tabella `STL_LOAD_ERRORS` di Amazon Redshift per verificare il motivo dell'errore COPY. Per ulteriori informazioni, consulta [STL_LOAD_ERRORS](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- Assicurati che la configurazione di Amazon Redshift nel tuo stream Firehose sia accurata e valida.
- Assicurati che il ruolo IAM specificato nel tuo stream Firehose possa accedere al bucket S3 da cui Amazon Redshift copia i dati e anche alla funzione Lambda per la trasformazione dei dati (se la trasformazione dei dati è abilitata). Inoltre, assicurati che il ruolo IAM abbia accesso al gruppo di log e ai flussi di CloudWatch log per controllare i log degli errori. Per ulteriori informazioni, consulta [Concedi a Firehose l'accesso a una destinazione Amazon Redshift](#).
- Se il cluster con provisioning di Amazon Redshift o il gruppo di lavoro Serverless Amazon Redshift si trova in un cloud privato virtuale (VPC), assicurati che il cluster consenta l'accesso dagli indirizzi IP Firehose. Per ulteriori informazioni, consulta [Concedi a Firehose l'accesso a una destinazione Amazon Redshift](#).
- Assicurati che il cluster con provisioning Amazon Redshift o il gruppo di lavoro Amazon Redshift serverless sia disponibile pubblicamente.

- Se utilizzi la trasformazione dei dati, verifica che la funzione Lambda non restituisca mai risposte con dimensioni del payload che superino i 6 MB. Per ulteriori informazioni, consulta [Amazon Data FirehoseData Transformation](#).

Risoluzione dei problemi con Amazon OpenSearch Service

Controlla quanto segue se i dati non vengono consegnati al tuo dominio OpenSearch di servizio.

È possibile eseguire simultaneamente il backup dei dati sul bucket Amazon S3. Se i dati non sono stati distribuiti sul bucket S3, consulta [Risoluzione dei problemi Amazon S3](#).

- Controlla Firehose IncomingBytes e le IncomingRecords metriche per assicurarti che i dati vengano inviati correttamente al tuo stream Firehose. Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose con parametri CloudWatch](#).
- Se la trasformazione dei dati con Lambda è abilitata, controlla la ExecuteProcessingSuccess metrica Firehose per assicurarti che Firehose abbia provato a richiamare la tua funzione Lambda. Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose con parametri CloudWatch](#).
- Controllate la DeliveryToAmazonOpenSearchService.Success metrica Firehose per assicurarvi che Firehose abbia provato a indicizzare i dati nel cluster di servizi. OpenSearch Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose con parametri CloudWatch](#).
- Abilitare la registrazione degli errori, se non è già attivata, e controllare i log di errore per gli errori di distribuzione. Per ulteriori informazioni, consulta [Monitora Amazon Data Firehose utilizzando i log CloudWatch](#).
- Assicurati che la configurazione del OpenSearch servizio nel tuo stream Firehose sia accurata e valida.
- Se la trasformazione dei dati con Lambda è abilitata, assicuratevi che la funzione Lambda specificata nel flusso Firehose esista ancora. Inoltre, assicurati che il ruolo IAM abbia accesso al gruppo di log e ai flussi di CloudWatch log per controllare i log degli errori. Per ulteriori informazioni, consulta [Concessione FirehoseAccess a una destinazione di OpenSearch servizio pubblico](#).
- Assicurati che il ruolo IAM specificato nel tuo stream Firehose possa accedere al cluster di OpenSearch servizio, al bucket di backup S3 e alla funzione Lambda (se la trasformazione dei dati è abilitata). Inoltre, assicurati che il ruolo IAM abbia accesso al gruppo di log e ai flussi di CloudWatch log per controllare i log degli errori. Per ulteriori informazioni, consulta [Concedi a Firehose l'accesso a una destinazione di servizio pubblico OpenSearch](#).

- Se utilizzi la trasformazione dei dati, verifica che la funzione Lambda non restituisca mai risposte con dimensioni del payload che superino i 6 MB. Per ulteriori informazioni, consulta [Amazon Data FirehoseData Transformation](#).
- Amazon Data Firehose attualmente non supporta l'invio di CloudWatch log alla destinazione di Amazon Service perché OpenSearch CloudWatch Amazon combina più eventi di registro in un unico record Firehose e OpenSearch Amazon Service non può accettare più eventi di log in un unico record. In alternativa, puoi prendere in considerazione [l'utilizzo del filtro di abbonamento per Amazon OpenSearch Service in CloudWatch Logs](#).

Risoluzione dei problemi di Splunk

Controlla quanto segue se i dati non vengono distribuiti sull'endpoint Splunk.

- Se la tua piattaforma Splunk è in un VPC, assicurati che Firehose possa accedervi. Per ulteriori informazioni, consulta [Accesso a Splunk in VPC](#).
- Se utilizzi un AWS load balancer, assicurati che sia un Classic Load Balancer o un Application Load Balancer. Inoltre, abilita sessioni permanenti basate sulla durata con la scadenza dei cookie disabilitata per Classic Load Balancer e la scadenza è impostata al massimo (7 giorni) per Application Load Balancer. [Per informazioni su come eseguire questa operazione, consulta Duration-Based Session Stickiness for Classic Load Balancer o un Application Load Balancer](#).
- Riesaminare i requisiti della piattaforma Splunk. Il componente aggiuntivo Splunk per Firehose richiede la versione 6.6.X o successiva della piattaforma Splunk. Per ulteriori informazioni, consulta [Estensione Splunk per Amazon Kinesis Firehose](#).
- Se disponete di un proxy (Elastic Load Balancing o altro) tra Firehose e il nodo HTTP Event Collector (HEC), abilitate le sessioni permanenti per supportare i riconoscimenti HEC (). ACKs
- Verificare che si stia utilizzando un token HEC valido.
- Verificare che il token HEC sia abilitato.
- Controllare se i dati che si sta inviando a Splunk sono formattati correttamente. Per ulteriori informazioni, consulta [Formattare eventi per HTTP Event Collector](#).
- Verificare che il token HEC e l'evento di input siano configurati con un indice valido.
- Quando un caricamento su Splunk non va a buon fine a causa di un errore del server dal nodo HEC, la richiesta viene automaticamente ripetuta. Se tutti i nuovi tentativi non riescono, viene eseguito il backup dei dati su Amazon S3. Controlla se i dati appaiono in Amazon S3, il che è un'indicazione di un errore di questo tipo.

- Verificare di aver abilitato il riconoscimento dell'indicizzatore sul token HEC.
- Aumenta il valore della configurazione `HECAcknowledgmentTimeoutInSeconds` di destinazione Splunk del tuo stream Firehose.
- Aumenta il valore di `DurationInSeconds` under `RetryOptions` nella configurazione di destinazione Splunk del tuo stream Firehose.
- Verificare lo stato di HEC. L'abilitazione del controllo dello stato è un prerequisito per il trasferimento dei dati a Splunk.
- Se utilizzi la trasformazione dei dati, verifica che la funzione Lambda non restituisca mai risposte con dimensioni del payload che superino i 6 MB. Per ulteriori informazioni, consulta [Amazon Data Firehose Data Transformation](#).
- Verificare che il parametro Splunk denominato `ackIdleCleanup` sia impostato su `true`. Per impostazione predefinita, è impostato su `false`. Per impostare questo parametro su `true`, procedi nel seguente modo:
 - Per una [distribuzione gestita Splunk Cloud](#), inviare un caso tramite il portale di supporto Splunk. In questo caso, chiedere al supporto Splunk di abilitare HTTP event collector, di impostare `ackIdleCleanup` su `true` in `inputs.conf` e di creare o modificare il sistema di bilanciamento del carico da utilizzare con questa estensione.
 - Per una [distribuzione Splunk Enterprise distribuita](#), impostare il parametro `ackIdleCleanup` su `true` nel file `inputs.conf`. Per gli utenti *nix, questo file si trova in `$SPLUNK_HOME/etc/apps/splunk_httpinput/local/`. Per gli utenti Windows, si trova in `%SPLUNK_HOME%\etc\apps\splunk_httpinput\local\`.
 - Per una [distribuzione Splunk Enterprise a istanza singola](#), impostare il parametro `ackIdleCleanup` su `true` nel file `inputs.conf`. Per gli utenti *nix, questo file si trova in `$SPLUNK_HOME/etc/apps/splunk_httpinput/local/`. Per gli utenti Windows, si trova in `%SPLUNK_HOME%\etc\apps\splunk_httpinput\local\`.
- Assicurati che il ruolo IAM specificato nel tuo stream Firehose possa accedere al bucket di backup S3 e alla funzione Lambda per la trasformazione dei dati (se la trasformazione dei dati è abilitata). Inoltre, assicurati che il ruolo IAM abbia accesso al gruppo CloudWatch Logs e ai flussi di log per controllare i log degli errori. Per maggiori informazioni, consulta [Grant FirehoseAccess to a Splunk Destination](#).
- [Per reindirizzare i dati che sono stati consegnati al bucket di errore S3 \(backup S3\) su Splunk, segui i passaggi indicati nella documentazione di Splunk.](#)
- Consulta [Risoluzione dei problemi dell'estensione Splunk per Amazon Kinesis Firehose](#).

Risoluzione dei problemi relativi a Snowflake

Questa sezione descrive i passaggi più comuni per la risoluzione dei problemi relativi all'utilizzo di Snowflake come destinazione

La creazione dello stream Firehose non riesce

Se la creazione di un flusso Firehose non riesce per uno stream che fornisce dati a un cluster Snowflake PrivateLink abilitato, significa che il VPCE-ID non è raggiungibile da Firehose. Ciò può essere dovuto a uno dei seguenti motivi:

- VPCE-ID errato. Verificare che non vi siano errori tipografici.
- Firehose non supporta Snowflake senza regione in anteprima. URL Fornisci l'URL utilizzando Snowflake Account Locator. Consulta la documentazione di [Snowflake per maggiori dettagli](#).
- Verificate che lo stream Firehose sia stato creato nella stessa AWS regione della regione Snowflake.
- Se il problema persiste, contatta l'assistenza. AWS

Errori di consegna

Controlla quanto segue se i dati non vengono recapitati alla tua tabella Snowflake. I dati con consegna non riuscita di Snowflake verranno recapitati al bucket di errore S3 insieme a un codice di errore e a un messaggio di errore corrispondenti al payload. Di seguito sono riportati alcuni scenari di errore comuni. Per l'elenco completo dei codici di errore, vedere [Errori di consegna dei dati Snowflake](#).

- Codice di errore: Snowflake. DefaultRoleMissing: indica che il ruolo snowflake non è configurato durante la creazione del flusso Firehose. Se il ruolo Snowflake non è configurato, assicurati di impostare un ruolo predefinito per l'utente Snowflake specificato.
- Codice di errore: Snowflake. ExtraColumns: indica che l'inserimento in Snowflake viene rifiutato a causa di colonne aggiuntive nel payload di input. Le colonne non presenti nella tabella non devono essere specificate. Nota che i nomi delle colonne Snowflake fanno distinzione tra maiuscole e minuscole. Se la consegna non riesce con questo errore nonostante la colonna sia presente nella tabella, assicuratevi che il nome della colonna nel payload di input corrisponda al nome della colonna dichiarato nella definizione della tabella.

- Codice di errore: Snowflake. MissingColumns: Indica che l'inserimento in Snowflake viene rifiutato a causa della mancanza di colonne nel payload di input. Assicuratevi che i valori siano specificati per tutte le colonne che non possono essere annullate.
- Codice di errore: Snowflake. InvalidInput: Questo può accadere quando Firehose non riesce ad analizzare il payload di input fornito in un formato JSON valido. Assicuratevi che il payload json sia ben formato, che non contenga virgolette doppie, virgolette, caratteri di escape, ecc. Attualmente Firehose supporta solo un singolo elemento JSON come payload di record, gli array JSON non sono supportati.
- Codice di errore: Snowflake. InvalidValue: indica che la consegna non è riuscita a causa di un tipo di dati errato nel payload di input. Assicuratevi che i valori JSON specificati nel payload di input aderiscano al tipo di dati dichiarato nella definizione della tabella Snowflake.
- Codice di errore: Snowflake. InvalidTableType: indica che il tipo di tabella configurato nel flusso Firehose non è supportato. Fai riferimento alle [limitazioni \(in Limitazioni\)](#) dello streaming snowpipe per le tabelle, le colonne e i tipi di dati supportati.

Note

Per qualsiasi motivo, se la definizione della tabella o i permessi dei ruoli vengono modificati nella destinazione Snowflake dopo aver creato lo stream Firehose, Firehose può impiegare diversi minuti per rilevare tali modifiche. Se riscontrate errori di consegna a causa di ciò, prova a eliminare e ricreare lo stream Firehose.

Risoluzione dei problemi di raggiungibilità degli endpoint Firehose

Se l'API Firehose rileva un timeout, effettuate le seguenti operazioni per testare la raggiungibilità degli endpoint:

- Controlla se le richieste API vengono effettuate da un host in un VPC. Tutto il traffico proveniente da un VPC richiede la configurazione di un endpoint VPC Firehose. Per ulteriori informazioni, vedere [Utilizzo di Firehose](#) con AWS PrivateLink
- Se il traffico proviene da una rete pubblica o da un VPC con l'endpoint VPC Firehose configurato in una particolare sottorete, esegui i seguenti comandi dall'host per verificare la connettività di rete. L'endpoint Firehose è disponibile negli endpoint e nelle quote [Firehose](#).
 - Usa strumenti come traceroute o tcping per verificare se la configurazione di rete è corretta. Se fallisce, controlla le impostazioni di rete:

Esempio:

```
tracert firehose.us-east-2.amazonaws.com
```

or

```
tcping firehose.us-east-2.amazonaws.com 443
```

- Se sembra che l'impostazione di rete sia corretta e il seguente comando fallisce, controlla se [Amazon CA \(Certificate Authority\)](#) è nella catena di fiducia.

Esempio:

```
curl firehose.us-east-2.amazonaws.com
```

Se i comandi precedenti hanno esito positivo, riprova a utilizzare l'API per verificare se l'API restituisce una risposta.

Risoluzione dei problemi degli endpoint HTTP

Questa sezione descrive le procedure di risoluzione dei problemi più comuni quando si ha a che fare con Amazon Data Firehose che fornisce dati a destinazioni endpoint HTTP generiche e a destinazioni partner, tra cui Datadog, Dynatrace, LogicMonitor MongoDB, New Relic, Splunk o Sumo Logic. Ai fini di questa sezione, tutte le destinazioni applicabili sono indicate come endpoint HTTP. Assicurati che il ruolo IAM specificato nel tuo stream Firehose possa accedere al bucket di backup S3 e alla funzione Lambda per la trasformazione dei dati (se la trasformazione dei dati è abilitata). Inoltre, assicurati che il ruolo IAM abbia accesso al gruppo di log e ai flussi di CloudWatch log per controllare i log degli errori. Per ulteriori informazioni, vedere [Concedere l'accesso a Firehose a una destinazione di endpoint HTTP](#).

Note

Le informazioni contenute in questa sezione non si applicano alle seguenti destinazioni: Splunk, OpenSearch Service, S3 e Redshift.

CloudWatch Registri

Si consiglia vivamente di abilitare la [CloudWatch registrazione per](#). I log vengono pubblicati solo in caso di errori durante la distribuzione alla destinazione.

Eccezioni di destinazione

ErrorCode: HttpEndpoint.DestinationException

```
{
  "deliveryStreamARN": "arn:aws:firehose:us-east-1:123456789012:deliverystream/ronald-test",
  "destination": "custom.firehose.endpoint.com...",
  "deliveryStreamVersionId": 1,
  "message": "The following response was received from the endpoint destination.
413: {\"requestId\": \"43b8e724-dbac-4510-adb7-ef211c6044b9\", \"timestamp\":
1598556019164, \"errorMessage\": \"Payload too large\"}",
  "errorCode": "HttpEndpoint.DestinationException",
  "processor": "arn:aws:lambda:us-east-1:379522611494:function:httpLambdaProcessing"
}
```

Le eccezioni di destinazione indicano che Firehose è in grado di stabilire una connessione all'endpoint ed effettuare una richiesta HTTP, ma non ha ricevuto un codice di risposta 200. Anche le risposte 2xx che non sono 200 genereranno un'eccezione di destinazione. Amazon Data Firehose registra il codice di risposta e un payload di risposta troncato ricevuto dall'endpoint configurato in Logs. CloudWatch Poiché Amazon Data Firehose registra il codice di risposta e il payload senza modifiche o interpretazioni, spetta all'endpoint fornire il motivo esatto per cui ha rifiutato la richiesta di consegna HTTP di Amazon Data Firehose. Di seguito sono riportati i suggerimenti per la risoluzione dei problemi più comuni per queste eccezioni:

- 400: indica che stai inviando una richiesta errata a causa di un'errata configurazione di Amazon Data Firehose. Assicurati di avere [URL](#), [attributi comuni](#), [codifica del contenuto](#), [chiave di accesso](#) e [suggerimenti di buffering](#) corretti per la destinazione. Consulta la documentazione specifica della destinazione sulla configurazione richiesta.
- 401: indica che la chiave di accesso configurata per lo stream Firehose è errata o mancante.
- 403: indica che la chiave di accesso configurata per lo stream Firehose non dispone delle autorizzazioni per fornire dati all'endpoint configurato.

- 413: indica che il payload della richiesta che Amazon Data Firehose invia all'endpoint è troppo grande per essere gestito dall'endpoint. Prova a [ridurre il suggerimento di buffering](#) alla dimensione consigliata per la destinazione.
- 429: indica che Amazon Data Firehose invia richieste a una velocità superiore a quella gestita dalla destinazione. Ottimizza il suggerimento per il buffering aumentando il tempo di buffering e and/or aumentando la dimensione del buffering (ma sempre entro il limite della destinazione).
- 5xx: indica che esiste un problema con la destinazione. Il servizio Amazon Data Firehose funziona ancora correttamente.

Important

Importante: sebbene questi siano i suggerimenti più comuni per la risoluzione dei problemi, endpoint specifici possono avere diversi motivi per fornire i codici di risposta e i suggerimenti specifici per gli endpoint devono essere seguiti per primi.

Risposta non valida

ErrorCode: HttpEndpoint.InvalidResponseFromDestination

```
{
  "deliveryStreamARN": "arn:aws:firehose:us-east-1:123456789012:deliverystream/ronald-test",
  "destination": "custom.firehose.endpoint.com...",
  "deliveryStreamVersionId": 1,
  "message": "The response received from the specified endpoint is invalid. Contact the owner of the endpoint to resolve the issue. Response for request 2de9e8e9-7296-47b0-bea6-9f17b133d847 is not recognized as valid JSON or has unexpected fields. Raw response received: 200 {\"requestId\": null}\",
  "errorCode": "HttpEndpoint.InvalidResponseFromDestination",
  "processor": "arn:aws:lambda:us-east-1:379522611494:function:httpLambdaProcessing"
}
```

Le eccezioni di risposta non valida indicano che Amazon Data Firehose ha ricevuto una risposta non valida dalla destinazione dell'endpoint. La risposta deve essere conforme alle [specifiche di risposta](#), altrimenti Amazon Data Firehose considererà il tentativo di consegna un fallimento e riconsegnerà nuovamente gli stessi dati fino al superamento della durata del nuovo tentativo configurata. Amazon

Data Firehose considera le risposte che non rispettano le specifiche di risposta come errori, anche se la risposta ha lo stato 200. Se stai sviluppando un endpoint compatibile con Amazon Data Firehose, segui le specifiche di risposta per assicurarti che i dati vengano consegnati correttamente.

Di seguito sono riportati alcuni dei tipi comuni di risposte non valide e come risolverli:

- JSON non valido o campi imprevisti: indica che la risposta non può essere deserializzata correttamente come JSON o contiene campi imprevisti. Assicurati che la risposta non sia codificata nel contenuto.
- Mancante RequestId: indica che la risposta non contiene un RequestId.
- RequestId not match: indica che il RequestID nella risposta non corrisponde al RequestID in uscita.
- Timestamp mancante: indica che la risposta non contiene un campo timestamp. Il campo timestamp deve essere un numero e non una stringa.
- Intestazione Content-Type mancante: indica che la risposta non contiene un'intestazione "content-type: application/json". Non sono accettati altri content-type.

Important

[Importante: Amazon Data Firehose può fornire dati solo agli endpoint che seguono le specifiche di richiesta e risposta di Firehose.](#) Se stai configurando la tua destinazione con un servizio di terze parti, assicurati di utilizzare l'endpoint compatibile con Amazon Data Firehose corretto, che probabilmente sarà diverso dall'endpoint di ingestione pubblico. Ad esempio, l'endpoint Amazon Data Firehose di Datadog è `https://aws-kinesis-http-intake.logs.datadoghq.com/` mentre l'endpoint pubblico lo è `https://api.datadoghq.com/`

Altri errori comuni

Di seguito sono elencati codici di errore e definizioni aggiuntivi.

- Codice HttpStatusCode di errore: RequestTimeout - Indica che l'endpoint ha impiegato più di 3 minuti per rispondere. Se sei il proprietario della destinazione, riduci il tempo di risposta dell'endpoint di destinazione. Se non sei il proprietario della destinazione, contatta il proprietario e chiedi può ridurre il tempo di risposta (ad esempio ridurre il suggerimento di buffering in modo che la quantità di dati elaborati per richiesta sia inferiore).

- Codice di errore: `HttpEndpoint. ResponseTooLarge` - Indica che la risposta è troppo grande. La risposta deve essere inferiore a 1 MiB incluse le intestazioni.
- Codice di errore: `HttpEndpoint. ConnectionFailed` - Indica che non è stato possibile stabilire una connessione con l'endpoint configurato. Ciò potrebbe essere dovuto a un errore di battitura nell'URL configurato, all'inaccessibilità dell'endpoint ad Amazon Data Firehose o al fatto che l'endpoint impiega troppo tempo a rispondere alla richiesta di connessione.
- Codice di errore: `HttpEndpoint ConnectionReset` - Indica che è stata effettuata una connessione ma è stata ripristinata o chiusa prematuramente dall'endpoint.
- Codice di errore: `HttpEndpoint SSLHandshakeError`: indica che non è stato possibile completare correttamente un handshake SSL con l'endpoint configurato.

Risoluzione dei problemi relativi a MSK come origine

Questa sezione descrive le fasi comuni per la risoluzione dei problemi relativi all'utilizzo di MSK come origine

Note

Per la risoluzione dei problemi di elaborazione, trasformazione o distribuzione di S3, consulta le sezioni precedenti

Creazione di hose non riuscita

Controllate quanto segue se la creazione del tubo con MSK As Source non funziona:

- Verifica che lo stato del cluster MSK di origine sia attivo.
- Se utilizzi la connettività privata, assicurati che [Private Link sul cluster sia attivato](#).
- Se utilizzi la connettività pubblica, assicurati che [l'accesso pubblico sul cluster sia attivato](#).
- Se utilizzi la connettività privata, assicurati di aggiungere una [policy basata sulle risorse che consenta a Firehose di creare Private Link](#). Consultate anche: [Autorizzazioni MSK per più account](#).
- Assicurati che il ruolo nella configurazione del codice sorgente sia [autorizzato a importare dati dall'argomento del cluster](#).
- Assicurati che i tuoi gruppi di sicurezza VPC consentano il traffico in entrata sulle [porte utilizzate dai server bootstrap del cluster](#).

Hose sospeso

Controlla quanto segue se l'hose è in stato SOSPESO

- Verifica che lo stato del cluster MSK di origine sia attivo.
- Verifica che l'argomento di origine esista. Nel caso in cui l'argomento sia stato eliminato e ricreato, sarà necessario eliminare e ricreare anche lo stream Firehose.

Hose in contropressione

Il valore di `DataReadFromSource .Backpressured` sarà 1 quando `BytesPerSecondLimit` per partizione viene superato o se il normale flusso di distribuzione è lento o interrotto.

- Se stai raggiungendo, controlla la metrica `DataReadFromSource .Bytes` e `BytesPerSecondLimit` richiedi un aumento del limite.
- Controlla CloudWatch i log, le metriche di destinazione, le metriche di trasformazione dei dati e le metriche di conversione del formato per identificare i colli di bottiglia.

Aggiornamento dei dati non corretto

L'aggiornamento dei dati sembra errato

- Firehose calcola l'aggiornamento dei dati in base al timestamp del record utilizzato. Per garantire che questo timestamp venga registrato correttamente quando il record del produttore viene mantenuto nei log del broker di Kafka, imposta la configurazione del tipo di timestamp dell'argomento Kafka su `message .timestamp .type=LogAppendTime`.

Problemi di connessione al cluster MSK

La procedura seguente spiega come convalidare la connettività ai cluster MSK. Per informazioni dettagliate sulla configurazione del client Amazon MSK, consulta la [Guida introduttiva all'uso di Amazon MSK nella Amazon Managed Streaming for Apache Kafka Developer Guide](#).

Per convalidare la connettività ai cluster MSK

1. Crea un'istanza Amazon EC2 basata su UNIX (preferibilmente AL2). Se sul cluster è abilitata solo la connettività VPC, assicurati che l'istanza EC2 venga eseguita sullo stesso VPC. Accedi

tramite SSH all'istanza una volta che è disponibile. Per ulteriori informazioni, consulta [questo tutorial](#) nella Amazon EC2 User Guide.

2. Installa Java utilizzando il gestore di pacchetti Yum eseguendo il comando seguente. Per ulteriori informazioni, consulta le [istruzioni di installazione](#) nella Guida per l'utente di Amazon Corretto 8.

```
sudo yum install java-1.8.0
```

3. Installa il [AWS client](#) eseguendo il comando seguente.

```
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"  
unzip awscliv2.zip  
sudo ./aws/install
```

4. Scarica la versione 2.6* del client Apache Kafka eseguendo il comando seguente.

```
wget https://archive.apache.org/dist/kafka/2.6.2/kafka_2.12-2.6.2.tgz  
tar -xzf kafka_2.12-2.6.2.tgz
```

5. Vai alla directory `kafka_2.12-2.6.2/libs`, quindi esegui il comando per scaricare il file JAR IAM di Amazon MSK.

```
wget https://github.com/aws/aws-msk-iam-auth/releases/download/v1.1.3/aws-msk-iam-auth-1.1.3-all.jar
```

6. Crea il `client.properties` file nella cartella `bin` di Kafka.
7. Sostituiscilo `awsRoleArn` con il ruolo ARN che hai usato nel tuo Firehose `SourceConfiguration` e verifica la posizione del certificato. Consenti all'utente AWS client di assumere il ruolo. `awsRoleArn` AWS l'utente client tenterà di assumere il ruolo che hai specificato qui.

```
[ec2-user@ip-xx-xx-xx-xx bin]$ cat client.properties  
security.protocol=SASL_SSL  
sasl.mechanism=AWS_MSK_IAM  
sasl.jaas.config=software.amazon.msk.auth.iam.IAMLoginModule required  
  awsRoleArn="<role arn>" awsStsRegion="<region name>";  
sasl.client.callback.handler.class=software.amazon.msk.auth.iam.IAMClientCallbackHandler  
awsDebugCreds=true  
ssl.truststore.location=/usr/lib/jvm/java-1.8.0-  
openjdk-1.8.0.342.b07-1.amzn2.0.1.x86_64/jre/lib/security/cacerts
```

```
ssl.truststore.password=changeit
```

8. Esegui il seguente comando Kafka per elencare gli argomenti. Se la tua connessione è pubblica, usa i server Bootstrap degli endpoint pubblici. Se la tua connessione è privata, usa i server Bootstrap endpoint privati.

```
bin/kafka-topics.sh --list --bootstrap-server <bootstrap servers> --command-config  
bin/client.properties
```

Se la richiesta ha esito positivo, dovresti vedere un output simile all'esempio seguente.

```
[ec2-user@ip-xx-xx-xx-xx kafka_2.12-2.6.2]$ bin/kafka-topics.sh --list --bootstrap-  
server <bootstrap servers> --command-config bin/client.properties  
  
[xxxx-xx-xx 05:49:50,877] WARN The configuration 'awsDebugCreds' was supplied but  
isn't a known config. (org.apache.kafka.clients.admin.AdminClientConfig)  
[xxxx-xx-xx 05:49:50,878] WARN The configuration 'ssl.truststore.location' was  
supplied but isn't a known config.  
(org.apache.kafka.clients.admin.AdminClientConfig)  
[xxxx-xx-xx 05:49:50,878] WARN The configuration 'sasl.jaas.config' was supplied  
but isn't a known config. (org.apache.kafka.clients.admin.AdminClientConfig)  
[xxxx-xx-xx 05:49:50,878] WARN The configuration  
'sasl.client.callback.handler.class' was supplied but isn't a known config.  
(org.apache.kafka.clients.admin.AdminClientConfig)  
[xxxx-xx-xx 05:49:50,878] WARN The configuration 'ssl.truststore.password' was  
supplied but isn't a known config.  
(org.apache.kafka.clients.admin.AdminClientConfig)  
[xxxx-xx-xx 05:50:21,629] WARN [AdminClient clientId=adminclient-1] Connection to  
node...  
__amazon_msk_canary  
__consumer_offsets
```

9. In caso di problemi durante l'esecuzione dello script precedente, verifica che i server di bootstrap forniti siano raggiungibili sulla porta specificata. A tale scopo, è possibile scaricare e utilizzare telnet o un'utilità simile, come illustrato nel comando seguente.

```
sudo yum install telnet  
telnet <bootstrap servers><port>
```

Se la richiesta ha esito positivo, si otterrà il seguente risultato. Ciò significa che puoi connetterti al tuo cluster MSK all'interno del tuo VPC locale e che i server di bootstrap sono integri sulla porta specificata.

```
Connected to ..
```

10. [Se la richiesta non va a buon fine, controlla le regole in entrata sul tuo gruppo di sicurezza VPC.](#) Ad esempio, è possibile utilizzare le seguenti proprietà sulla regola in entrata.

```
Type: All traffic  
Port: Port used by the bootstrap server (e.g. 14001)  
Source: 0.0.0.0/0
```

Riprova la connessione telnet come mostrato nel passaggio precedente. [Se non riesci ancora a connetterti o se la connessione Firehose continua a fallire, contatta l'assistenza.AWS](#)

Quota Amazon Data Firehose

Questa sezione descrive le quote attuali, precedentemente denominate limiti, all'interno di Amazon Data Firehose. Salvo dove diversamente specificato, ogni quota si applica a una Regione specifica.

La console Service Quotas è una posizione centrale in cui è possibile visualizzare e gestire le quote per AWS i servizi e richiedere un aumento della quota per molte delle risorse utilizzate. Utilizza le informazioni sulle quote che forniamo per gestire la tua AWS infrastruttura. Pianifica le richieste di incremento delle quote con un certo anticipo rispetto a quando ne avrai effettivamente bisogno.

Per ulteriori informazioni, consulta gli [endpoint e le quote di Amazon Data Firehose](#) nel. Riferimenti generali di Amazon Web Services

La sezione seguente mostra che Amazon Data Firehose ha la seguente quota.

- Con Amazon MSK come origine per il flusso Firehose, ogni flusso Firehose ha una quota predefinita di 10% di velocità effettiva di lettura per partizione e una dimensione massima del record di MB/sec 10 MB.
- Con Amazon MSK come origine per lo stream Firehose, è prevista una dimensione di record massima di 6 MB se AWS Lambda è abilitata e una dimensione massima di record di 10 MB se Lambda è disabilitata. AWS Lambda limita il record in entrata a 6 MB e Amazon Data Firehose inoltra i record superiori a 6 Mb a un bucket S3 con errore. Se Lambda è disabilitata, Firehose limita il record in entrata a 10 MB. Se Amazon Data Firehose riceve da Amazon MSK una dimensione del record superiore a 10 MB, Amazon Data Firehose invia questo record al bucket di errore S3 ed emette i parametri di Cloudwatch sul tuo account. [Per ulteriori informazioni sui limiti AWS Lambda, consulta Quote Lambda.](#)
- Quando il [partizionamento dinamico](#) su un flusso Firehose è abilitato, è possibile creare una quota predefinita di 500 partizioni attive per quel flusso Firehose. Il conteggio delle partizioni attive corrisponde al numero totale di partizioni attive all'interno del buffer di distribuzione. Ad esempio, se la query di partizionamento dinamico costruisce 3 partizioni al secondo e disponi di una configurazione di suggerimento per il buffering che attiva la distribuzione ogni 60 secondi, in media si avranno 180 partizioni attive. Una volta che i dati vengono distribuiti in una partizione, quest'ultima non è più attiva. Se sono necessarie più partizioni, è possibile creare più flussi Firehose e distribuire le partizioni attive su di essi.
- Quando il [partizionamento dinamico](#) su un flusso Firehose è abilitato, è supportato un throughput massimo di 1 GB al secondo per ogni partizione attiva.

- Ogni account avrà la seguente quota per il numero di stream Firehose per regione:
 - Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon), Europa (Irlanda), Asia Pacifico (Tokyo): 5.000 flussi Firehose
 - Europa (Francoforte), Europa (Londra), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Seoul), Asia Pacifico (Mumbai), (Stati Uniti occidentali), Canada AWS GovCloud (Ovest), Canada (Centrale): 2.000 flussi Firehose
 - Europa (Parigi), Europa (Milano), Europa (Stoccolma), Asia Pacifico (Hong Kong), Asia Pacifico (Osaka), Sud America (San Paolo), Cina (Ningxia), Cina (Pechino), Medio Oriente (Bahrein), (Stati Uniti orientali), Africa AWS GovCloud (Città del Capo): 500 flussi Firehose
 - Europa (Zurigo), Europa (Spagna), Asia Pacifico (Hyderabad), Asia Pacifico (Giacarta), Asia Pacifico (Melbourne), Medio Oriente (Emirati Arabi Uniti), Israele (Tel Aviv), Canada occidentale (Calgary), Canada (Centrale), Asia Pacifico (Malesia), Asia Pacifico (Tailandia), Messico (Centrale): 100 flussi Firehose
 - Se superi questo numero, una chiamata a [CreateDeliveryStream](#) genera un'eccezione `LimitExceededException`. Per aumentare questa quota, è possibile utilizzare le [Service Quotas](#) se disponibili nella propria regione. Per ulteriori informazioni sull'utilizzo di Service Quotas, consulta [Richiesta di un aumento delle quote](#).
- Quando Direct PUT è configurato come origine dati, ogni flusso Firehose fornisce la seguente quota [PutRecords](#) [PutRecordBatch](#) richieste combinate:
 - Per Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon) ed Europa (Irlanda): 500.000. records/second, 2,000 requests/second, and 5 MiB/second
 - Per altri Regioni AWS: 100.000. records/second, 1,000 requests/second, and 1 MiB/second

Se uno stream Direct PUT subisce una limitazione a causa di volumi di acquisizione dati più elevati che superano la capacità di throughput di uno stream Firehose, Amazon Data Firehose aumenta automaticamente il limite di throughput dello stream fino a contenere la limitazione. A seconda dell'aumento del throughput e del throttling, Firehose potrebbe impiegare più tempo per aumentare la velocità di trasmissione di uno stream ai livelli desiderati. Per questo motivo, continua a riprovare i record di acquisizione dei dati non riusciti. Se prevedi che il volume di dati aumenti in caso di picchi improvvisi di grandi dimensioni o se il tuo nuovo stream richiede una velocità di trasmissione superiore al limite di throughput predefinito, richiedi di aumentare il limite di throughput.

Esiste una scala proporzionale di tre quote per le quote. Ad esempio, se si aumenta la quota di throughput negli Stati Uniti orientali (Virginia settentrionale), negli Stati Uniti occidentali (Oregon) o in Europa (Irlanda) a 10. MiB/second, the other two quota increase to 4,000 requests/second and 1,000,000 records/second

Note

- Non utilizzate limiti e quote a livello di risorsa per controllare l'utilizzo del servizio.
 - Quando Kinesis Data Streams è configurato come origine dati, questa quota non si applica e Amazon Data Firehose è scalabile verso l'alto e verso il basso senza limiti.
 - Se la quota aumentata è molto superiore al traffico in esecuzione, può causare la distribuzione di piccoli batch sulle destinazioni. Questo è inefficiente e può comportare costi più alti per i servizi di destinazione. Assicurati di aumentare la quota solo per adattarla al traffico in esecuzione attuale e di aumentarla ulteriormente in caso di incremento del traffico.
 - Record di dati più piccoli possono comportare costi più elevati. [I prezzi di importazione di Firehose](#) si basano sul numero di record di dati inviati al servizio, moltiplicato per la dimensione di ciascun record arrotondato per eccesso ai 5 KB (5120 byte) più vicini. Quindi, a parità di volume di dati in entrata (byte), se c'è un numero maggiore di record in entrata, il costo da sostenere sarà maggiore. Ad esempio, se il volume totale di dati in entrata è di 5 MiB, l'invio di 5 MiB di dati oltre 5.000 record costa di più rispetto all'invio della stessa quantità di dati utilizzando 1.000 record. [Per ulteriori informazioni, consulta Amazon Data Firehose in the AWS Calculator.](#)
- Ogni stream Firehose archivia i record di dati per un massimo di 24 ore nel caso in cui la destinazione di consegna non sia disponibile e se la fonte lo è. DirectPut Se l'origine è Kinesis Data Streams (KDS) e la destinazione non è disponibile, i dati vengono conservati in base alla configurazione KDS.
 - La dimensione massima di un record inviato ad Amazon Data Firehose, prima della codifica base64, è 1.000 KiB.
 - L'operazione [PutRecordBatch](#) può sostenere fino a 500 record o 4 MiB per chiamata, a seconda del limite raggiunto per primo. Questa quota non può essere modificata.
 - Ciascuna delle seguenti operazioni può fornire fino a cinque chiamate al secondo, un limite massimo.
 - [CreateDeliveryStream](#)
 - [DeleteDeliveryStream](#)
 - [DescribeDeliveryStream](#)
 - [ListDeliveryStreams](#)
 - [UpdateDestination](#)

- [TagDeliveryStream](#)
- [UntagDeliveryStream](#)
- [ListTagsForDeliveryStream](#)
- [StartDeliveryStreamEncryption](#)
- [StopDeliveryStreamEncryption](#)
- Gli hint dell'intervallo di buffer variano da 60 secondi a 900 secondi.
- Per la distribuzione da Amazon Data Firehose ad Amazon Redshift, sono supportati solo i cluster Amazon Redshift accessibili pubblicamente.
- L'intervallo di durata dei nuovi tentativi è compreso tra 0 secondi e 7.200 secondi per Amazon Redshift OpenSearch e Service Delivery.
- Quando la destinazione è Amazon S3, Amazon Redshift o OpenSearch Service, Amazon Data Firehose consente fino a 5 chiamate Lambda eccezionali per shard. Per Splunk, la quota è di 10 invocazioni Lambda in sospeso per partizione.
- È possibile utilizzare un CMK di tipo CMK CUSTOMER_MANAGED_CMK per crittografare fino a 500 stream Firehose.

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti alla documentazione di Amazon Data Firehose.

Modifica	Descrizione	Data della modifica
Rimozione del database come fonte (anteprima pubblica)	Il database come fonte (anteprima pubblica) è ora rimosso.	24 settembre 2025
Aggiunto il supporto per la gerarchia multicatena di Glue	Ciò semplifica l'integrazione di Firehose con Amazon S3 Tables senza la necessità di collegamenti di risorse tra il catalogo dati predefinito e <code>S3TablesCatalog</code> . Vedi Configurazione di uno stream Firehose sulle tabelle Amazon S3 .	14 maggio 2025
Database aggiunto come sorgente (anteprima pubblica)	Ora puoi replicare le modifiche del database su Apache Iceberg Tables in Amazon S3.	15 novembre 2024
Versione General Availability (GA) per le tabelle Apache Iceberg aggiunte come destinazione	È possibile creare uno stream Firehose con Apache Iceberg Tables come destinazione. Per informazioni, consulta Fornisci dati a Apache Iceberg Tables .	30 settembre 2024
Sono stati aggiunti esempi di tipi di dati	Sono stati aggiunti esempi di tipi di dati supportati per Apache Iceberg Tables. Per informazioni, consulta Comprendi i tipi di dati supportati .	22 agosto 2024
Lancio di una nuova regione	Amazon Data Firehose è ora disponibile in Asia Pacifico (Malesia). Per informazioni, consulta Quota Amazon Data Firehose .	22 agosto 2024

Modifica	Descrizione	Data della modifica
Aggiunte le tabelle Apache Iceberg come destinazione (anteprima pubblica)	È possibile creare uno stream Firehose con Apache Iceberg Tables come destinazione. Per informazioni, consulta Fornisci dati a Apache Iceberg Tables .	25 luglio 2024
Suggerimenti per il buffering di Snowflake	Snowflake ora supporta i suggerimenti per il buffering. Per informazioni, consulta the section called “Configura le impostazioni di destinazione per Snowflake” .	25 luglio 2024
Snowflake come destinazione in nuove regioni	Snowflake è ora disponibile come destinazione in Asia Pacifico (Singapore), Asia Pacifico (Seoul) e Asia Pacifico (Sydney). Per informazioni, consulta the section called “Configura le impostazioni di destinazione per Snowflake” .	25 luglio 2024
Sezioni ristrutturare del manuale utente	Navigazione semplificata per le sezioni della guida per l'utente. Consulta Inviare dati a uno stream Firehose e Risoluzione degli errori .	5 luglio 2024
Amazon Data Firehose si integra con Gestione dei segreti AWS	Ora puoi accedere ai tuoi segreti e automatizzare la rotazione delle credenziali in modo sicuro con Secrets Manager. Per informazioni, consulta the section called “Effettua l'autenticazione con Gestione dei segreti AWS” .	06 giugno 2024
Aggiunto il supporto per l'acquisizione dei log per Dynatrace	Ora puoi inviare log ed eventi a Dynatrace per ulteriori analisi. Per informazioni, consulta the section called “Configura le impostazioni di destinazione per Dynatrace” .	18 aprile 2024
Versione General Availability (GA) per Snowflake come destinazione	Snowflake è ora disponibile a livello generale come destinazione. Per informazioni, consulta the section called “Configura le impostazioni di destinazione per Snowflake” .	17 aprile 2024

Modifica	Descrizione	Data della modifica
Amazon Kinesis Data Firehose è ora noto come Amazon Data Firehose	Amazon Kinesis Data Firehose è stato rinominato Amazon Data Firehose. Per informazioni, consultare Che cos'è Amazon Data Firehose .	9 febbraio 2024
Aggiunta Snowflake come destinazione (anteprima pubblica)	È possibile creare uno stream Firehose con Snowflake come destinazione. Per informazioni, consulta the section called “Configura le impostazioni di destinazione per Snowflake” .	19 gennaio 2024
È stata aggiunta la decompressione automatica dei registri CloudWatch	È possibile abilitare la decompressione su stream nuovi o esistenti per inviare dati di log decompressi alle destinazioni CloudWatch Firehose. Per informazioni, consulta the section called “Invia CloudWatch log a Firehose” .	15 dicembre 2023
Aggiunto Splunk Observability Cloud come destinazione	Puoi creare uno stream Firehose con Splunk Observability Cloud come destinazione. Per informazioni, consulta the section called “Configura le impostazioni di destinazione per Splunk Observability Cloud” .	3 ottobre 2023
Aggiunto Amazon Managed Streaming for Apache Kafka come origine dati	Ora puoi configurare Amazon MSK per inviare informazioni a uno stream Firehose. Per informazioni, consulta the section called “Configurazione delle impostazioni di origine per Amazon MSK” .	26 settembre 2023

Modifica	Descrizione	Data della modifica
È stato aggiunto il supporto per il tipo DocumentID per la destinazione del servizio OpenSearch	Se OpenSearch Service è la destinazione dello stream Firehose, il tipo DocumentID indica il metodo per impostare l'ID del documento. I metodi supportati sono l'ID del documento generato da Firehose e l'ID del documento generato dal OpenSearch servizio. Per informazioni, consulta the section called “Configure le impostazioni di destinazione” .	10 maggio 2023
Aggiunto il supporto per il partizionamento dinamico	È stato aggiunto il supporto per il partizionamento dinamico continuo dei dati di streaming in Amazon Data Firehose. Per informazioni, consulta Partizione dei dati di streaming .	31 agosto 2021
Aggiunta di un argomento sui prefissi personalizzati.	È stato aggiunto un argomento sulle espressioni che è possibile utilizzare durante la creazione di un prefisso personalizzato per i dati distribuiti ad Amazon S3. Per informazioni, consulta the section called “Comprendi i prefissi personalizzati per gli oggetti Amazon S3” .	20 dicembre 2018
Aggiunto un nuovo tutorial su Amazon Data Firehose	È stato aggiunto un tutorial che dimostra come inviare i log di flusso di Amazon VPC a Splunk tramite Amazon Data Firehose. Per informazioni, consulta Inserisci i log di flusso VPC in Splunk utilizzando Amazon Data Firehose .	30 ottobre 2018
Aggiunte quattro nuove regioni Amazon Data Firehose	Aggiunta di Parigi, Mumbai, San Paolo e Londra. Per ulteriori informazioni, consulta Quota Amazon Data Firehose .	27 giugno 2018
Aggiunte due nuove regioni Amazon Data Firehose	Aggiunta di Seul e Montreal. Per ulteriori informazioni, consulta Quota Amazon Data Firehose .	13 giugno 2018

Modifica	Descrizione	Data della modifica
Nuovo Kinesis Streams come funzione di origine	È stato aggiunto Kinesis Streams come potenziale fonte di record per uno stream Firehose. Per ulteriori informazioni, consulta Scegli la fonte e la destinazione per il tuo stream Firehose .	18 agosto 2017
Aggiornamento alla documentazione della console	La procedura guidata per la creazione di stream Firehose è stata aggiornata. Per ulteriori informazioni, consulta Tutorial: Creare uno stream Firehose dalla console .	19 luglio 2017
Nuova trasformazione dei dati	Puoi configurare Amazon Data Firehose per trasformare i tuoi dati prima della consegna dei dati. Per ulteriori informazioni, consulta Trasforma i dati di origine in Amazon Data Firehose .	19 dicembre 2016
Nuovo tentativo del comando COPY di Amazon Redshift	Puoi configurare Amazon Data Firehose per riprovare un comando COPY sul tuo cluster Amazon Redshift in caso di errore. Per ulteriori informazioni, consultare Tutorial: Creare uno stream Firehose dalla console , Comprendi la distribuzione dei dati in Amazon Data Firehose e Quota Amazon Data Firehose .	18 maggio 2016
Nuova destinazione Amazon Data Firehose, Amazon Service OpenSearch	Puoi creare uno stream Firehose con Amazon OpenSearch Service come destinazione. Per ulteriori informazioni, consultare Tutorial: Creare uno stream Firehose dalla console , Comprendi la distribuzione dei dati in Amazon Data Firehose e Concedi a Firehose l'accesso a una destinazione di servizio pubblico OpenSearch .	19 aprile 2016
Nuove CloudWatch metriche e funzionalità di risoluzione dei problemi migliorate	Aggiornati gli argomenti Monitoraggio di Amazon Data Firehose e Risolvi gli errori in Amazon Data Firehose .	19 aprile 2016

Modifica	Descrizione	Data della modifica
Nuovo agente Kinesis avanzato	Aggiornato Configurare l'agente Kinesis per l'invio di dati .	11 aprile 2016
Nuovi agenti Kinesis	Aggiunto Configurare l'agente Kinesis per l'invio di dati .	2 ottobre 2015
Rilascio iniziale	Versione iniziale della Amazon Data Firehose Developer Guide.	4 ottobre 2015